ЗАПРОС

о предоставлении ценовой информации на выполнение работ по миграции АИС «Регистрация заявлений получателей техпомощи» (версия 2.0) в облачную инфраструктуру объединенного ЦОД правительственного комплекса, включая доработку под требования Технических условий и требования информационной безопасности

Сведения об Исполнителе и Заказчике

Государственный Заказчик: Министерство экономического развития Российской Федерации (далее – Заказчик).

Исполнитель выбирается по результатам открытого конкурса в электронной форме на право заключения государственного контракта (далее – Исполнитель).

Объект закупки:

АИС «Регистрация заявлений получателей техпомощи» (версия 2.0), выполнение работ по миграции в облачную инфраструктуру объединенного центра обработки данных (далее – ЦОД) правительственного комплекса, включая доработку под требования Технических условий по размещению информационных систем федеральных органов исполнительной власти объединённом центре обработки данных правительственного комплекса и требования информационной безопасности (прилагаются к настоящему запросу).

Сокращения, термины и определения

IP	(аббр. от англ. Internet Protocol, досл. «межсетевой протокол») — маршрутизируемый протокол сетевого уровня стека TCP/IP
VLAN	(аббр. от англ. Virtual Local Area Network) — топологическая («виртуальная») локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену
ПК	правительственный комплекс
ИС	информационная система
ПО	программное к прикладному программному обеспечению (application software) относятся компьютерные программы, написанные для пользователей или самими пользователями, для задания компьютеру конкретной работы. Программы обработки заказов или создания списков рассылки — пример прикладного программного обеспечения
МСЭ	межсетевой экран
НСД	несанкционированный доступ
ЦОД	центр обработки данных
ОЦОД ПК	объединённый центр обработки данных правительственного комплекса
ОК	открытый контур ОЦОД ПК
ЗК	закрытый контур ОЦОД ПК
ОС	операционная система
Облако	совокупность виртуальных сред ОЦОД ПК
Системное ПО (СПО)	системное программное обеспечение - комплекс программ, которые обеспечивают управление компонентами компьютерной системы, такими как процессор, оперативная память, устройства ввода-вывода, сетевое оборудование, выступая как «межслойный интерфейс», с одной стороны которого аппаратура, а с другой — приложения

	пользователя. В отличие от прикладного программного обеспечения, системное не решает конкретные практические задачи, а лишь обеспечивает работу других программ, предоставляя им сервисные функции, абстрагирующие детали аппаратной и микропрограммной реализации вычислительной системы, управляет аппаратными ресурсами вычислительной системы
ТУ ИС ФОИВ ОЦОД ПК	Технические условия по размещению информационных систем федеральных органов исполнительной власти в объединённом центре обработки данных правительственного комплекса (предоставляется Заказчиком).
ФОИВ	федеральный орган исполнительной власти
Комиссия	Комиссия по вопросам международной гуманитарной и технической помощи при Правительстве Российской Федерации
Система, АИС	АИС (автоматизированная информационная система) «Регистрация заявлений получателей техпомощи» (версия 2.0)
СМЭВ	система межведомственного электронного взаимодействия
Удостоверение	удостоверение о признании средств, товаров и услуг технической помощью (содействием)
ФТС	Федеральная таможенная служба

1. ЦЕЛИ И ЗАДАЧИ

Цель

Обеспечение бесперебойного функционирования АИС, размещенной в ОЦОД ПК и готовой к проведению аттестационных испытаний по требованиям информационной безопасности.

Задачи

В рамках выполнения Работ требуется:

- разработать необходимые для миграции и последующей аттестации Системы проекты документов;
- доработать модули Системы в соответствии с требованиями информационной безопасности и ТУ ИС ФОИВ ОЦОД ПК;
- разместить Систему в ОЦОД ПК.

2. ПЕРЕЧЕНЬ ДОКУМЕНТОВ, В СООТВЕТСТВИИ С КОТОРЫМИ ДОЛЖНЫ ВЫПОЛНЯТЬСЯ РАБОТЫ

Результаты выполняемых работ должны в полной мере соответствовать требованиям следующих нормативных правовых актов Российской Федерации:

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
- постановление Правительства Российской Федерации от 5 июня 2008 г. № 437 «О Министерстве экономического развития Российской Федерации»;
- постановление Правительства Российской Федерации от 18 мая 2009 г. № 424 «Об особенностях подключения федеральных государственных систем к информационно-

телекоммуникационным сетям»;

- постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- постановление Правительства Российской Федерации от 06 июля 2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;
- постановление Правительства Российской Федерации от 8 сентября 2010 г. № 697 «О единой системе межведомственного электронного взаимодействия»;
- постановление Правительства Российской Федерации от 24 октября 2011 г. № 861 «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)»;
- приказ ФСБ России от 09 февраля 2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- методический документ ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах»;
- методический документ ФСТЭК России от 5 февраля 2021 г. «Методика оценки угроз безопасности информации»;
- ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»;
- ГОСТР 58412-2019 «Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке безопасного программного обеспечения».

В случае издания новых нормативных правовых актов, а также иных нормативных документов (приказов, методических рекомендаций, ГОСТов и т.п.) связанных с информационными технологиями, информационной безопасностью и защитой информации в государственных информационных системах, до момента завершения выполнения первого этапа

работ, Исполнителю необходимо также ими руководствоваться при выполнении работ.

3. О СИСТЕМЕ

Система предназначена для:

− подачи заявителями в электронном виде заявлений в Комиссию: о регистрации проектов и программ технической помощи (содействия) и внесения в них изменений, о подтверждении средств, товаров, работ и услуг технической помощью (содействием), о внесении изменений в удостоверения, с последующей их печатью на бумажный носитель;

− отслеживания статуса поданных заявлений в Комиссию;

− просмотра нормативной правовой базы, связанной с технической помощью (содействием) и получения информацию о работе Комиссии и Системы (портала для заявителей);

− рассмотрения поступивших заявления в электронном виде секретариатом Комиссии (сотрудниками Минэкономразвития России) и членами Комиссии и рабочей группы Комиссии (сотрудники федерльных органов исполнительной власти и Госкорпорации «Росатом») на своих рабочих местах;

− распечатывания на бумажном носителе: удостоверений, протоколов Комиссии и рабочей группы Комиссии, по рассмотренным заявлениям;

− предоставления сведений в ФТС России по СМЭВ.

Кроме того, Система позволяет:

− вести Единый реестр проектов и программ технической помощи (содействия);

− вести Единую базу выданных удостоверений и рассмотренных заявлений;

− регистрировать пользователей, и вести реестр зарегистрированных пользователей.

В соответствии с государственным контрактом от 8 ноября 2019 г. № 0173100008619000065 система была модернизирована (переконфигурирована и переведена на новое российское программное обеспечение) на версию 2.0.

Система функционирует на базе системы RNSWeb – российского программного обеспечения, зарегистрированного в Едином реестре российских программ для электронных вычислительных машин и баз данных (https://reestr.minsvyaz.ru/reestr/107134/), функционирующего под управлением операционной системы Microsoft Windows Server Standard 2008 R2 (сертификат ФСТЭК №3366) и использующего для управления базой данных свободно распространяемую СУБД PostgreSQL.

Система доступна в информационно-телекоммуникационной сети «Интернет» по адресу https://commission.ecomomy.gov.ru» (в системе учета информационных систем ее идентификатор № 10.0006660). Описание Системы приведено в Приложении № 1 к настоящему техническому заданию.

4. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ

Все работы в части информационной безопасности должны осуществляться с учетом положений Федерального закона от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности».

4.1. Подготовка к миграции Системы в соответствие требованиям ТУ ИС ФОИВ ОЦОД ПК.

4.1.1 Разработка документа «Частное техническое задание на модернизацию системы защиты информации АИС» (далее – ЧТЗ ИБ).

В данный документ должны быть включены все аспекты по приведению Системы в соответствие с ТУ ИС ФОИВ ОЦОД ПК. Данный документ должен отражать необходимый перечень доработок и дополнительных настроек Системы, обеспечивающий после их реализации беспрепятственное размещение Системы в ОЦОД ПК.

ЧТЗ ИБ и Модель угроз безопасности информации (п. 4.1.3) направляется Заказчиком на согласование с федеральным органом исполнительной власти, уполномоченным в области безопасности, и с федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий в части, касающейся выполнения установленных требований о защите информации. В случае наличия замечаний к указанным документам в процессе согласования Исполнитель обеспечивает устранение указанных замечаний в том числе в рамках гарантийных обязательств.

4.1.2 Разработка документа «Частное техническое задание на доработку АИС» (далее – ЧТЗ на доработку),

ЧТЗ должно быть разработано с учетом требований государственных стандартов (ГОСТ 34.601-90 — в части определения стадий и этапов работ; ГОСТ 34.602-89 — в части состава, содержания и правил оформления документа «Частное техническое задание»).

ЧТЗ должно содержать уточненную постановку задачи по доработке Системы в целях приведения ее в соответствие с требованиями ТУ ИС ФОИВ ОЦОД ПК .

При разработке ЧТЗ на доработку должно быть предусмотрено требование использования СПО, внесенное в Единый реестр российских программ для электронных вычислительных машин и баз данных (реестр отечественного ПО) или ПО с открытым кодом.

Используемое программное обеспечение должно иметь вариант бессрочной лицензии, а также поддержку производителя в части выпуска обновлений с исправлениями ошибок и проблем безопасности, а также реализации поддержки нового оборудования в течении не менее 1 года

с момента размещения в ОЦОД ПК. Допускается поддержка производителя в части выпуска только обновлений критических проблем безопасности и важных ошибок в течение не менее 2 лет с момента размещения в ОЦОД ПК.

Данный документ, по согласованию с Заказчиком, может быть дополнен необходимыми требованиями, не противоречащими ТУ ИС ФОИВ ОЦОД ПК.

Данный документ должен быть согласован с Заказчиком и (или) организацией, обслуживающей ОЦОД ПК.

4.1.3 Разработка документа «Техническое решение по размещению АИС в Облаке (далее – Техническое решение) в составе следующих разделов (при необходимости):

- Общие положения (Наименование проекта, Наименования и реквизиты);
- Описание ИС, подлежащей размещению в Облаке, а именно:
  - Наименование ИС, подлежащей размещению в Облаке ОЦОД ПК;
  - Исходное описание ИС, в том числе:
    - Исходная схема компонент ИС;
    - Исходный состав ИС;
- Основные решения по размещению ИС в Облаке ОЦОД ПК, а именно:
  - Целевая схема ИС, в том числе:
    - Продуктивная зона;
    - Предпродуктивная зона;

- Зона разработки и тестирования;

• Решения по виртуальным ресурсам;
• Решения по ОС и ПО на ВМ;
• Решения по обновлению ОС и ПО;
• Решения по использованию услуг ПК;
• Решения по сетевой связности;
• Решения по организации VLAN и IP-адресации;
• Решения по переносу, репликации и синхронизации данных ИС;
• Решения по резервному копированию;
• Решения по переключению пользователей ИС;
• Решения по внешним каналам связи;
• Решения по использованию и взаимодействию с инфраструктурными и технологическими сервисами ОЦОД ПК;
• Решения по размещению и использованию средств разработки;
• Решения по информационной безопасности, включающие:
  - Схема размещения и использования компонент безопасности ИС;
  - Решения по ограничениям сетевого трафика (правила фильтрации для МСЭ);
  - Решения по удаленному доступу к оборудованию и компонентам ИС;
  - Решения по организации защиты виртуальной среды ИС;
  - Решения по контролю целостности и защите от НСД;
  - Решения по организации антивирусной защиты;
  - Решения по контролю действий привилегированных пользователей;
  - Решения по контролю и поиску уязвимостей;
  - Решения по переносу и использованию защищённых сетей;
• План размещения ИС, включающий:
  - Технология размещения ИС в Облаке ОЦОД ПК;
  - План размещения ИС в Облаке ОЦОД ПК;
  - Технологические окна для размещения ИС;
  - План аварийного восстановления и отката изменений;
• Виртуальные ресурсы, IP-план и организация VLAN для ИС, включающие:
  - Зона разработки и тестирования (при обоснованной необходимости);
  - Препродуктивная зона ОК;
  - Препродуктивная зона ЗК;
  - Продуктивная зона ОК;
  - Продуктивная зона ЗК;
• Схема связи внешних сервисов или приложений;
• Матрица межсетевого взаимодействия;
• Схема размещения компонент по контурам, зонам и VLAN;
• Заявки на размещение компонент системы;
• Заявки на доступ;
• Инструкции для обсуживающей ИС организации.

При разворачивании Системы в Облаке должно использоваться СПО, внесенное в Единый реестр российских программ для электронных вычислительных машин и баз данных (реестр отечественного ПО) или СПО с открытым кодом.

Используемое программное обеспечение должно иметь бессрочную лицензию, а также поддержку производителя в части выпуска обновлений с исправлениями ошибок и проблем безопасности, а также реализации поддержки нового оборудования в течении не менее 1 года с момента размещения в ОЦОД ПК. Допускается поддержка производителя в части выпуска только обновлений критических проблем безопасности и важных ошибок в течение не менее 2 лет с момента размещения в ОЦОД ПК.

Данный документ должен быть согласован с Заказчиком и организацией, обслуживающей ОЦОД ПК.

4.1.4 Разработка документа документ «Модель угроз безопасности информации».

Должны быть определены угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации в системе, и разработана на их основе модель угроз безопасности информации.

Данный документ должен быть составлен в качестве документации, необходимой для проведения аттестации Системы и не противоречить ТУ ИС ФОИВ ОЦОД ПК.

Кроме того, разработчиком программного обеспечения должен быть определен перечень мер, подлежащих реализации при его разработке в целях предотвращения появления и устранения уязвимостей программ в процессах их жизненного цикла. Выбор и уточнение мер по разработке безопасного ПО должен основываться на результатах проводимого разработчиком ПО анализа угроз безопасности информации, в результате которого должны быть определены актуальные для среды разработки ПО угрозы безопасности информации.

4.2. Доработка Системы в соответствии с требованиями ТУ ИС ФОИВ ОЦОД ПК.

Необходимо провести доработку всех модулей Системы в соответствии с подготовленным ЧТЗ на доработку, Техническим решением и ЧТЗ ИБ, а также необходимую конфигурацию и настройку СПО и ППО. Также развернуть компоненты Системы на новое СПО и ППО или новые версии СПО и ППО (при наличии такой необходимости), а также провести миграцию данных Системы. Кроме того, необходимо проверить работоспособность всех компонентов, их взаимодействия между собой и с внешними ИС в рамках используемой интеграции.

Для текущей версии необходимо выполнить доработку следующих модулей Системы:

Перечень модулей (подсистем), подлежащих доработке, с указанием конкретных работ.

Доработка Системы должна быть произведена в необходимом объеме для миграции в Облако ОЦ ОД ПК, включая доработку и дополнительную настройку, обеспечивающую готовность

к проведению аттестации Системы по требованиям информационной безопасности в соответствии с установленным в Акте классификации федеральной государственной информационной системы АИС «Регистрация заявлений получателей техпомощи» от 17.07.2018 № Д13вн-788 третьим классом защищенности государственной информационной системы (К3).

При разворачивании Системы в Облаке должно использоваться СПО, внесенное в Единый реестр российских программ для электронных вычислительных машин и баз данных (реестр отечественного ПО) или СПО с открытым кодом.

Окончательный объем доработок и дополнительных настроек Системы определяется в процессе согласования документа ЧТЗ на доработку, Технического решения и документа ЧТЗ ИБ. Могут быть, как добавлены, так и исключены работы по доработкам и дополнительным настройкам модулей Системы.

4.3. Миграция Системы в ОЦОД ПК.

Необходимо провести работы по развертыванию Системы во всех необходимых контурах ОЦОД ПК, миграции данных, проверить работоспособность всех компонентов, их взаимодействия между собой и с внешними ИС в рамках используемой интеграции.

Во время работ по миграции актуальные данные Системы не должны быть потеряны.

При этом работы по миграции Системы не должны нарушать его работоспособность на длительный период (более одного дня).

В период проведения работ необходимо провести предварительные испытания, опытную эксплуатацию Системы, приемочные испытания с учетом сделанных доработок в соответствии с ПМИ и программой опытной эксплуатации.

Все работы по миграции Системы в рабочем порядке согласуются с представителями эксплуатирующей организации ОЦОД ПК.

5. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО МИГРАЦИИ СИСТЕМЫ

№ п/п	Наименование работ	Срок выполнения работ	Результаты работ
1	Подготовка к миграции Системы в соответствии с требованиями ТУ ИС ФОИВ ОЦОД ПК в соответствии с требованиями п. 4.1 настоящего Технического задания	с даты заключения государственного контракта в течение 30 календарных дней	- документ «Частное техническое задание на модернизацию системы защиты информации АИС «Регистрация заявлений получателей техпомощи» (версия 2.0)»; - документ «Техническое решение по размещению АИС «Регистрация заявлений получателей техпомощи» (версия 2.0) в Облаке»; - документ «Частное техническое задание на доработку АИС «Регистрация заявлений получателей техпомощи» (версия 2.0)»; - документ «Модель угроз безопасности информации»
2	Доработка Системы в соответствии с требованиями ТУ ИС ФОИВ ОЦОД ПК в соответствии с требованиями п. 4.2 настоящего Технического задания	с момента окончания 1-го этапа в течение 70 календарных дней	- Доработанная по результатам ЧТЗ на доработку, Технического решения и ЧТЗ ИБ Система; - Отчет о выполнении работ по доработке Системы; Остальные документы, описанные в п.8 настоящего ТЗ.
3	Миграция Системы в ОЦОД ПК в соответствии с требованиями п. 4.3 настоящего Технического задания	с момента окончания 2-го этапа в течение 20 календарных дней	- Доработанная по результатам испытаний и функционирующая в Облаке ОЦОД ПК Система; - Измененные по результатам испытаний эксплуатационные и другие документы (в случае, если были внесены изменения); - Исходные коды ППО Системы на электронном носителе информации; - Протокол предварительных испытаний; - Журнал опытной эксплуатации; - Протокол приемочных испытаний

6. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ РАБОТ

В рамках настоящих Работ должны быть проведены следующие испытания:

- выполнение квалификационного тестирования ПО в соответствии с ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»:
  - предварительные автономные испытания;
  - предварительные комплексные испытания:
  - опытная эксплуатация;
  - приемочные испытания.

Испытания Системы должны проводиться в следующем порядке:

- проведение тестирования;
- проведение предварительных испытаний доработок;
- проведение опытной эксплуатации;
- проведение приемочных испытаний.

Предварительные испытания после окончания доработок Системы должны проводиться по разработанной Исполнителем и согласованной с Заказчиком Программе и методике.

В Программе и методике предварительных испытаний должна быть приведена следующая информация:

- перечень функций Системы, подлежащих испытаниям;
- описание взаимосвязей объекта испытаний с другими частями Системы;
- условия, порядок и методы проведения испытаний и обработки результатов;
- критерии приемки частей по результатам испытаний.

При подготовке документа необходимо руководствоваться ГОСТ 34.603.

По результатам предварительных испытаний должны быть оформлены следующие документы:

- Протокол предварительных испытаний доработок Системы (проект).
- Акт предварительных испытаний доработок Системы (проект).

Протокол предварительных комплексных испытаний и акт должны содержать заключение о возможности (невозможности) приемки Системы в опытную эксплуатацию.

Предварительные испытания должны проводиться в соответствии с ГОСТ 34.603-92.

Предварительные испытания проводятся на территории Заказчика с участием его представителей. Исполнитель должен предоставить для проведения предварительных испытаний тестовый стенд, включающий все необходимое аппаратное и программное обеспечение, в том числе необходимые инструменты тестирования.

При проверке взаимодействия задач в системе и выполнения требований ЧТЗ ИБ допускается использование программных заглушек, имитирующих работу сервисов смежных и внешних,
по отношению к Системе систем, в случае неготовности этих систем к испытаниям и (или) недоступности сервисов этих систем, и (или) отсутствии необходимых данных в этих системах.

Для проверки правильности функционирования Системы при выполнении каждой его функции и готовности пользователей к работе с Системой должна быть проведена опытная эксплуатация.

Исполнителем должен быть разработан документ «Программа опытной эксплуатации Системы», в соответствии с которой должна быть проведена опытная эксплуатация.

При подготовке документа необходимо руководствоваться ГОСТ 34.603.

В документе должна быть приведена следующая информация:

1) условия и порядок функционирования Системы и ее сервисов;

2) продолжительность опытной эксплуатации;

3) порядок устранения недостатков, выявленных в процессе опытной эксплуатации.

Программа опытной эксплуатации должна быть согласована с Заказчиком.

В опытной эксплуатации принимают участие специалисты Минэкономразвития России с привлечением сотрудников Исполнителя.

Исполнитель обеспечивает консультирование специалистов в период опытной эксплуатации.

До начала проведения опытной эксплуатации Система должна быть развернута в предпродуктивной среде и доступна для проведения опытной эксплуатации;

По итогам должен быть составлен документ «Акт приемки АИС «Регистрация заявлений получателей техпомощи» (версия 2.0) в опытную эксплуатацию».

Минимальная продолжительность опытной эксплуатации должна составлять не менее одной недели. Точный срок проведения опытной эксплуатации определяется Заказчиком и должен быть указан в программе опытной эксплуатации.

Во время опытной эксплуатации должен вестись рабочий журнал (журнал опытной эксплуатации Системы), в который заносятся сведения о продолжительности ее функционирования, отказах, сбоях, аварийных ситуациях, изменениях параметров, корректировках документации и программных средств, наладке технических средств. Сведения фиксируют в журнале с указанием даты и ответственного лица.

По результатам опытной эксплуатации комиссия с участием представителей Заказчика и Исполнителя принимает решение о возможности предъявления Системы на приемочные испытания.

Опытная эксплуатация завершается оформлением документа «Акт о завершении опытной эксплуатации и допуске системы к приемочным испытаниям».

Исполнителем должен быть разработан документ «Программа и методика приемочных испытаний АИС «Регистрация заявлений получателей техпомощи» (версия 2.0)». При подготовке документа необходимо руководствоваться ГОСТ 34.603.

В документе должна быть приведена следующая информация:

1) перечень объектов, выделенных для испытаний, и перечень требований, которым они должны соответствовать (со ссылкой на пункты Технического задания);

2) критерии приемки Системы и ее частей;

3) условия и сроки проведения испытаний;

4) средства для проведения испытаний;

5) фамилии лиц, ответственных за проведение испытаний;

6) методику испытаний и обработки их результатов;

7) перечень оформляемой документации.

Программа и методика приемочных испытаний должна включать (при необходимости), помимо функциональных проверок, также проверки инсталляции, деинсталляции решения, сборки дистрибутива из исходных кодов (в случае компилируемых кодов), проверку требований к производительности, восстановлению после сбоев и другие нефункциональные проверки требований ЧТЗ на доработку и Технического решения.

Программа и методика приемочных испытаний должна быть согласована с Заказчиком.

Приемочные испытания проводятся комиссией с участием представителей Заказчика и Исполнителя и в соответствии с документом «Программа и методика приемочных испытаний».

При проведении испытаний необходимо руководствоваться ГОСТ 34.603.

Испытания должны проходить на территории Заказчика.

При проверке взаимодействия задач в системе и выполнения требований ЧТЗ ИБ допускается использование программных заглушек, имитирующих работу сервисов смежных и внешних,
по отношению к Системе систем, в случае неготовности этих систем к испытаниям и (или) недоступности сервисов этих систем, и (или) отсутствии необходимых данных в этих системах.

Результаты испытаний оформляются документом «Протокол приемочных испытаний», в котором должны быть указаны результаты проведения испытаний и заключение о возможности приемки Системы в постоянную (промышленную) эксплуатацию.

По результатам приемочных испытаний должны быть подготовлены следующие документы:

- Протокол приемочных испытаний Системы.
- Акт о готовности к вводу в постоянную (промышленную) эксплуатацию.

Все выявленные в ходе испытаний недостатки и несоответствия требованиям ЧТЗ на доработку, Техническому решению и ЧТЗ ИБ должны быть устранены до момента окончания соответствующих испытаний.

Результаты работ должны оформляться и предъявляться Заказчику в соответствии с Перечнем работ и соответствующих результатов согласно разделам 4, 5 и 9 настоящего Технического задания.

7. ТРЕБОВАНИЯ К СРОКАМ И ОБЪЕМАМ ПРЕДОСТАВЛЕНИЯ ГАРАНТИИ КАЧЕСТВА

На результаты выполненных Работ устанавливается гарантийный срок 12 (Двенадцать) месяцев с даты утверждения Заказчиком Акта приемки выполненных Работ.

Исполнитель обязуется устранить все ошибки, возникшие в разработанных и/или доработанных решениях, в подготовленных документах бесплатно в течение гарантийного периода, если они возникли по вине Исполнителя.

Исполнитель обеспечивает гарантии в следующем объеме:

- исправление ошибок в программном обеспечении;
- исправление недостатков, не являющихся ошибками, но препятствующих использованию программного обеспечения в целях, заявленных при его модернизации;
- исправление ошибок в технической и эксплуатационной документации;
- исправление ошибок и недостатков конвертирования данных, если оно производилось.
- исправление ошибок и недостатков, препятствующих получению положительного заключения по результатам проведения аттестационных мероприятий;

После исправления ошибок Исполнитель передает Заказчику исходные коды ППО Системы на электронном носителе информации, а также комплект дистрибутивов на все исправленные модули с расчетом хеш-сумм на электронном носителе информации, и комплект исправленной документации (при необходимости).

В случаях, когда выявленные ошибка и/или недостаток компонентов Системы приводят к существенному нарушению деловых процессов Заказчика, Исполнитель обязан полностью устранить выявленные ошибки и/или недостатки в течение 4 рабочих часов.

Если в период гарантийного срока обнаружатся неисправности, то Исполнитель устранит их за свой счет в минимально возможные сроки, но не более 4 календарных дней с момента обращения со стороны Заказчика.

8. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

По окончании Работ Исполнитель должен представить Заказчику документацию, указанную в разделе 9 настоящего технического задания.

Документация должна полностью соответствовать требованиям к Системе, представленным в данном техническом задании, и содержать актуальные данные (в т.ч. иллюстрации, примеры и т.д.).

В состав поставляемого ПО должны быть включены эксплуатационные документы в объеме, достаточном для правильной настройки и безопасного применения программы.

Вся подготовленная документация должна быть представлена Заказчику на русском языке: в 1-м экземпляре на бумажном носителе и в 2-х экземплярах на электронном носителе (FLASH-карта или внешний жесткий диск) в формате Microsoft Word.

9. СОСТАВ ОТЧЕТНОЙ ДОКУМЕНТАЦИИ

В составе отчетной документации должны присутствовать:

1. Частное техническое задание на модернизацию системы защиты информации АИС «Регистрация заявлений получателей техпомощи» (версия 2.0);
2. Частное техническое задание на доработку АИС «Регистрация заявлений получателей техпомощи» (версия 2.0);
3. Техническое решение по размещению АИС «Регистрация заявлений получателей техпомощи» (версия 2.0) в Облаке;
4. Модель угроз безопасности информации;
5. Отчет о выполнении работ по доработке Системы;
6. Руководство пользователя (в случае необходимости внесения изменений, предоставляется измененный документ)
7. Руководство администратора. (в случае необходимости внесения изменений, предоставляется измененный документ)
8. необходимая по условиям миграции в ОЦОД ПК проектная и эксплуатационная документация на систему защиты информации Системы (состав документации уточняется на стадии согласования ЧТЗ ИБ)
9. Программа и методика предварительных испытаний;
10. Протокол предварительных испытаний (проект);
11. Программа опытной эксплуатации;
12. Акт о готовности доработок Системы к передаче в опытную эксплуатацию (проект);
13. Журнал опытной эксплуатации;
14. Акт о завершении опытной эксплуатации и допуске системы к приемочным испытаниям (проект)
15. Программа и методика приемочных испытаний;
16. Протокол приемочных испытаний (проект);
17. Акт о готовности Системы к вводу в промышленную эксплуатацию (проект).

10. РЕЗУЛЬТАТЫ ВЫПОЛНЕНИЯ РАБОТ

1. доработанная и размещенная в Облаке ОЦОД ПК Система;
2. обеспечение готовности Системы к аттестации по требованиям информационной безопасности;
3. комплект дистрибутивов на все модули с расчетом хеш-сумм на электронном носителе информации;
4. документация, в составе, описанном в п. 9 настоящего Технического задания, включая необходимую проектную и эксплуатационную документацию на систему защиты информации Системы для проведения аттестации по требованиям информационной безопасности;
5. исходные коды ППО Системы на электронном носителе информации.

Предполагаемый срок проведения процедуры закупки: апрель-июнь 2021 г.

Срок предоставления ценовой информации: до 5 марта 2021 г.

Просим всех заинтересованных лиц представить свои предложения по цене поставки товара (проведения работы, оказания услуги) по прилагаемой форме (Приложение 2) и направить их в письменной форме.

Адрес предоставления ценовой информации: Департамент инвестиционной политики и развития предпринимательства, адрес: 123112, Москва, Пресненская наб., д.10, стр.2., тел. +7 (495) 870 29 21 доб. 11357.

Адрес электронной почты для предоставления сканированных копий писем: comissia@economy.gov.ru.

Контактные лица: Григорьева Анастасия Игоревна, Гилёва Анна Александровна.

Информируем, что направленные в адрес Заказчика предложения не будут рассматриваться в качестве заявки на участие в закупке и не дают в дальнейшем каких-либо преимуществ для лиц, подавших указанные предложения.

Настоящий запрос не является извещением о проведении закупки, офертой или публичной офертой и не влечет возникновения каких-либо обязательств Заказчика.

Из ответа на запрос должны однозначно определяться цена единицы работы и общая цена контракта на условиях, указанных в запросе, срок действия предлагаемой цены, расчет такой цены с целью предупреждения намеренного завышения или занижения цен работ.

Приложение № 1

Описание АИС «Регистрация заявлений получателей техпомощи», ее структуры и функций

АИС «Регистрация заявлений получателей техпомощи» (далее – АИС, Система) предназначена для:

- подачи пользователями в электронном виде заявлений в Комиссию:
  - о регистрации проектов и программ технической помощи (содействия) и внесения в них изменений,
  - о подтверждении средств, товаров, работ и услуг технической помощью (содействием),
  - о внесении изменений в удостоверения, с последующей их печатью на бумажный носитель;
- отслеживания статуса поданных заявлений в Комиссию;
- просмотра нормативной правовой базы, связанной с технической помощью (содействием);
- получения информации о работе Комиссии и Системы;
- рассмотрения поступивших заявлений в электронном виде секретариатом Комиссии (сотрудниками) и членами Комиссии и рабочей группы Комиссии (сотрудники федеральных органов исполнительной власти и Госкорпорации «Росатом») на своих рабочих местах;
- распечатывания на бумажном носителе: удостоверений, протоколов Комиссии и рабочей группы Комиссии, по рассмотренным заявлениям;
- предоставления сведений в ФТС России с помощью электронного сервиса, используя в качестве среды информационного обмена СМЭВ.

Пользователями Системы являются:

- внешние пользователи (получатели технической помощи (содействия) – юридические и физические лица – представители юридических лиц);
- внутренние пользователи (сотрудники Минэкономразвития России, члены Комиссии и рабочей группы Комиссии).

Система размещена в сети Интернет по адресу https://commission.economy.gov.ru.

В рамках создания Системы автоматизированы:

− процессы получения и рассмотрения документов по технической помощи (содействия), регистрации проектов и программ технической помощи (содействия) и контроль, их выполнения, а также выдачи соответствующих документов, подтверждающих их принадлежность к указанной помощи;

− межведомственное взаимодействие с ФТС в технологической среде СМЭВ 3.

1. Структура Системы и назначение ее частей

В состав Системы входят следующие подсистемы:

- Подсистема аутентификации и авторизации;
- Подсистема «Информационная поддержка заявителей»;
- Подсистема «Оформление удостоверений»;

- Подсистема «Администрирование»;
- Подсистема «Информационная безопасность»;
- Подсистема «Межведомственное взаимодействие»;
- Подсистема «Нормативно-справочная информация»;
- Подсистема хранения данных.

Подсистема аутентификации и авторизации обеспечивает проверку подлинности пользователя и предоставление доступа к данным и функциям Системы в соответствии с выданными пользователю полномочиями. Определение полномочий выполняется путем назначения пользователю роли (ролей) в соответствии с реализованной в системе ролевой моделью.

Подсистема «Информационная поддержка заявителей» предназначена для реализации процедур подачи заинтересованными физическими и юридическими лицами заявлений на регистрацию проектов или программ технической помощи (содействия) и выдачу удостоверения, подтверждающего принадлежность средств, товаров, работ и услуг к технической помощи (содействию). Подсистема предоставляет заявителям возможности подачи заявлений путем заполнения соответствующих форм в их личных кабинетах, и получения информации о ходе и результатах рассмотрения заявлений.

Подсистема «Оформление удостоверений» предназначена для централизованной обработки заявлений получателей технической помощи (содействия) и выдачи получателям технической помощи Удостоверения в электронном виде. Подсистема автоматизирует процессы обработки заявлений «Выдача удостоверения, подтверждающего принадлежность средств, товаров, работ и услуг к технической помощи (содействию)» и «Внесение изменений в удостоверение, подтверждающего принадлежность средств, товаров, работ и услуг к технической помощи (содействию).

Подсистема «Администрирование» предназначена для управления структурой и содержимым Системы, выполнения настроек Системы, а также управления пользователями и ролевой моделью.

Подсистема «Информационная безопасность» обеспечивает информационную безопасность Системы в части обеспечения соответствия требованиям по обеспечению целостности, устойчивости функционирования и безопасности Системы, а также по классификации и защите информации, в части ее касающейся, в соответствии требованиями приказов Минкомсвязи России от 25 августа 2009г. № 104, ФСБ России и ФСТЭК от 31 августа 2010 г. № 416/489, приказа ФСТЭК №17 от 11 февраля 2013 г., а также других нормативных правовых актов.

Подсистема «Межведомственное взаимодействие» предназначена для предоставления электронных копий выданных Удостоверений из АИС в информационную систему ФТС России для осуществления его государственной функции по контролю за соблюдением условий предоставления льгот по уплате таможенных платежей посредством СМЭВ.

Подсистема «Нормативно-справочная информация» предназначена для управления справочниками и классификаторами, используемыми в системе.

Подсистема хранения данных предназначена для хранения, модификации и обработки взаимосвязанной информации Системы.

1.1 Сведения об АИС в целом и ее частях, необходимых для обеспечения эксплуатации Системы

Система обеспечивает функционирование в следующих режимах:

- штатный режим (режим, обеспечивающий выполнение функций Портала в полном объеме);
- сервисный режим (режим для проведения реконфигурирования, обновления и профилактического обслуживания);
- аварийный режим.

Основным режимом функционирования Системы является штатный режим, при котором:

- программное обеспечение Системы обеспечивает возможность круглосуточного функционирования с регламентированными перерывами на техническое обслуживание и обновление программного обеспечения.

В штатном режиме функционирования Портал обеспечивает:

- работу пользователей в режиме – 24 часа в день, 7 дней в неделю;
- коэффициент готовности не ниже 0,99;
- выполнение всех функций в полном объеме.

Для обеспечения штатного режима функционирования Системы необходимо соблюдать требования и выдерживать условия эксплуатации программного обеспечения, указанные в технической документации в составе: руководства пользователя и руководство администратора Системы.

Сервисный режим функционирования используется для выполнения операций подготовки и проведения испытаний или настройки Системы. В данном режиме Система или его подсистемы становятся недоступными для групп пользователей. В данном режиме осуществляется:

- проведение на сервере Системы регламентных и других работ;
- модернизация аппаратно-программного комплекса Системы;
- модернизация Системы или отдельных подсистем.

В сервисном режиме Система обеспечивает работоспособность подсистемы хранения данных и предоставляет инструментарий администрирования.

При включении сервисного режима, на время проведения сервисных работ, пользователям демонстрируется страница-заставка с предупреждением о проведении работ. На странице присутствует только статический текст.

Аварийный режим функционирования Системы характеризуется отказом в работе Системы. Переход Системы в аварийный режим происходит по причине нарушения работоспособности Системы или одной из подсистем.

1.2 Описание функционирования Системы и ее частей

Перечень функций, реализуемых Системой, приведен в разделах 3.3-3.7, посвященных описанию компонентов и подсистем АИС «Регистрация заявлений получателей техпомощи».

2 ОПИСАНИЕ ВЗАИМОСВЯЗЕЙ АИС С ДРУГИМИ СИСТЕМАМИ

2.1 Перечень систем, с которыми связана данная АИС

АИС взаимодействует со следующими информационными системами:

- Система межведомственного взаимодействия (СМЭВ).
- Единая система идентификации и авторизации (ЕСИА).

2.2 Описание связей между системами

Взаимодействие Системы со СМЭВ осуществляется с использованием электронных сервисов, реализованных в виде веб-сервисов. Для передачи электронных сообщений используется протокол SOAP поверх HTTP.

Взаимодействие Системы с ЕСИА реализовано для выполнения процедур идентификации пользователей и осуществляется посредством электронных сообщений, основанных на стандарте OpenID Connect 1.0, получая на вход запрос на идентификацию и отдавая на выход личные данные пользователя и сведения о его привязки к юридическому лицу.

2.3 Описание регламента связей

Межведомственное взаимодействие АИС с ФТС России осуществляется в технологической среде СМЭВ 3 с использованием электронного сервиса Минэкономразвития России, который предоставляет электронные копии выданных Удостоверений из АИС в информационную систему ФТС России для осуществления соблюдений условий предоставления льгот по уплате таможенных платежей. Электронный сервис осуществляет:

- передачу в ФТС удостоверений, которые ранее не были переданы,
- передача в ФТС удостоверения по запрошенному номеру.

При осуществлении сценария идентификации пользователя АИС направляет пользователя в ЕСИА на страницу аутентификации. После успешного прохождения аутентификации ЕСИА возвращает пользователя в АИС вместе с идентификационными данными пользователя (состав возвращаемых данных содержит личные данные пользователя и сведения о его привязки к юридическому лицу).

3 ОПИСАНИЕ ПОДСИСТЕМ АИС

3.1 Структура подсистем

Подсистема аутентификации и авторизации не имеет структуры.

Подсистема «Информационная поддержка заявителей» не имеет структуры.

Подсистема «Оформление удостоверений» не имеет структуры.

Подсистема «Администрирование» не имеет структуры.

Подсистема «Информационная безопасность» не имеет структуры.

Подсистема «Межведомственное взаимодействие» состоит из следующих частей:

- Модуль электронного сервиса
- Модуль электронной подписи.

Подсистема «Нормативно-справочная информация» не имеет структуры.

Подсистема хранения данных не имеет структуры.

3.2 Сведения об аппаратно-программной платформе

Для корректного функционирования подсистем и их частей необходима установка Системы в полной комплектации на сервер.

Сервер, на котором установлено и функционирует программное обеспечение Системы:

- ОС Microsoft Windows Server Standard 2008 или выше;
- СУБД PostgreSQL 9.6;
- Процессор: 16 ядер, 2.5 ГГц или больше;
- Оперативная память: 32 Гб;
- Дисковое пространство
- Системный диск: 250 Гб;
- Диск для хранения данных и БД: 500 Гб;
- Пропускная способность сетевого интерфейса 100 Мбит/с.

Сервер, на котором установлено и функционирует программное обеспечение, осуществляющее межведомственное взаимодействие через СМЭВ:

- ОС Ubuntu v.10.4;
- СУБД Postgresql v.8.4, MongoDB 2.6.0 Community;
- Процессор: 4 ядра, 2.5 ГГц или больше;
- Оперативная память: 8 Гб;
- Дисковое пространство: 500 Гб;
- Пропускная способность сетевого интерфейса 100 Мбит/с.

Система рассчитана на работу с одним из следующих браузеров:

- Mozilla Firefox v.68.0 и выше;
- Google Chrome v.75.0 и выше;
- Yandex browser v.17.1 и выше;
- Safari 10.1.2 и выше (MacOS), 5.1.7 (Windows).

3.3 Описание функционирования подсистем и их частей

3.3.1 Описание функционирования подсистемы аутентификации и авторизации

Подсистема аутентификации и авторизации в соответствие со своим назначением выполняет следующие функции:

- Блок управления ролевой моделью:
  - Настройка прав и полномочий для ролей пользователей;

- Предоставление пользователям прав на доступ к информации и функциям системы путем назначения пользователям соответствующей роли.

- Блок регистрации пользователя:
  - Предоставление пользователю-заявителю возможности заполнить форму регистрации на сайте,
  - Проверка правильности заполнения формы регистрации,
  - Сохранение указанных пользователем учетных данных,
  - Предоставление данных, указанных пользователем при регистрации, для проверки администратору.
- Блок аутентификации и авторизации пользователя:
  - Проверка действительности введенных логина и пароля,
  - Выполнение процедур авторизации пользователя через ЕСИА,
  - Проверка прав пользователя и предоставление пользователю доступа к разделам и функциям системы в соответствии с назначенной ему ролью.
- Блок восстановления пароля пользователя:
  - Проверка данных пользователя, указанных в форме восстановления пароля,
  - Сброс пароля пользователя,
  - Отправка пользователю уведомления с ссылкой для восстановления пароля,
  - Предоставление пользователю возможности задать новый пароль,
  - Регистрация нового пароля пользователя.

3.3.2 Описание функционирования подсистемы «Информационная поддержка заявителей»

Подсистема «Информационная поддержка заявителей» в соответствие со своим назначением выполняет следующие действия:

- Блок информирования пользователей:
  - Публикация информации о заявлениях;
  - Публикация вопросов и ответов о работе Комиссии,
  - Предоставление пользователям нормативно-правовых документов в электронном виде,
  - Предоставление пользователям образцов документов,
  - Публикация новостной и контактной информации.
- Блок Личный кабинет пользователя:
  - Предоставление пользователю возможности просмотра своих данных указанных при регистрации (или полученных при авторизации через ЕСИА),
  - Предоставление пользователю возможности редактирования своих данных,
  - Предоставление списка поданных и рассмотренных заявлений и данных в этих заявлениях,
  - Предоставление пользователю возможности отслеживания хода исполнения поданных заявлений.
- Блок подачи заявления в электронном виде:
  - Предоставление пользователю возможности подачи заявления в электронном виде путем заполнения соответствующей формы,
  - Предоставление возможности сохранения черновика заявления в ходе заполнения формы заявления,
  - Формирование печатной формы заявления и приложений.

3.3.3 Описание функционирования подсистемы «Оформление удостоверений»

Подсистема «Оформление удостоверений» в соответствие со своим назначением выполняет следующие действия:

- Блок «Работа с заявлениями»:
  - Отображение реестра поданных заявлений и возможность поиска, фильтрации и сортировки в нём,
  - Просмотр данных заявления (включая открытие прикрепленных файлов),
  - Редактирование данных заявления,
  - Формирование печатной формы заявления и приложений,
  - Возврат заявления на доработку заявителю,
  - Возврат заявления с любого этапа (за исключением конечного) на этап проведения экспертизы,
  - Предоставление эксперту возможности смены статуса заявления и перевода его с этапа на этап с указанием принятого решения,
  - Формирование печатных форм таблиц для рассмотрения на заседаниях рабочей группы и Комиссии,
  - Формирование печатных форм протоколов заседаний Рабочей группы и Комиссии.
- Блок «Архив»:
  - Отображение реестра исполненных заявлений и возможность поиска, фильтрации и сортировки в нём,
  - Просмотр данных заявления,
  - Отображение реестра протоколов заседаний Комиссии и возможность поиска, фильтрации и сортировки в нем,
  - Добавление в реестр новой записи о протоколе,
  - Просмотр и редактирование данных протокола,
  - Удаление записи из реестра протоколов заседаний Комиссии,
  - Отображение Единого реестра проектов и программ технической помощи (содействия),
  - Добавление в реестр записи о новом зарегистрированном проекте/программе,
  - Просмотр и редактирование данных проекта/программы,
  - Удаление записи из Единого реестра проектов/программ,
  - Отображение реестра Удостоверений и возможность поиска, фильтрации и сортировки в нем,
  - Добавление в реестр новой записи о выданном удостоверении,
  - Просмотр и редактирование данных удостоверения.
  - Удаление записи из реестра удостоверений.
- Блок «Уведомление пользователей»:
  - Отправка уведомлений о регистрации пользователя на e-mail пользователя и администратора,
  - Отправка уведомления на e-mail пользователя при активации его учетной записи,
  - Отправка уведомлений на e-mail заявителя и эксперта о создании нового заявления,
  - Отправка уведомлений заявителю о смене статуса заявления.

3.3.4 Описание функционирования подсистемы «Администрирование»

Подсистема «Администрирование» в соответствие со своим назначением выполняет следующие действия:

- Блок управления учетными записями пользователей:
  - Ведение реестра учетных записей пользователей (заявителей и сотрудников Минэкономразвития РФ),
  - Просмотр данных пользователя, указанных при регистрации пользователя в Системе,
  - Добавление и редактирование учетной записи пользователя,
  - Активация учетной записи пользователя,
  - Блокировка учетной записи пользователя,
  - Изменение прав пользователя,
  - Удаление учетной записи пользователя.
- Блок управления данными печатных форм документов:
  - Задание констант для печатных форм заявлений и удостоверений (фамилий, контактных данных, пр.),
  - Загрузка шаблонов печатных форм документов
  - Функции блока «Реестр вопросов и ответов»:
  - Предоставление администратору системы возможности создания вопросов и ответов на них,
  - Управление реестром вопросов и ответов: редактирование, удаление, публикация и снятие с публикации.
- Блок «События»:
  - Создание и редактирование события (заголовок, описание, дата)
  - Управлять публикацией событий в общедоступном разделе Системы.
  - Удаление события.
- Блок «Отчеты»:
  - Формирование отчета по зарегистрированным за год проектам/программам,
  - Формирование отчета по выданным за год удостоверениям.

3.3.5 Описание функционирования подсистемы «Информационная безопасность»

Подсистема «Информационная безопасность» в соответствие со своим назначением выполняет следующие действия:

- Обеспечение целостности, конфиденциальности, доступности информации,
- Реализация мер защиты от несанкционированного доступа к информации Системы,
- Организация защищенного (шифрованного) соединения между пользователем и сайтом при подключении к Системе через Интернет (протокол https).

3.3.6 Описание функционирования подсистемы «Межведомственное взаимодействие»

Подсистема «Межведомственное взаимодействие» в соответствие со своим назначением выполняет следующие действия:

- Передача в ФТС удостоверений, которые ранее не были переданы,
- Передача в ФТС удостоверения по запрошенному номеру.

3.3.6.1 Описание функционирования модуля

Модуль электронного сервиса обеспечивает передачу в ФТС удостоверений, которые еще не переданы, и сведений об определенном запрошенном удостоверении.

3.3.6.2 Описание функционирования модуля электронной подписи

Модуль обеспечивает конфиденциальность, контроль целостности и придания юридической значимости электронных копий выданных удостоверений при межведомственном взаимодействии.

3.3.7 Описание функционирования подсистемы «Нормативно-справочная информация»

Подсистема «Нормативно-справочная информация» в соответствие со своим назначением выполняет следующие действия:

- Добавление и редактирование записей справочников и классификаторов системы,
- Управление публикацией записей справочников и классификаторов,
- Удаление записей справочников и классификаторов.

3.3.8 Описание функционирования подсистемы хранения данных

Подсистема хранения данных в соответствие со своим назначением выполняет следующие действия:

- Ведение системного каталога (словаря данных);
- Поддержка независимости от данных;
- Выполнение логического контроля при внесении данных;
- Контроль целостности (корректность и непротиворечивость) данных;
- Простота обновления данных;
- Контроль избыточности данных и возможности снижения избыточности;
- Защита данных от разрушения в результате аварийных ситуаций, возможность создания резервных копий базы данных и восстановления базы данных из резервной копии;
- Обеспечение коллективного доступа к данным (возможность одновременного доступа к одним и тем же данным нескольких пользователей);
- Поддержка параллельной работы (корректное обновление базы данных при параллельном выполнении операций обновления многими пользователями);
- Контроль доступа к данным и защита от несанкционированного доступа к данным;
- Быстрый поиск информации по запросам пользователей.

3.4 Личный кабинет заявителя

Пользователь, зарегистрированный в системе как заявитель (или авторизованный через ЕСИА как представитель организации), имеет возможность сформировать и подать на рассмотрение следующие заявления:

- Заявление на регистрацию проекта/программы и выдачу удостоверения.
- Заявление на регистрацию проекта/программы.
- Заявление на внесение изменений в проект /программу.
- Заявление на выдачу удостоверения.
- Заявление на внесение изменений в удостоверение.

Заявление подается в электронном виде путем заполнения соответствующей формы в системе и прикрепления к нему необходимых файлов документов.

В процессе заполнения формы заявления пользователь может сохранять промежуточные результаты в виде черновика. Заполненное заявление отправляется на рассмотрение в Минэкономразвития РФ.

Для заявления и приложений формируется печатная форма с возможностью предпросмотра и сохранения в файл.

У заявителя в личном кабинете есть возможность:

- Редактировать данные о себе, менять пароль.
- Просматривать поданные заявления и следить за ходом их рассмотрения.
- Присматривать рассмотренные заявления.
- Сохранять черновики заявлений и возобновлять работу с ними.
- Корректировать возвращенные на доработку заявления.

3.5 Личный кабинет эксперта

Пользователь с ролью Эксперт в своем личном кабинете имеет возможность:

- Редактировать свои личные данные, сменить пароль
- Выполнять операции, связанные с рассмотрением заявлений:
  - Просматривать данные поступивших на рассмотрение заявлений.
  - Формировать печатные формы заявлений и приложений к ним.
  - Вносить изменения в заявления в ходе их рассмотрения, а также возвращать на доработку заявителям.
  - Изменять статус заявления и фиксировать решения после каждого этапа рассмотрения заявления: экспертом, на заседании рабочей группы Комиссии и заседании Комиссии.
  - Формировать печатные формы таблиц со списком заявлений для заседаний и печатные формы протоколов заседаний рабочей группы и Комиссии.
- Вести реестр проектов/программ (просматривать, редактировать, добавлять, удалять).
- Вести реестр удостоверений (просматривать, редактировать, добавлять, удалять, формировать печатные формы с возможностью сохранения в файл).
- Вести реестр протоколов (просматривать, редактировать, добавлять, удалять).
- Просматривать реестр рассмотренных заявлений.
- Управлять справочниками (просматривать, добавлять и редактировать позиции справочников раздела нормативно-справочной информации).

Кроме того, у эксперта есть возможность выполнения групповых действий: отметить в реестре заявлений нужные заявления и изменить их статус, щелкнув соответствующую кнопку.

В части управления данными печатных форм документов эксперт имеет возможность в соответствующем разделе личного кабинета задать статическую информацию, используемую в шаблонах печатных форм (адрес, контакты, ФИО и должность подписанта, пр.).

В части управления информацией Системы эксперт имеет возможность изменять и дополнять информацию, размещённую в общедоступных разделах Системы: текстовую, новостную, нормативно-справочную, контактную, вопрос-ответ.

3.6 Личный кабинет Наблюдателя Комиссии

Пользователь с ролью Наблюдатель Комиссии в своем личном кабинете тоже может изменить информацию о себе и сменить пароль. Кроме того, ему доступен реестр рассмотренных заявлений и рассматриваемых заявлений, пользователь может просматривать карточки заявлений и контролировать ход их рассмотрения.

3.7 Личный кабинет администратора Системы

Помимо редактирования своих данных и смены пароля, пользователь с ролью «Администратор системы» может:

- Просматривать статистические отчеты по заявлениям и удостоверениям.

- Проверять данные зарегистрировавшихся в Системе пользователей и подтверждать или отклонять регистрацию. Кроме того, Администратор может создавать учетные записи пользователей, назначать им права, блокировать доступ в Систему при необходимости.
- Управлять ролевой моделью: составом ролей и правами на разделы и функции Системы для каждой роли.
- Выполнять различные настройки Системы.
- Управлять структурой системы и меню.
- Просматривать журнал логов.

Приложение 2

Предложение по цене _____

№ п/п	Наименование работ	Результаты работ	Цена (тыс. руб.)
1.	*по пунктам указанных в требованиях*	*Возможны предложения по уточнению сроков выполнения этапов работ*	
2.			

Общая цена контракта: _____

Расчет общей цены контракта:

№ п/п и наименование работы	Привлекаемые специалисты	Кол-во человеко-дней	Средняя оплата труда за 1 день (руб.)/ Общая оплата труда (руб.)	Наименование статей расходов	Ставка	Цена, руб.
по работам				ФОТ		
				Материалы	-	
				Страховые взносы		
				Накладные расходы (от ФОТ)		
				Себестоимость		
				Прибыль (от себестоимости)		
				Стоимость		
				НДС		
				Стоимость с НДС		

Срок действия предлагаемой цены: _____

Руководитель организации:

_____ _____

(подпись) М.П. (расшифровка подписи)

ПАО «Ростелеком»

УТВЕРЖДЕНО

_____

Технические условия по размещению информационных систем федеральных органов исполнительной власти в объединённом центре обработки данных Правительственного комплекса

АГРВ.466459.301-01ТУ

Согласовано:

Разработано:

Москва, 2020

Подп. и дата

Инв. № дубл.

Взам. инв. №

Подп. и дата

Инв. № подл.

Содержание

1 Общие сведения

Настоящие технические условия определяют техническую возможность размещения информационных систем (далее – ИС) федеральных органов исполнительной власти (далее – ФОИВ) в инфраструктуре Правительственного комплекса (далее – ПК).

При подготовке данных технических условий использовались следующие нормативные документы:

- Раздел «Общие критерии» ГОСТ Р ИСО/МЭК 15408 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий) часть 2 «Функциональные требования безопасности».
- Приказ ФСТЭК России от 11.02.2013 N 17 (ред. от 28.05.2019) "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".
- Методический документ Меры защиты информации в Государственных информационных системах. Утвержден ФСТЭК России 11 февраля 2014 г.
- Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
- Приказ Минкомсвязи от 26.11.2019 № 763 «Об утверждении требований, необходимых для проведения эксперимента по переводу информационных систем и информационных ресурсов федеральных органах исполнительной власти и государственных внебюджетных фондов в государственную единую облачную платформу, а также по обеспечению федеральных органов исполнительной власти и

государственных внебюджетных фондов автоматизированными рабочими местами и программным обеспечением».

- Модель угроз и нарушителя безопасности информации объединенного центра обработки данных ИТ-инфраструктуры Единого правительственного комплекса.

1.1 Участвующие стороны и зоны ответственности

Заказчик – Федеральное казенное учреждение «Центр поддержки».

Функциональный Заказчик – ФОИВ, размещающий свои ИС в ОЦОД ПК ПАО «Ростелеком».

Исполнитель - ПАО «Ростелеком», организация которая оказывает услугу по предоставлению ресурсов ЦОД и прочих услуг в ОЦОД ПК.

С учетом требований, указанных в настоящем документе, Функциональный Заказчик принимает решение о составе оборудования и ИС, подлежащих размещению в ОЦОД ПК.

Заказчик обеспечивает заказ и приемку выполнения Исполнителем работ, предоставления информационно-технологических сервисов, в том числе по информационной безопасности для целей обеспечения деятельности федеральных органов исполнительной власти и организаций, расположенных в здании Правительственного комплекса по адресу г. Москва, Пресненская наб., д. 10, строение 2 (Башня 2).

Функциональный заказчик дает рекомендации по составу переносимого оборудования и ИС, с учетом требований настоящего документа. Исполнитель проводит работы по переносу такого оборудования и размещению ИС с учетом требований настоящего документа.

Исполнитель обеспечивает ресурсы ОЦОД, осуществляет прием и постановку на учет оборудования, реализует организационно-режимные меры по физической безопасности и обеспечивает сервисное сопровождение серверной инфраструктуры в сегменте «Colocation» в соответствии с положениями и условиями настоящего документа.

2 Общее описание объединенного ЦОД ПК

Объединенный ЦОД Правительственного комплекса (далее – ОЦОД) расположен в дата-центре «Москва II» ПАО «Ростелеком», по адресу пл. Академика Курчатова, д.1, стр.119.

В ОЦОД для размещения оборудования и компонентов ИС ФОИВ предусмотрены следующие физически независимые разделённые контуры:

- Открытый контур (далее – ОК) – предназначен для размещения оборудования и компонентов ИС ФОИВ, к которым предоставляется доступ из сети Интернет. В ОК предусмотрена возможность размещения оборудования и компонентов ИС ФОИВ как в формате услуги «Colocation» (размещение аппаратных компонентов Заказчика в монтажных конструктивах и помещениях Исполнителя), так и в формате услуги «Облако» (размещение виртуальных компонентов ИС Заказчика в среде виртуализации Исполнителя). В Облаке ОК не может храниться, обрабатываться в открытом виде служебная, конфиденциальная информация ФОИВ, а также информация, которую можно отнести к персональным данным.
- Закрытый контур (далее – ЗК) – предназначен для размещения компонентов ИС ФОИВ, не взаимодействующих непосредственно с сетью Интернет. В ЗК предусмотрена возможность размещения компонентов ИС ФОИВ только в формате услуги «Облако». Таким образом, в ЗК Правительственного комплекса возможно размещение только виртуальных компонентов ИС ФОИВ[1].
- Контур подключения к сети Интернет – реализует возможности подключения к сетям связи общего пользования.

[1] При необходимости размещения физического оборудования в ЗК решение должно быть проработано отдельно и включать стадию проектирования.

- Шлюзовой контур – представляет собой изолированный сетевой сегмент с развернутыми СЗИ, предназначенный для контролируемого обмена данными между ОК и ЗК.
- Сегмент «Colocation» – представляет собой совокупность логически раздельных на уровне L2 сетевых сегментов, отделенных от других сетей межсетевым экраном Исполнителя.

ОЦОД имеет аттестат соответствия ФСТЭК по требованиям безопасности информации для государственных информационных систем (К1), информационных систем персональных данных (УЗ1) и информационных систем общего пользования (II класса).

Структурная схема и целевая схема покрытия ОЦОД сервисами ИБ, после завершения миграции, представлены в Приложении А.

2.1 Описание сегмента «Colocation»

Сегмент «Colocation» физически представляет собой выделенную часть инфраструктуры ОЦОД, оборудованную необходимыми инженерными системами, монтажными конструктивами, СКС и коммутационным/маршрутизирующим сетевым оборудованием, предназначенную для размещения оборудования Функционального заказчика. Логически, сегмент «Colocation» представляет собой изолированный сертифицированными ФСТЭК средствами межсетевого экранирования сетевой сегмент, с возможностями сетевой связности с сетями общего пользования, Облаком в ОЦОД и ресурсами Правительственного комплекса.

2.2 Описание Облака Правительственного комплекса

Облачная инфраструктура (далее – Облако) для размещения ИС ФОИВ представляет собой программно-аппаратный комплекс, в который входят вычислительные ресурсы и ресурсы хранения данных, управляемые с помощью средств виртуализации VMware актуальной версии (на текущий момент, актуальная версия компонентов среды виртуализации – 6.7).

2.3 Описание архитектуры Облака Правительственного комплекса

Облако размещается на виртуальных серверных ресурсах ЗК и ОК ОЦОД.

Предполагается, что ИС ФОИВ, размещаемые в Облаке, имеют модульную (минимум один модуль) архитектуру, в которой модули этой ИС осуществляют информационное взаимодействие через IP-сеть.

Для каждой ИС в каждом контуре выделяется IP-сеть в соответствии с IP-адресацией, определенной в Облаке. Сегментация сети в Облаке и размещение в сегментах модулей (серверов) ИС ФОИВ описано в подразделе 2.4. Сетевые взаимодействия между разными IP-сетями по умолчанию не разрешены.

Для модулей ИС ФОИВ, размещаемых в ЗК Облака, могут быть разрешены следующие сетевые взаимодействия[2]:

- с АРМ пользователей/администраторов ИС, расположенных в ЗК ФОИВ в Башне;
- с удалёнными АРМ администраторов, при условии использования ГОСТ VPN и системы контроля действий привилегированных пользователей (далее – РАМ);
- с модулями других ИС (ведомственных/ФОИВ/инфраструктурных), расположенных в ЗК;
- с другими модулями этой же ИС, расположенными в ЗК и ОК[3];
- с технологическими серверами ИТ и ИБ систем в ЗК, на базе которых предоставляются Исполнителем сервисы и услуги в рамках Государственного контракта.

Для модулей ИС ФОИВ, размещаемых в ОК Облака, могут быть разрешены следующие сетевые взаимодействия[4]:

[2] Другие сетевые взаимодействия должны быть рассмотрены отдельно, в рамках заявок на доступ

[3] Взаимодействие между модулями в ЗК и ОК происходит через защищенное сертифицированными средствами соединение, при этом использование протоколов администрирования ОС серверов не допускается.

[4] Другие сетевые взаимодействия должны быть рассмотрены отдельно, в рамках заявок на доступ

- с удаленными АРМ[5] пользователей/администраторов ИС, при условии использования VPN или ГОСТ VPN[6];
- с АРМ пользователей/администраторов ИС, расположенных в ОК ФОИВ в Башне;
- с АРМ пользователей сетей передачи данных общего пользования (для публичных информационных ресурсов);
- с другими удаленными ИС;
- с модулями других ИС (ведомственных/ФОИВ/инфраструктурных), расположенных в ОК;
- с серверами ИТ и ИБ систем, предоставляемых Исполнителем в ОК сервисов в рамках Государственного контракта.
- с другими модулями этой же ИС, расположенными в ЗК[7] и в ОК;
- с ресурсами в сети Интернет в соответствии с условиями и ограничениями на доступ, описанных в разделе 2.4.

Предполагается, что ИС ФОИВ, размещаемые в Облаке, имеют модульную (минимум один модуль) архитектуру, в которой модули этой ИС осуществляют информационное взаимодействие через IP-сеть.

Для обеспечения жизненного цикла ИС, имеющих собственный цикл разработки, в Облаке организуется несколько логических зон, предназначенных для размещения функциональных модулей ИС:

- Зона разработки и тестирования ИС (TST)
- Предпродуктивная зона ИС (PPD)
- Продуктивная зона ИС (PRD)
- Подготовительная зона ИС (PREP).

[5] АРМ и/или ИС считаются удаленными, если каналы связи, по которым осуществляется взаимодействие, выходят за пределы контролируемой зоны и не расположены в ПК. Взаимодействие удаленных АРМ и ИС с ресурсами/оборудованием ЦОД ПК осуществляется только посредством VPN.

[6] Необходимость использования криптографических алгоритмов ГОСТ определяется требованиями регулятора и функциональным назначением ресурса.

[7] Взаимодействие между модулями в ЗК и ОК происходит через защищенное сертифицированными средствами соединение протоколов администрирования ОС серверов не допускается.

2.3.1 Зона разработки и тестирования ИС

- располагается Облаке ОК Правительственного комплекса;
- предназначена для разработки ПО ИС и не содержит данных, подлежащих защите; (обеспечение целостности ПО и отсутствие НДВ является зоной ответственности ФОИВ и его подрядчиков);
- предназначена для тестирования работоспособности обновлений/ПО ИС в Облаке с общесистемным ПО определенной версионности и наложенными средствами ИБ;
- не содержит данных подлежащих защите, т.е. используются только обезличенные или тестовые данные;
- располагается в Облаке ОК Правительственного комплекса;
- доступна для разработчиков, тестировщиков, администраторов ИС;
- безопасность удаленного доступа в зону обеспечивается на безе технологий ГОСТ VPN.

2.3.2 Предпродуктивная зона ИС

- предназначена для тестирования ПО в условиях и на данных, максимально приближенных к продуктивным. По сути, является технологической копией продуктивной ИС;
- содержит данные, подлежащие защите, согласно результатам категорирования ИС, т.к. используется копия продуктивных данных;
- может быть расположена в Облаке ОК и ЗК Правительственного комплекса (определяется архитектурой ИС);
- доступна для разработчиков, тестировщиков, администраторов ИС по согласованию с Функциональным Заказчиком (владельцем системы).

2.3.3 Продуктивная зона ИС

- предназначена для работы пользователей с ИС ФОИВ;

- содержит данные, подлежащие защите, согласно результатам категорирования ИС;
- располагается в Облаке ОК и ЗК ПК (определяется архитектурой ИС);
- доступна для администраторов и пользователей ИС;
- запрещается размещение программных средств разработки.

2.3.4 Подготовительная зона ИС

- предназначена для размещения ИС в процессе подготовки и проведения миграции ИС в ОЦОД в соответствии с ТУ размещения ИС в Облаке Правительственного комплекса;
    - по сути, Подготовительная зона является зоной «Colocation» на вычислительных ресурсах Облака ОЦОД:
- содержит данные, подлежащие защите, согласно результатам категорирования ИС, т.к. используются продуктивные данные;
- может быть расположена в Облаке ОК и ЗК (определяется архитектурой ИС);
    - компоненты ИС, содержащие данные, подлежащие защите, и/или к которым осуществляется доступ пользователей с АРМ ЗК должны быть размещены в Облаке ЗК;
    - фронтальные компоненты ИС, предназначенные для информационного обмена с сетью Интернет, должны быть размещены в Облаке ОК (для программных компонентов) или в зоне Colocation (для отдельных физических компонентов);
- ресурсы ИС, размещенные в PREP, доступны в режимах опытной и опытно промышленной эксплуатации;
- ИС, размещенная в зоне PREP не может быть аттестована;
- ресурсы ИС, размещаемой в данной зоне, по согласованию с Функциональным Заказчиком (владельцем системы), доступны для пользователей, разработчиков, тестировщиков, администраторов ИС.

2.4 Обеспечение ИБ в ОЦОД Правительственного комплекса

Удаленный защищенный доступ к ЦОД: сегменту «Colocation», виртуальным средам ЗК и ОК Облака ЦОД – реализуется на базе сертифицированных СКЗИ класса КС3. Криптографическая защита информационного обмена обеспечивается построением VPN на уровне протоколов SSL\TLS, так и на IP-уровне. При этом в качестве базовых в ЦОД используются решения фирмы Инфотекс «VipNet», для доступа администраторов ИС/ГИС/Системного ПО, а также КроптоПРО «nGate», для доступа пользователей ИС/ГИС. Для получения VPN доступа ФОИВам необходимо самостоятельно приобрести VipNet-клиентов и/или сертификат для nGate-клиента.

Доступ удалённых администраторов и удалённых пользователей к ресурсам ОЦОД (помимо VPN-соединения) осуществляется через терминальный сервер.

Между контурами и зонами возможен файловый обмен только через Фонд программной документации (ФПД). Более подробно ФПД описан в разделе 2.4.3.

Протоколы удалённого управления разрешены только в направлении из ЗК в ОК.

Организация сетевого взаимодействия через МСЭ в ЦОД ПК осуществляется после подачи заявки на сетевой доступ.

2.4.1 Требования информационной безопасности, выполняемые ФОИВ, при размещении оборудования и миграции ИС в сегменте «Colocation»

Выполнение данных требований необходимо для обеспечения ИБ в сегменте «Colocation», а также для возможности проведения аттестации ИС ФОИВ, являющихся ГИС и/или ИСПДн, на соответствие требованиям по защите информации.

Все ПО, обеспечивающее ИБ на оборудовании, должно быть лицензировано и иметь действующие сертификаты ФСТЭК России (в том числе, в

случае наличия сертификатов ФСТЭК России на прикладное ПО), а лицензии должны быть сроком не менее 3 месяцев с момента размещения оборудования в сегменте «Colocation».

Количество лицензий на ПО в части ИБ должно быть не меньше актуального количества перевозимого оборудования, ОС или пользователей (в зависимости от типа применимости). В случае недостаточности Функциональный Заказчик должен осуществить дополнительную поставку необходимого количества действующих лицензий.

ОС серверов и гипервизоры в сегменте «Colocation» должны соответствовать актуальным, на момент миграции, требованиям совместимости производителей СЗИ, применяемых в инфраструктуре ОЦОД ПК: «Лаборатория Касперского», «Код Безопасности». В случае несоответствия указанным требованиям, Функциональному Заказчику рекомендуется произвести обновление (замену) ОС и гипервизора до актуальных версий.

В случае невозможности обновления ОС и гипервизоров до актуальных версий, поддерживаемых сертифицированными СЗИ, или в случае отсутствия поддержки ОС и гипервизоров в технической документации производителей СЗИ, такие ОС/гипервизоры не могут быть подключены к контуру безопасности ИТ-инфраструктуры Правительственного комплекса, и на них не могут оказываться услуги и сервисы информационной безопасности ОЦОД ПК. Такие технические средства размещаются в сегменте «Colocation» без подключения каких-либо услуг и сервисов ИБ ОЦОД ПК. Обеспечение информационной безопасности таких технических средств находится в зоне ответственности Функционального заказчика и выполняется текущими СЗИ ФОИВ, которые также перемещаются в сегмент «Colocation» ОЦОД ПК.

На оборудовании Функционального Заказчика должно быть установлено антивирусное ПО (АВПО). Лицензии на АВПО могут быть предоставлены Исполнителем. Возможно применение лицензий АВПО «Лаборатории Касперского», имеющихся у Функционального Заказчика.

В случае применения виртуализации на оборудовании Функционального Заказчика рекомендуется установить АВПО для виртуальных сред и сертифицированное средство защиты среды виртуализации. Возможно применение ранее установленного АВПО для виртуальных сред и сертифицированного средства защиты среды виртуализации Функционального Заказчика. При необходимости аттестации ИС/ГИС, размещающейся на виртуальной среде «Colocation» требуется установка сертифицированного средства защиты среды виртуализации.

В случае наличия, применяются установленные в серверы на момент перевозки аппаратно-программные модули доверенной загрузки, обладающие действующими сертификатами ФСТЭК России (в случае отсутствия действующих сертификатов модули не подлежат миграции).

До и/или после осуществления миграции ИС в сегменте «Colocation» Исполнитель проводит анализ защищенности (инструментальное сканирование), а Функциональный заказчик должен устранить выявленные уязвимости. После устранения проводится повторный анализ защищенности (инструментальное сканирование) и устранение уязвимостей.

2.4.2 Описание СЗИ и требований по обеспечению ИБ в сегменте «Colocation»

Обеспечение информационной безопасности внутри сегмента «Colocation» находится зоне ответственности Функционального Заказчика. Вместе с тем Исполнитель, разместивший физическое оборудование Функционального Заказчика в ОЦОД, накладывает ограничения на информационный обмен сегмента «Colocation», который может негативно повлиять на информационные ресурсы ОЦОД и сегментов «Colocation» иных Функциональных Заказчиков, а также АРМ ФОИВ, размещенные в Правительственном комплексе.

Исполнитель обеспечивает контроль информационного обмена сегмента «Colocation» посредством применения сертифицированных межсетевых экранов, а также сертифицированных средств обнаружения вторжений.

Политика межсетевого экранирования обеспечивает возможность сетевой связности с сетями общего пользования, ОЦОД и ресурсами Правительственного комплекса. Межсетевые экраны Исполнителя реализуют политику информационной безопасности, обеспечивающую ограничение, в том числе проксирование входящего, исходящего информационного обмена.

Требования по организации информационного обмена сегмента «Colocation» Заказчика с сетью Интернет:

- По умолчанию установление соединения с сетью Интернет с серверов ОК «Colocation» невозможно. При условии принятия ФОИВ рисков ИБ организация такого взаимодействия возможна, при условии проксирования исходящих соединений на уровне L7.
- Перенос ресурсов (хостов, серверов) Заказчика, имеющих белые IP-адреса в сегмент «Colocation», производится путем изменения адресации этих узлов на частные IP адреса. В дальнейшем для выхода в сеть Интернет такие хосты используют «белые» (публичные) адреса, предоставляемые Исполнителем. Исключение может составлять случай использования хостов, используемых для построения VPN на базе отечественных алгоритмов шифрования.
- Блокировка доступа к разделяемым серверным ресурсам (каталогам хранеиня обмена), реализованного с использованием небезопасных, протоколов взаимодействия (SMB, FTP и т.д.).
- Блокировка удаленного доступа пользователей, администраторов к серверам, по небезопасным протоколам удаленного управления (Telnet, HTTP и т.д.).
- Ограничение использования внешних ИТ-сервисов таких как NTP, DNS. Доступ серверам ОК будет разрешен по NTP только на адрес NTP-сервера ОЦОД. Доступ серверов ОК по DNS может быть разрешен только на ограниченный перечень предварительно согласованных внешних DNS-серверов, при условии принятия ФОИВ возникающих рисков ИБ.

В соответствии с Регламентом эксплуатации ИТ-инфраструктуры Правительственного комплекса, осуществляемого ПАО «Ростелеком», проводится периодический контроль защищенности, путём сетевого сканирования внешних и внутренних IP-адресов и анализа полученных данных на предмет наличия уязвимостей. По результатам проведенной работы Исполнитель предоставляет Функциональному Заказчику отчет, содержащий требования и рекомендации по усилению мер информационной безопасности.

Для защиты от вирусов в сегменте «Colocation» используются средства антивирусной защиты Лаборатории Касперского. Политика ИБ, настройки антивирусной защиты, контролируются Исполнителем.

2.4.3 Описание СЗИ и требований по обеспечению ИБ в Облаке ПК

В Облаке ОЦОД ОК и ЗК Предпродуктивной зоны и Продуктивной зоны Исполнитель предоставляет Заказчику полный перечень сервисов ИБ на условиях, определенных текущей редакцией Государственного контракта.

В Облаке ОЦОД в Подготовительной зоне (ОК и ЗК) и Тестовой зоне ОК Исполнитель, на условиях, определенных текущей редакцией Государственного контракта может предоставить Заказчику следующие сервисы информационной безопасности:

- Сервис антивирусной защиты;
- Сервис межсетевого экранирования и защиты от сетевых атак для ЦОД;
- Сервис управления уязвимостями, инцидентами и компьютерными атаками (SOC);
- Сервис защиты от распределённых атак вида «отказ в обслуживании» (DDOS атак);
- Сервисы защищенного удаленного доступа (ГОСТ – VPN);
- Сервис защиты от утечек информации.

Все сетевые взаимодействия между физическими контурами и логическими сетевыми сегментами/зонами ОЦОД осуществляются посредством

сертифицированных ФСТЭК межсетевых экранов. Все сетевые взаимодействия отслеживаются сертифицированными ФСТЭК средствами обнаружения вторжений.

Все компоненты ИС, требующие взаимодействия с сетью Интернет размещаются в ОК, все компоненты ИС не требующие непосредственного взаимодействия с сетью Интернет размещаются в ЗК[8].

Доступ из сети Интернет к ресурсам зон ОК определяется политикой информационного обмена, реализованной на МСЭ. При оформлении заявки на развертывание ГИС\ИС в ОЦОД Функциональный Заказчик должен указать минимальный перечень, IP-адресов, портов и протоколов, необходимых для организации работы серверов ГИС/ИС в сети Интернет.

Инициирование информационного обмена с сетью Интернет возможно только для серверов, размещенных в открытом контуре ОЦОД: Тестовой зоне (TST) ОК, Подготовительной зоне (PREP) ОК.

Сервера Предпродуктивной зоны (PPD) ОК, Продуктивной зоны (PRD) ОК в общем случае не должны являться инициаторами соединения с ресурсами сети Интернет[9].

Контроль и ограничение инициирования соединения серверов ИС/ГИС ОК с сетью Интернет осуществляется с помощью Proxy-сервера, определяющего политику информационного взаимодействия только по заранее согласованным URL-ссылкам. При этом политика Proxy-сервера не должна допускать взаимодействие с облачными ресурсами, например, GitHub, Google Drive и т.п.. в целом. Получение доступа через Proxy-сервер в сеть Интернет возможно только к отдельным разделам облачных ресурсов, либо к отдельным официальным серверам производителей ПО, с целью получения дистрибутивов, исходных кодов, документации, используемой для разработки и сопровождения прикладного ПО ИС/ГИС ФОИВ.

[8] При этом должны выполняться общие требования к ИС, размещаемым в Облаке (раздел 5.1), в частности, размещение front-end компоненты в ОК, а back-end компонент в ЗК.

[9] В отдельных технологически обоснованных случаях, при наличии согласования ФОИВ возможна организация кратковременного доступа к отдельным url-ссылкам.

Безопасность информационного взаимодействия модулей одной ИС, расположенных в разных контурах (ОК и ЗК), обеспечивается посредством шлюзов прикладного уровня (например, XML-шлюз), размещённых в шлюзовом контуре.

В виртуальных средах ЗК и ОК Облака устанавливается сертифицированное средство защиты среды виртуализации.

Для защиты от вирусов каждой ВМ в виртуальных средах ЗК и ОК Облака на усмотрение Исполнителя используются антивирусные решения ЗАО «Лаборатории Касперского».

На каждую ВМ в виртуальных средах ЗК и ОК Облака устанавливается СЗИ от НСД Secret Net Studio (SNS).

В Облаке осуществляется периодический контроль уязвимостей платформы и среды виртуализации путём сетевого сканирования внешних и внутренних IP-адресов и анализа полученных данных на предмет наличия уязвимостей, а также дополнительных сетевых и программных сенсоров различных уровней, средств поведенческого анализа, средств защиты от направленных (таргетированных) атак.

Для своевременного устранения известных уязвимостей на платформу виртуализации, ОС и системное ПО регулярно, по мере появления, должны устанавливаться актуальные обновления, опубликованные производителем ПО, что подразумевает проверки совместимости обновлений и ПО на тестовой зоне ИС, в соответствии с регламентом обновления ИС.

2.4.4 Дополнительные требования ИБ по размещению ИС в Подготовительной зоне (ОК и ЗК) ОЦОД

В Подготовительной зоне принимается следующий порядок размещения ИС:

- лицензии на системное ПО предоставляются в соответствии с контрактом на ИТ-инфраструктуру ПК установленным порядком, либо предоставляются подрядчиком ФОИВ;
- в случае инсталляции ИС с дистрибутивов

- установку ОС производит Исполнитель с официальных дистрибутивов, полученных от вендоров, либо разработчиков ИС ФОИВ,
- прикладное ПО устанавливает и настраивает администратор ИС ФОИВ;

- в случае переноса/копирования образа существующей ВМ
  - создание копии/образа ВМ осуществляет администратор ИС,
  - установку/копирование образа ВМ на Облако ПК осуществляет Исполнитель.

Неудовлетворительное состояние ИБ любой из ИС, размещенных в ОЦОД, может оказать негативное влияние на работу ИС других ФОИВ в объединённом ЦОД. В этой связи перед проведением переноса образа существующей ВМ в ОЦОД Исполнитель может выполнить анализ архитектуры, состояния ИС, а также ОС ВМ на предмет соответствия регуляторным требованиям ИБ. В случае наличия в ИС рисков ИБ, которые невозможно компенсировать наложенными средствами ИБ, миграция ИС в ОЦОД путем переноса существующей ВМ не производится. Перенос ИС в ОЦОД в этом случае может быть выполнен только инсталляцией ИС с дистрибутивов, предоставляемых ФОИВ.

Ответственным за обеспечение информационной безопасности в Подготовительной зоне является Функциональный заказчик. Это обусловлено тем, что при подготовке/проведении миграции ИС в Облако, со стороны Функционального заказчика и его соисполнителей требуется комплекс мер по приведению компонентов ИС в соответствие требованиям настоящих ТУ, в том числе, доработка прикладной части ИС, что выходит за пределы зоны ответственности Исполнителя.

Для ГИС, имеющих в своём составе публичные WEB-приложения по запросу Функционального Заказчика может оказываться сервис межсетевого экранирования уровня приложения (WAF).

При этом, в зоне ответственности Заказчика находится обеспечение:

- Актуальности прикладного и системного ПО, входящего в пакет программ ИС, развернутых в Подготовительной зоне.
- Тестирование и, в случае успеха, применение публикуемых на сайтах производителей обновлений ПО, устраняющих критичные уязвимости.
- Лицензионной чистоты прикладного и специального ПО, полученного из доверенных источников.

2.4.5 Фонд программ и документации ФОИВ ОЦОД

Фонд программ и документации (ФПД) обеспечивает хранение эталонных образов дистрибутивов и документации на ИС ФОИВ, а также передачу данных между контурами и зонами Облака.

Назначение ФПД:

- Размещение, развертывание ПО, используемого в составе ИС/ГИС ФОИВ в Продуктивной зоне, Предпродуктивной зоне, производится исключительно с дистрибутивов, находящихся в ФПД;
- Хранение эталонных образов, дистрибутивов на ПО ИС/ГИС ФОИВ, установленного в Подготовительной зоне; Продуктивной зоне, Предпродуктивной зоне.
- Хранение документации на ПО ИС/ГИС ФОИВ, развернутого в ЦОД;
- Загрузка/перенос данных в подготовительную, предродуктивную и продуктивную зоны из внешних источников, тестовой зоны или зоны Colocation. В ходе загрузки/переноса выполняются процедуры контроля на предмет отсутствия вредоносного программного кода;
- Обеспечение возможности оперативного восстановления ИС/ГИС из актуальных эталонных копий ПО.
- Переда данных из одной зоны в другую в ЗК.

ФПД по сути является файловым хранилищем и предполагает заказ ФОИВ дополнительных объемов по услуге «Файловый сервис». Заказ данной услуги является обязательным условием размещения ИС/ГИС в ЦОД. Выделяемый

объём на одну ИС/ГИС по умолчанию составляет 50 ГБ в ФПД ОК и 50 ГБ в ФПД ЗК. Изменение выделяемого объёма производится после согласования с ФОИВом.

В целях оптимизации места размещения, данные для размещения в ФПД могут быть сформированы в виде архива в форматах ZIP, ARG. Архивы, защищенные паролем, в ФПД предоставлять запрещено/не принимаются.

Данные в ФПД могут передаваться, как по сети, так и на съёмных носителях.

В Приложении Д приведена более подробная информация по организации ФПД и схеме информационного взаимодействия зон ЗК и ОК ЦОД.

2.4.6 Сегментация сети в Облаке ПК и размещение модулей ИС ФОИВ

Сеть Облака ПК разделяется сетевые сегменты, имеющие отдельный VLAN и IP-подсеть. Взаимодействие между сетевыми сегментами осуществляется через МСЭ.

Модули/серверы ИС ФОИВ располагаются в разных сетевых сегментах в соответствии со следующими правилами:

- В зоне разработки и тестирования
    - Модули/серверы каждой ИС располагаются в ОК в отдельном сегменте
- В подготовительной, предпродуктивной и продуктивной зонах
    - Для ИС, которые не подлежат аттестации
        - Модули/серверы, недоступные в сети Интернет каждой ИС, располагаются в ЗК в отдельном сегменте;
        - Модули/серверы, доступные в сети Интернет каждой ИС располагаются в ОК в одном общем сегменте продуктивной зоны;
    - Для ИС, которые являются ГИС, ИСПДн или КИИ (подлежат аттестации)
        - Модули/серверы, доступные из сети Интернет каждой ИС располагаются в ОК в отдельном сегменте;

- Модули/серверы каждой ИС, которые взаимодействуют с внешними организациями и внешними ИС, расположенными в сети Интернет или в ОК ОЦОД или ОК Башни Правительственного комплекса, располагаются в ОК в отдельном сегменте (в сегменте взаимодействия с внешними организациями);
- Модули/серверы СУБД каждой ИС располагаются в ЗК в отдельном сегменте (в сегменте СУБД);
- Модули/серверы приложений каждой ИС располагаются в ЗК в отдельном сегменте (в сегменте приложений)
- Модули/серверы резервного копирования каждой ИС располагаются в ЗК в отдельном сегменте (в сегменте backup);
- Инфраструктурные модули/серверы ИС размещаются в ЗК в отдельном общем сегменте для всех ИС ФОИВ.

3 Размещение оборудования в сегменте «Colocation»

3.1 Предоставляемые ресурсы и услуги в сегменте «Colocation» ОЦОД ПК

Исполнитель, в соответствии с требованиями настоящего документа, обеспечивает, в случае заказа, следующие ресурсы и услуги в сегменте «Colocation» ОЦОД ПК, при выполнении данных технических условий:

- Предоставление телекоммуникационной стойки с совокупным энергопотреблением оборудования, размещенного в ней, до 5 кВт (с возможностью увеличения до 7.5 кВт при наличии технических условий).
- Предоставление сетевого оборудования для телекоммуникационной стойки.
- Предоставление СКС ОЦОД для телекоммуникационной стойки.
- Администрирование инфраструктуры ОЦОД для телекоммуникационной стойки.
- Сервисное сопровождение серверной инфраструктуры ФОИВ в сегменте «Colocation»:
    - Конфигурирование оборудования и системного ПО за исключением Информационных систем Ведомств.
    - Устранение неисправностей в работе оборудования и системного ПО за исключением Информационных систем Ведомств, и восстановление его работоспособности в случае внезапного отказа.
    - Замена неисправного оборудования, удовлетворяющего требованиям настоящего документа.
- Межсетевое экранирование информационного обмена, в составе:
    - Между сегментом «Colocation» и сетью Интернет.
    - Между сегментом «Colocation» и ресурсами сети ПК.
    - Анализ трафика и обнаружение вторжений.
- Защита от атак типа «отказ в обслуживании» (Anti-DDoS).

- Обеспечение антивирусной защиты на серверах в сегменте «Colocation», в составе10:
    - Предоставление лицензии на антивирусное ПО Лаборатории Касперского.
    - Мониторинг вирусной активности на серверах в сегменте «Colocation».
    - Информирование Функционального Заказчика о вирусных инцидентах в инфраструктуре, размещенной в сегменте «Colocation».
- Контроль и анализ защищенности (включая инструментальное сканирование) для компонентов ИС, подлежащих миграции.

3.2 Описание процедуры по размещению оборудования Функционального Заказчика в сегменте «Colocation»

Функциональный Заказчик по результатам проверки соответствия оборудования требованиям настоящего документа и рекомендациям Исполнителя принимает решение о составе оборудования, которое подлежит переносу в сегмент «Colocation» ОЦОД Исполнителя.

Функциональный Заказчик разрабатывает и передает Исполнителю матрицы доступа пользователей к ИС сегмента «Colocation», ИС сегмента «Colocation» в Интернет.

В случае необходимости взаимодействия ИС Функционального Заказчика с технологическими системами ПК (серверы контроллеров домена, почтовые серверы и т.д.), Функциональный Заказчик предоставляет Исполнителю список необходимых взаимодействий, включая IP-адреса конкретных серверов ИС Заказчика, протоколы и порты взаимодействия. Взаимодействия вида «сеть-сеть» и «любой адрес-сеть» не допускаются.

Исполнитель готовит техно-рабочий проект (ТРП) на миграцию оборудования Функционального Заказчика в сегмент «Colocation» ОЦОД Исполнителя. Функциональный Заказчик и Исполнитель согласовывают ТРП.

[10] При условии соответствия списку поддерживаемых ОС, согласно официальной документации производителя СЗИ

При необходимости приведения оборудования в соответствие с требованиями настоящего документа Функциональный Заказчик проводит требуемые подготовительные работы с оборудованием, подлежащим перемещению в сегмент «Colocation» ОЦОД Исполнителя. Исполнитель проводит подготовительные работы в ОЦОД ПК в соответствии с задачами и требованиями, определенными в настоящем документе и ТРП.

Совместная комиссия, в которую входят представители Функционального Заказчика и Исполнителя, осуществляет тестирование работоспособности планируемого к перемещению и подключенного к сети электропитания оборудования и ИС, размещённых на них, в соответствии с регламентами производителя.

Исполнитель производит физическое перемещение оборудования Функционального Заказчика в телекоммуникационные стойки, предоставленные Исполнителем.

Оборудование принимается Исполнителем на основании Акта приёма-передачи и ставится на учет в соответствии с серийными номерами оборудования.

Исполнитель монтирует оборудование, переданное Функциональным Заказчиком, коммутирует его, подключает к электропитанию, к ЛВС ОЦОД и к ЛВС администрирования инфраструктуры ОЦОД, а также включает оборудование в сегменте «Colocation» ОЦОД Исполнителя в соответствии с инструкцией включения оборудования. Функциональный Заказчик вводит в эксплуатацию ИС и проверяет их работоспособность.

Совместная комиссия, в которую входят представители Функционального Заказчика и Исполнителя, осуществляет тестирование работоспособности смонтированного и подключенного к сети электропитания оборудования в соответствии с регламентами производителя.

По завершению вышеуказанных работ оборудование Функционального Заказчика, в случае выполнения условий настоящего документа, передается Исполнителю на сервисное обслуживание в соответствии с требованиями настоящего документа.

Каналы сегмента «Colocation», за исключением Интернет, с внешними ЦОД и иными внешними системами терминируются на оборудовании МСЭ/VPN-box Функционального Заказчика сегмента «Colocation». Канал Интернет терминируется на МСЭ Исполнителя.

При подключении к инфраструктуре ПК требуется обеспечить настройки политик аудита на ОС и СУБД ИС в соответствии с инструкциями Исполнителя, для обеспечения возможности расследования инцидентов ИБ.

После переезда в сегмент «Colocation» ОЦОД Функциональный Заказчик на контроллере домена (AD), находящимся на обслуживании у Функционального Заказчика, применяет, в случае его отсутствия, групповую политику (GPO), обеспечивающую установку агента управления IVANTI на все АРМ и сервера ИС Функционального Заказчика.

3.3 Условия оказания услуги «Предоставление телекоммуникационной стойки»

В рамках услуги «Предоставление телекоммуникационной стойки» Исполнителем организуется предоставление телекоммуникационных стоек размером 600x1000 и 800x1000 (по отдельному письменному запросу) с обеспечением постоянных условий эксплуатации в части бесперебойного гарантированного электропитания оборудования, необходимых параметров окружающей среды (температура, влажность), пожарной и физической безопасности.

Оборудование Функционального Заказчика должно соответствовать требованиям к эксплуатационно-техническому состоянию оборудования, указанным в настоящем документе, для возможности размещения его в сегменте «Colocation» ОЦОД ПК.

Передача оборудования Функционального Заказчика после проверки его эксплуатационно-технического состояния Исполнителю должна быть документально оформлена. Для этого Функциональный Заказчик должен

предоставить документы на оборудование в соответствии с требованиями настоящего документа. Оборудование принимается Исполнителем и ставится на учет в соответствии с серийными номерами оборудования и без его агрегирования в программно-аппаратные комплексы.

Ввод стойки в эксплуатацию (подключение стойки и установленного в ней оборудования Функционального Заказчика к электропитанию) Исполнитель осуществляет в соответствии с указанными ниже техническими условиями.

3.3.1 Требования к эксплуатационно-техническому состоянию оборудования Функционального Заказчика для размещения в сегменте «Colocation»

Оборудование должно передаваться Исполнителю в комплектном, технически исправном состоянии, без предупреждающих (желтых/оранжевых) и аварийных (красных) индикаций и без ошибок в интерфейсе управления оборудования.

Эксплуатационные характеристики оборудования должны соответствовать требованиям по размещению и монтажу оборудования в стойках.

Корпус оборудования не должен иметь механических повреждений, препятствующих его надлежащей эксплуатации; используемые кабели электропитания должны быть без дефектов.

В корпусе оборудования не должно быть не закрепленных деталей.

Оборудование должно передаваться Исполнителю в очищенном от пыли виде.

Гипервизоры и ОС, установленные на оборудовании, должны иметь действующие лицензии Правообладателя на момент передачи оборудования Исполнителю.

Целостность наклеек и (или) защитных пломб, подтверждающих соблюдение гарантийных обязательств, а также места их расположения, предусмотренные изготовителем оборудования, не должны быть нарушены.

В случае невыполнения требований данного пункта, ответственность за обслуживание оборудования, размещённых на нем ИС ФОИВ и обеспечение информационной безопасности, возлагается на ФОИВ.

3.3.2 Требования к документированию для размещения оборудования Функционального Заказчика в сегменте «Colocation»

Для документального оформления размещения оборудования в ОЦОД Исполнителя Функциональный Заказчик должен предоставить следующие данные о пассивном и активном оборудовании, обладающим серийным номером, без его агрегирования в программно-аппаратные комплексы:

- тип;
- наименование;
- производитель;
- серийный номер;
- стоимость каждой позиции оборудования (которая обладает серийным номером).

Дополнительно к вышеуказанным документам Функциональному Заказчику рекомендуется предоставить следующие данные о пассивном и активном оборудовании, обладающем серийным номером, без его агрегирования в программно-аппаратные комплексы:

- регистрационные реквизиты контракта на поддержку оборудования (при его наличии);
- наличие действующих сертификатов на оборудование: ССС/ССЭ, Ростест, электромагнитной безопасности.

Функциональный Заказчик также должен предоставить инструкцию с указанием порядка/последовательности включения оборудования Функционального Заказчика, обеспечивающую правильный ввод в эксплуатацию ИС, размещенных на оборудовании.

Окончательная приемка смонтированного в сегменте «Colocation» ОЦОД Исполнителю оборудования Функционального Заказчика производится по

окончанию работ по монтажу и тестированию такого оборудования в соответствии с регламентами производителя оборудования.

3.3.3 Требования по размещению и монтажу оборудования в стойках

Размещаемое оборудование в стойке подключается к сети 220-230 В переменного тока, частотой 50 Гц.

Совокупное энергопотребление размещаемого оборудования, размещенного в одной стойке, составляет 5 кВт, с возможностью увеличения до 7.5 кВт при наличии технических условий.

Максимальная подведённая мощность к стойке составляет не более 7,5кВт. Электрическая нагрузка на стойку рассчитывается, как алгебраическая сумма максимальной мощности устанавливаемого оборудования согласно паспорту производителя, с учетом количества всех установленных подключённых основных и резервных блоков питания. Стойки в ОЦОДе размещаются рядами – до 26 стоек в ряду. Общая подведенная мощность к ряду стоек составляет не более 130кВт.

Размещаемое в стойке оборудование должно по весовым характеристикам соответствовать ограничениям по нагрузочной способности фальшпола.

Размещение оборудования в телекоммуникационных стойках должно быть организовано так, чтобы «холодный» воздух поступал с передней стороны телекоммуникационной стойки (из холодного коридора), а «горячий» воздух выдувался с задней стороны телекоммуникационной стойки (в горячий коридор).

Оборудование принимается в стоечном исполнении.

Требуется наличие салазок (рельс) для серверов и кронштейнов для телекоммуникационного оборудования.

В стойки требуется устанавливать оборудование, имеющее специализированные крепежи для размещения в стойках.

Допускается размещение оборудования на полках в стойках (эти решения должны быть отражены в ТРП и согласованы с Исполнителем).

Допускается размещение оборудования с альтернативными схемами охлаждения. При этом такое оборудование должно быть при размещении

сгруппировано по стойкам (эти решения должны быть отражены в ТРП и согласованы с Исполнителем).

Стандартный тип подключения размещаемого оборудования в стойке имеет два независимых электроввода с номинальным выходным напряжением 220-230 В.

Размещаемое в стойке оборудование должно иметь два блока питания в режиме active-active в целях организации питания от двух независимых источников питания. В случае отсутствия в конструктиве оборудования двух и более блоков питания требуется установка устройства АВР (автомат включения резерва).

3.4 Условия оказания услуги «Предоставление сетевого оборудования для телекоммуникационной стойки»

Исполнитель обеспечивает подключение оборудования Функционального Заказчика к ЛВС ОЦОД со скоростью 1Гб/с и 10Гб/с по медным и оптическим интерфейсам.

Предоставление сетевого оборудования возможно по двум схемам:

- Предоставление сетевого оборудования для подключения перемещаемого в сегмент «Colocation» ОЦОД сетевого оборудования ФОИВ.
- Предоставление сетевого оборудования для подключения перемещаемого в сегмент «Colocation» ОЦОД серверного оборудования ФОИВ.

В связи с тем, что ЛВС ОЦОД входит состав ИТ-инфраструктуры ПК, Функциональный Заказчик должен обеспечить выполнение требований информационной безопасности на своем перемещаемого в сегмент «Colocation» ОЦОД оборудовании.

3.5 Условия оказания услуги «Администрирование инфраструктуры ОЦОД для телекоммуникационной стойки»

В рамках оказания услуги «Администрирование инфраструктуры ОЦОД для телекоммуникационной стойки» Исполнитель осуществляет по заявке Заказчика или Функционального Заказчика следующие операции:

- Смена/переустановка жёстких дисков (только поддерживающих возможность горячей замены и при наличии четких письменных инструкций) в рамках регламента взаимодействия основной услуги размещения.
- Подключение KVM-консолей (при наличии четких письменных инструкций) в рамках регламента взаимодействия основной услуги размещения.
- Перекоммутация промаркированных патч-кордов (при наличии четких письменных инструкций) в рамках регламента взаимодействия основной услуги размещения.
- Организация сетевых соединительных линий от помещений кроссовой до уровня стойки ОЦОД.
- Предоставление информации в рамках регламента взаимодействия основной услуги размещения; предоставление Заказчику или Функциональному Заказчику записи с камер видеонаблюдения, логов СКУД.

3.6 Условия оказания услуги «Сервисное сопровождение серверной инфраструктуры ФОИВ в сегменте «Colocation» ОЦОД ПК

Для обеспечения сервисной поддержки серверного оборудования Функционального Заказчика в сегменте «Colocation» ОЦОД Исполнителя организуется ЛВС мониторинга оборудования Функционального Заказчика. Исполнитель обеспечивает порты Gigabit Ethernet для подключения портов управления оборудованием. Для подключения к ЛВС мониторинга оборудование Функционального Заказчика должно соответствовать следующим условиям:

- Наличие активированной системы удаленного управления оборудованием по IP сети (IPMI).
    - Система должна обладать графическим WEB интерфейсом и/или интерфейсом командной строки.
    - Система должна отображать состояние оборудования, а также должна позволять удаленно управлять оборудованием.
    - Система должна обеспечивать мониторинг, управление, журналирование и инвентаризацию удаленного оборудования.
    - В системе должен быть настроен протокол SNMP в режиме Read Only.
- Функции управления оборудованием должны быть доступны, даже если оборудование находится в выключенном состоянии.

Оборудование должно соответствовать всем требованиям к эксплуатационно-техническому состоянию для размещения в сегменте «Colocation» ОЦОД Исполнителя, указанным в настоящем документе.

Должна быть предоставлена документация, указанная в настоящих требованиях.

Функциональный Заказчик обеспечивает предоставление программно-административного доступа, необходимого для выполнения работ по сервисной поддержке, в частности, реквизиты доступа на управляющие интерфейсы оборудования и BIOS.

Оборудование, передаваемое на сервисную поддержку, должно обладать действующей технической поддержкой производителя. Целостность наклеек и (или) защитных пломб, подтверждающих соблюдение гарантийных обязательств, а также места их расположения, предусмотренные изготовителем оборудования не должны быть нарушены. В случае снятия производителем оборудования с поддержки или нарушение целостности защитных пломб (места их расположения) также снимается сервисная поддержка оборудования Исполнителем (поддержка производителем оборудования должна включать возможность получения/приобретения вышедших из строя комплектующих).

Должна быть обеспечена возможность подключения оборудования к системе мониторинга ИТ-инфраструктуры ПК по протоколу SNMP, а если на серверном оборудовании установлена ОС Windows, то по протоколу WMI.

3.7 Условия оказания услуги «Межсетевое экранирование информационного обмена»

Услуга «Межсетевое экранирование информационного обмена» предоставляется Исполнителем на базе сертифицированных ФСТЭК по требованиям безопасности информации МСЭ/СОВ. В рамках данной услуги, межсетевое экранирование информационного обмена и анализ трафика для обнаружения вторжений обеспечивается:

- между сегментом «Colocation» и сетью Интернет;
- между сегментом «Colocation» и ресурсами сети Правительственного комплекса.

Политика безопасности, применяемая на МСЭ Исполнителя, разрабатывается на основании матрицы доступа, предоставленной Функциональным Заказчиком, в рамках процедуры подготовки к миграции. В случае необходимости взаимодействия ИС Функционального Заказчика с технологическими системами ПК (серверы контроллеров домена, почтовые серверы и другие инфраструктурные сервисы), Функциональный Заказчик включает список необходимых взаимодействий в матрицу доступа, с указанием IP-адресов конкретных серверов ИС Функционального Заказчика, протоколов и портов взаимодействия. Взаимодействия вида «сеть-сеть» и «любой адрес-сеть» не допускаются. Взаимодействия вида «все порты» или «все протоколы» также не допускаются.

Любые изменения политики межсетевого экранирования возможны на основании должным образом оформленной заявки. При этом, запрашиваемые изменения не должны нарушать требования регулятора по защите информации в ГИС/ИСПДн, а также не создавать рисков ИБ для ИС других ФОИВ ПК. В случае необходимости организации трансляции сетевых адресов (NAT) на МСЭ

Функционального заказчика, установленный внутри периметра ОЦОД Исполнителя, такая заявка может быть выполнена только с оговоркой, что ответственное лицо на стороне Функционального заказчика принимает ответственность за возможные последствия в виде инцидентов ИБ, и понимает все риски, связанные с выполнением такой заявки.

3.8 Условия оказания услуги «Защита от атак типа «отказ в обслуживании» (Anti-DDoS)»

Услуга Anti-DDoS предоставляется Исполнителем для ИС Функционального заказчика, имеющих подключение к Интернет с «белым» (публичным) IP-адресом. Услуга предназначена для выявления и предотвращения атак типа «отказ в обслуживании», путем фильтрации вредоносного трафика. При оформлении заказа на данную услугу Функциональный заказчик предоставляет ФИО и контакты ответственного работника, которому поручено оперативное взаимодействие с представителями Исполнителя.

3.9 Условия оказания услуги «Обеспечение антивирусной защиты на серверах в сегменте «Colocation»

Услуга «Обеспечение антивирусной защиты на серверах в сегменте «Colocation» может предоставляется Исполнителем на базе сертифицированных по требованиям безопасности информации средств антивирусной защиты, в составе:

- предоставление лицензии на антивирусное ПО Лаборатории Касперского;
- мониторинг вирусной активности на серверах в сегменте «Colocation»;
- информирование Функционального Заказчика о вирусных инцидентах в инфраструктуре в сегменте «Colocation».

Предоставление услуги для серверов ИС Функционального заказчика возможно только при условии соответствия версии ОС на серверах ИС Функционального заказчика требованиям совместимости применяемого антивирусного ПО.

Возможно применение ранее установленного антивирусного ПО Функционального Заказчика (за исключением ПО «Лаборатории Касперского»).

3.10 Условия оказания услуги «Контроль и анализ защищенности для компонентов ИС, подлежащих миграции»

Услуга «Контроль и анализ защищенности для компонентов ИС, подлежащих миграции» предоставляется Исполнителем на базе сертифицированных по требованиям безопасности информации средств анализа защищенности. Услуга может быть предоставлена как в процессе подготовки ИС Функционального заказчика к миграции, так и после завершения миграции ИС Функционального заказчика в ОЦОД Исполнителя. При этом, в процессе подготовки к миграции должен использоваться режим тестирования на проникновение, а в случае, если анализ защищенности производится после миграции – в режиме аудита (с использованием учетной записи, имеющей административные привилегии в целевой системе). В каждом отдельном случае, решение о формате предоставлении услуги прорабатывается отдельно в рамках подготовки проектного решения по миграции ИС Функционального заказчика.

4 Предоставление ресурсов в Облаке ПК

4.1 Общие сведения о предоставлении ресурсов

В Облаке ПК предоставляются следующие ресурсы:

- Виртуальный процессор vCPU
- Виртуальная оперативная память vRAM
- Виртуальный жёсткий диск типа 1 vHDD тип 1 (SATA)
- Виртуальный жёсткий диск типа 2 vHDD тип 2 (SAS)
- Виртуальный жёсткий диск типа 3 vHDD тип 3 (SSD)

4.2 Предоставление виртуального процессора vCPU

В Облаке ПК предоставляются виртуальные процессоры, доступные для виртуальных машин (ВМ) Заказчика.

Вычислительные мощности предоставляются на базе Intel Xeon с базовой тактовой частотой 2,4 ГГц. Переподписка CPU в Облаке ПК возможна не больше 5.

Примечание 1. Переподписка CPU – это коэффициент отношения vCPU к ядрам CPU без учета использования технологий Hyper Threading при подсчете количества ядер CPU.

Примечание 2. В Облаке ПК не предоставляются ресурсы физических процессоров (pCPU). Если требуются вычислительные мощности сопоставимые с выделением физических процессоров, то требуется заказывать большее количество vCPU (до 5 раз).

На одну ВМ может быть выделено целое число vCPU от 1 vCPU до 40 vCPU (с учётом переподписки CPU).

В случае, если для ВМ требуется от 41 vCPU до 320 vCPU (с учётом переподписки CPU), то требуется дополнительно заказать vCPU в количестве не менее 50% от требуемых для ВМ. (Требование вызвано тем, что требуется дополнительное резервирование ресурсов на другом физическом хосте для

обеспечения беспрепятственной миграции ВМ в случае отказа физического оборудования.)

Предоставление для одной ВМ более 320 vCPU (с учётом переподписки CPU) невозможно.

4.3 Предоставление виртуальной оперативной памяти vRAM

В Облаке ПК предоставляется виртуальная оперативная память vRAM, доступная для виртуальных машин (ВМ) Заказчика.

Переподписка (RAM Swapped) по оперативной памяти отсутствует.

На одну ВМ может быть выделено целое число vRAM от 1 Gb до 128 Gb.

В случае, если для ВМ требуется от 129 Gb до 870 Gb, то требуется дополнительно заказать vRAM в объёме не менее 100% от требуемых для ВМ. (Требование вызвано тем, что требуется дополнительное резервирование ресурсов на другом физическом хосте для обеспечения беспрепятственной миграции ВМ в случае отказа физического оборудования.) Возможно уменьшение совокупного объёма дополнительно резервируемых ресурсов для двух и более ВМ работающих в кластерном режиме и/или в случае упрощения требований по времени переноса/восстановления ВМ на другом физическом хосте.

Предоставление для одной ВМ более 870 Gb vRAM невозможно.

4.4 Предоставление виртуального жесткого диска типа 1 vHDD SATA

В Облаке ПК предоставляются виртуальные ресурсы хранения, доступные для виртуальных машин (ВМ) Заказчика.

Виртуальный жесткий диск типа 1 (SATA) рекомендован для долгосрочного хранения больших объемов данных.

Размер одного диска для ВМ должен иметь целое значение от 2 Gb до 10000 Gb.

Один диск для одной ВМ объёмом более 10000 Gb не может быть предоставлен. Если для ВМ требуется объём хранения более 10000 Gb, то следует заказывать 2 и более дисков.

Производительность диска тип 1 (SATA) составляет не более 40 IOPS на 1000 ГБ. Предоставляется максимальная суммарная дисковая производительность данных типов дисков до 400 IOPS на машину.

4.5 Предоставление виртуального жесткого диска типа 2 vHDD SAS

В Облаке ПК предоставляются виртуальные ресурсы хранения, доступные для виртуальных машин (ВМ) Заказчика.

Виртуальный жесткий диск типа 2 (SAS) рекомендован как для хранения данных, так и для виртуальных машин со средней интенсивностью операций ввода-вывода.

Размер одного диска для ВМ должен иметь целое значение от 2 Gb до 10000 Gb.

Один диск для одной ВМ объёмом более 10000 Gb не может быть предоставлен. Если для ВМ требуется объём хранения более 10000 Gb, то следует заказывать 2 и более дисков.

Производительность диска тип 2 (SAS) составляет не более 100 IOPS на ВМ на 1000 ГБ. Предоставляется максимальная суммарная дисковая производительность данных типов дисков до 1000 IOPS на ВМ.

4.6 Предоставление виртуального жесткого диска типа 3 vHDD SSD

В Облаке ПК предоставляются виртуальные ресурсы хранения, доступные для виртуальных машин (ВМ) Заказчика.

Виртуальный жесткий диск типа 3 (SSD) рекомендован для виртуальных машин с высокими требованиями по скорости доступа к дискам и интенсивности операций ввода-вывода.

Размер одного диска для ВМ должен иметь целое значение от 2 Gb до 10000 Gb.

Один диск для одной ВМ объёмом более 10000 Gb не может быть предоставлен. Если для ВМ требуется объём хранения более 10000 Gb, то следует заказывать 2 и более дисков.

Производительность диска тип 3 (SSD) не менее 400 IOPS на 1000 ГБ.

Предоставляется максимальная суммарная дисковая производительность данных типов дисков до 10000 IOPS на ВМ.

4.7 Система технологического резервного копирования

Система технологического резервного копирования (СТРК) предназначена для обеспечения возможности восстановления работоспособности ВМ в случае выхода из строя систем хранения данных. Система не предназначена в качестве замены стандартных процедур обеспечения консистентности данных при бекапировании (Application Consistent Backup).

В СТРК используется схема GFS (Grand-Father-Son) и в общем случае расписание выглядит следующим образом:

- полный бекап (Full backup) делается каждые 6 месяцев;
- каждую неделю делается синтетический полный бэкап – хранится только 1 полная копия для каждой ВМ;
- 1 раз в день осуществляется инкрементальный бекап (Incremental backup) - хранится 6 инкрементальных бекапов, позволяющих создание синтетического полного бекапа.

СТРК проводит резервное копирование данных и в общем случае без какого-либо влияния на функционирование ВМ. Ограничение составляют ВМ с большими объемами данных. Максимальный объем виртуальной машины, для которой производится СТРК составляет 2,5 ТБ.

СТРК не производится ввиду невозможности или не целесообразности для следующих ВМ:

- ВМ содержит БД или приложения с БД (например, MS SQL, MS Exchange, MS SharePoint и другие);
- ВМ, данные которых расположены на независимых (independent) дисках;
- ВМ, данные которых расположены на RDM (raw device mapping) дисках.

РК таких ВМ обсуждается отдельно, для каждой ВМ, поскольку для создания резервной копии требуется установка агента РК, создание учетной записи с необходимыми для осуществления бекапа правами и согласование время запуска агента РК с владельцем (администратором) ВМ.

5 Размещение ИС ФОИВ в Облаке

5.1 Общие требования к ИС, размещаемым в Облаке

ИС, перемещаемые в ОЦОД, должны быть построены на основе трехзвенной архитектуры, которая в терминах клиент-серверной модели представляется следующим образом: сервер, предоставляющий доступ к ресурсам, например, сервер СУБД (уровень доступа к ресурсам), сервер приложений (уровень прикладной логики), клиент (уровень представления данных). Все вычисления (бизнес-логика) должны быть реализованы на сервере приложения и/или СУБД.

Модули ИС должны иметь возможность быть установленными в виртуальной среде[11] под управлением гипервизора VMWare не ниже 6.7. Модули ИС, размещаемые в Облаке, должны иметь поддержку стандартной архитектуры x86.

Каждый модуль ИС должен иметь определенные IP-адреса в соответствии с IP-адресацией, определенной в Облаке. Модули ИС ОК, модули ИС ЗК и пользователи ИС должны находиться в разных IP-сетях, т.е. взаимодействие модулей ИС из разных контуров и пользователей ИС по L2 не допустимо.

При организации взаимодействия между модулями ИС передача информации должна осуществляться непосредственно между этими модулями ИС. Обмен информацией между модулями ИС через АРМ пользователя должен быть исключен.

В случае, если ИС имеет выход в Интернет и, при этом, предназначена для работы пользователей с аттестованных АРМ, в обязательном порядке должны соблюдаться следующие требования:

- ИС должна быть архитектурно разделена на модули/сервисы: часть модулей будет располагаться в ОК, другая часть в ЗК;

[11] При необходимости размещения физического оборудования в ЗК решение должно быть проработано отдельно, на стадии проектирования.

- данные, с которыми работают модули ОК должны быть отделены от данных, с которыми работают модули ЗК, т.е. храниться соответственно в системе хранения данных (СХД) ОК и СХД ЗК.

Должна быть обеспечена возможность определения авторства каждой операции в ИС за счет использования уникальных персонифицированных идентификаторов каждого пользователя, процедуры аутентификации и протоколирования действий пользователей. Проведение неавторизованных операций должно быть запрещено.

При установке программных модулей ИС на платформе ОС Windows в определенные каталоги файловой системы следует соблюдать следующие ограничения:

- запрещено осуществлять запись в системные разделы реестра; приложения должны при необходимости создавать собственные разделы реестра вне системных разделов;
- запрещено осуществлять запись в системные директории (%windir%, %windir%/REPAIR, %windir%/SYSTEM, %windir%/SYSTEM32).

При установке программных модулей ИС на платформе ОС *NIX запрещено осуществлять запись в системные директории (\bin, \sbin).

В ИС использование внешних программных средств допускается только в том случае, если их вызов не создает предпосылок к нарушению функциональной замкнутости среды т.е. расширение возможностей по работе с файловой системой, возможность создания исполняемого программного кода, возможность запуска из используемых внешних программных средств программ, не предназначенных для нормального функционирования ИС и т.д.

В случае использования аппаратных средств (токенов) для аутентификации пользователей и администраторов в ПО ИС или лицензирования ПО, электронный ключ (токен) должен быть с интерфейсом USB.

Запрещается использовать r-протоколы (rsh, rlogin, rexec и пр.) при организации взаимодействия между модулями одной ИС или же различными ИС.

5.2 Матрица и управление правами доступа обслуживающего персонала ИС

В целях соблюдения требований информационной безопасности, в части разделения доступа обслуживающего персонала, в Облаке ПК определены роли и разрешения доступа к различным зонам ИС, приведенные в таблице

Таблица 5.1 – матрица доступа обслуживающего персонала ИС

	TST	PPD	PRD	PREP
Пользователь	-	-	x	x
Администратор	x	x*	x*	x*
Тест-инженер	x	-	-	x*
Разработчик	x	x*	-	x*

* при условии использования ГОСТ VPN для удаленного доступа и сервиса контроля действий привилегированных пользователей (Privileged Access Management - PAM)

Помимо этого, в Облаке ПК действуют следующие условия аутентификации и управления правами доступа:

- ИС должна требовать от пользователя ввода аутентификационной информации (имя и пароль пользователя) при каждом запуске клиентского приложения т.е. доступ к информации и функциям ИС должен предоставляться пользователю только после предъявления уникального персонифицированного идентификатора (имени) пользователя и проведения процедуры аутентификации на основе некоторой представленной пользователем информации (пароль, ключи).
- Аутентификация пользователя не должна требовать создания учетной записи пользователя в операционной системе модуля ИС и в СУБД.
- После успешной аутентификации в системе и открытия сеанса работы пользователю должна предоставляться информация о предыдущем успешном входе в систему (как минимум дата и время).
- При взаимодействии модулей ИС, реализованных на разных хостах (виртуальных машинах) необходимо реализовывать двухстороннюю межмодульную аутентификацию.

- При взаимодействии модулей ИС, размещенных на одном хосте (виртуальной машине) аутентификация инициатора взаимодействия является обязательной.
- В алгоритмах аутентификации не должны использоваться сужающие преобразования аутентификационных данных (например, приведение букв идентификатора пользователя и/или пароля к одному регистру, ограничение количества значащих символов пароля).
- Должно быть исключено наличие аутентификационных данных, необходимых для доступа компонентов ИС к другим ИС, в программном коде компонентов ИС и (или) в доступных пользователям конфигурационных файлах.
- По окончании определенного периода неактивности пользователя система должна принудительно завершать сеанс работы пользователя и освобождать затребованные пользователем ресурсы. Наличие запущенного пользователем длительного процесса обработки (например, формирование сложного объемного отчета) должно рассматриваться как признак активности. Принудительное завершение сеанса работы до завершения данного процесса осуществляться не должно. Значение периода неактивности пользователя должно задаваться в параметрах системы администратором и быть одинаковым для всех групп пользователей.
- Должно ограничиваться количество одновременно открытых сеансов от имени одного пользователя в ИС. Максимальное значение должно задаваться в параметрах системы администратором отдельно для каждого пользователя (по умолчанию – один сеанс).
- Основным механизмом управления доступом и предоставления полномочий пользователям ИС должен быть ролевой механизм (механизм ролевого разграничения доступа). Доступ к объектам системы должен в явном виде разрешаться или запрещаться на основе атрибутов безопасности пользователя.

- При первичном заведении в системе пользователю должен быть предоставлен минимальный набор прав доступа к объектам данной системы.
- Пользовательские права (определяющие группы, к которым пользователь принадлежит, назначенные ему роли и доступные ему объекты) должны предоставляться из единого дерева прав по единым непротиворечивым правилам.
- Механизм распределения прав доступа к ресурсам и функциям системы должен обеспечивать предоставление пользователям прав, минимально необходимых для выполнения их функциональных обязанностей.
- Приложения не должны требовать наличия у пользователей ИС (включая администратора ИС) административных полномочий в операционной системе рабочего места.
- Модулю ИС при функционировании и подключении к СУБД не должно не требоваться прав администратора ОС, администратора СУБД.
- Модуль ИС необходимо ограничить правами выделенной технологической учетной записи, не имеющей прав локального входа в ОС или сервера СУБД. При этом в случае необходимости более высокие привилегии могут быть использованы, но после выполнения требуемых операций их необходимо освобождать.
- Выполнение административных задач в рамках ИС не должно требовать предоставления администратору ИС расширенных прав, равнозначных правам администраторов системного слоя: администратор СУБД (DBA, semi DBA), владельца (DBO) базы данных, администратор сервера приложений, администратор LDAP-каталога и т.п.
- Запрещается назначать группе пользователей базы данных PUBLIC какие-либо права по доступу к таблицам и хранимым процедурам (пакетам) в ИС. Для распределения прав пользователей на уровне СУБД должны использоваться специализированные группы, созданные для пользователей

ИС. Использование штатных групп СУБД для распределения прав доступа запрещено.

- Должны быть реализованы встроенные возможности контроля и мониторинга с целью проведения аудита неактивных учетных записей пользователей, например, с помощью периодического запуска отчета по пользователям, которые не осуществляли вход в систему в течение установленного периода времени. По окончании данного периода, который должен задаваться администратором в настройках ИС (значение по умолчанию – 60 дней), учетная запись такого пользователя должна блокироваться до разблокировки администратором.

5.2.1 Условия администрирования и управления учетными записями

Выполнение административных функций ИС должно быть вынесено на прикладной уровень в виде отдельного автоматизированного рабочего места (АРМ) или модуля «Администрирование», чья функциональность должна позволять осуществлять все необходимые при эксплуатации ИС административные операции. Выполнение администратором ИС своих функций не должно требовать привилегированного доступа в СУБД и ОС.

Реализация механизма администрирования должна исключать возможность прямого соединения администратора с базой данных системы в обход АРМ или модуля «Администрирование».

Возможность осуществления административных функций пользователями, не являющимися администраторами ИС, должна быть исключена. Допускается назначение пользователю определенного набора административных прав, в рамках специализированной роли «Администратор предметной области».

Должна быть исключена возможность доступа к личным паролям пользователей.

ИС должна обладать минимальными полномочиями в выполняемой среде:

- Клиентская часть ИС (АРМ пользователя) должна выполняться с правами, соответствующими правам непривилегированного пользователя в операционной системе (например, группа «Пользователи/Users», и не

требовать предоставления пользователю дополнительных прав в рамках операционной системы.

- Серверную часть ИС рекомендуется максимально изолировать от внешнего окружения (должны быть установлены разрешения на файловую систему, ветки реестра, доступ к сети, а также на использование политики доступа для Java или .NET приложений, или режима «safe mode» для PHP-приложений и пр.).

Для ИС, использующих интегрированную доменную аутентификацию, создание учетных записей пользователей в домене должно осуществляться администраторами домена. Администраторы ИС, включая администраторов узлов нижестоящего уровня, должны иметь возможность сопоставления пользователей ИС с уже созданными в домене учетными записями и управления правами пользователей в ИС.

5.2.2 Условия использования технологических учетных записей

Пароли для технологических учетных записей должны задаваться двумя сотрудниками (например, администратором сервера приложений и сотрудником службы безопасности)

Присутствие в ИС учетных технологических записей со стандартными (устанавливаемыми производителем по умолчанию) паролями должно быть исключено.

Пароли для технологических учетных записей в процессе работы системы должны храниться в модуле ИС в защищенном от несанкционированного ознакомления виде.

Определение прав технологической учётной записи должно осуществляться на уровне технологической группы, которой присваиваются необходимые права для работы данной учётной записи.

Технологическая учетная запись, от имени которой функционирует модуль ИС, должна обладать только теми правами доступа, которые являются безусловно необходимыми для выполнения операций, предусмотренных для этого модуля ИС проектной документацией, в том числе у технологических учетных записей,

используемых составными частями ИС для доступа к СУБД, должны быть только те права, которые являются безусловно необходимыми для выполнения предусмотренных документацией операций.

5.2.3 Требования к парольной защите

В случае отсутствия интеграции с внешней системой управления доступом, определяющей политику парольной защиты, контроль качества используемых паролей должен быть реализован ИС. Критерии качества паролей, допускаемых к использованию в ИС, изложены в приложении.

При попытке подбора паролей при входе в ИС (неправильный набор пароля пять раз подряд) система должна блокировать работу пользователя не менее чем на 30 минут или до разблокировки учетной записи администратором, данное событие должно регистрироваться в журнале аудита; также в журнале аудита должен фиксироваться любой неправильный набор пароля с указанием IP-адреса или имени компьютера, с которого осуществлялась данная попытка.

5.3 Условия взаимодействия модулей ИС, размещаемых в разных контурах

Т.к. взаимодействие модулей ИС ЗК с модулями ИС в ОК осуществляется через шлюзы прикладного уровня, то протоколы взаимодействия должны позволять проводить анализ информации, передаваемой между Открытым и Закрытым контуром сети, на предмет выявления потенциально небезопасного содержимого.

Передаваемые данные должны быть структурированы и типизированы. Формат передаваемых данных должен позволять осуществлять парсинг (разбор) данных на составные части для последующей проверки и строго соответствовать стандарту (например, XML). В случае получения сообщения в формате, отличном от XML, необходимо провести его конвертацию во внутренний формат XML для дальнейшей проверки, анализа и обработки.

Каждое поле XML-сообщения вида request и response с помощью политик обработки запроса по согласованным XSD-схемам на шлюзах прикладного уровня проходит контроль на соответствие разрешенному формату и валидацию на соответствие содержимого и используемым символам, поэтому тип запросов и ответов в конфигурации должен быть указан как «XML».

В XML-сообщениях должна отсутствовать передача SQL-команд (SQL-injection), в частности управляющих SQL-команд (UNION, UNION SELECT, DELETE и пр.).

В XML-сообщениях должен отсутствовать управляющий JavaScript-код.

Запрещена и будет заблокирована передача данных из ОК в ЗК, не прошедших проверку корректности:

- данных не прошедших валидацию и проверки корректности по XSD-схемам;
- сообщений или вложений, содержащих вирус, архивный запароленный или исполняемый файл;
- файлов в бинарном виде.

5.4 Условия взаимодействия с СУБД ИС

При доступе модулей ИС к функциям СУБД ИС аутентификация является обязательной.

Соединение сервера приложений с базой данных должно устанавливаться с использованием выделенной технологической учетной записи[12], пароль для которой должен задаваться двумя сотрудниками (например, администратором сервера приложений и сотрудником службы безопасности) и в процессе работы системы храниться на сервере приложений в защищенном от несанкционированного ознакомления вида.

В ИС прямой доступ к серверам СУБД должен быть открыт только серверам приложений ИС, владельцам СУБД и системным администраторам СУБД. Полномочия пользователей ИС не должны прописываться в СУБД.

[12] К технологическим относятся учетные записи, используемые процессами (сервисами) прикладного и системного уровня, для реализации функций ИС.

Для обеспечения анализа состояния базы данных ИС SQL-запросы разрешается выполнять исключительно в режиме «только чтение», т.е. запросы, не изменяющие информацию в СУБД.

5.5 Условия обеспечения безопасности программных компонентов на АРМе пользователя

Программные компоненты (Java-апплеты, ActiveX-компоненты), загружаемые на АРМы пользователей ФОИВ, должны подписываться сертификатом разработчика ПО.

Потенциально опасными функциями ActiveX-компонента можно считать: RunCode, PrintDoc, EraseFile, Shell, Call, Write, Read и т.п. поэтому рекомендуется добавлять в компоненты проверку на вызов функций только из разрешенного домена (в соответствии с описанием механизма в статье Microsoft Knowledge Base «HOWTO: Tie ActiveX control to a Specific Domain»).

Недопустимо хранить в Java-апплетах критичную информацию (пароли доступа к СУБД, ресурсам и т.п.) т.к. исходный код Java-апплетов может быть восстановлен и проанализирован

5.6 Условия организационно-технического взаимодействия при размещении ИС в Облаке[13]

Для размещения в предпродуктивной и продуктивной зонах Облака допускается только программное обеспечение, переданное в ФПД ФОИВ (с обязательной фиксацией значения хэш-функции дистрибутива) и прошедшее в установленном в ФОИВ порядке процедуру приемо-сдаточных испытаний.

ИС не должны требовать установки программного обеспечения, не имеющего отношения к реализации прикладных функций. Необходимые для функционирования ИС программные компоненты определенных версий должны входить в комплект поставки ПО.

[13] Условия организационно-технического взаимодействия при размещении ИС в Подготовительной зоне описаны в отдельном разделе

При необходимости размещения обрабатываемых в ИС данных в тестовой зоне в состав дистрибутива ИС должен быть включен специализированный конвертор, необратимо преобразующий информацию одним из следующих способов:

- использования необратимых алгоритмов хеширования (ГОСТ);
- использования набора данных, логически не связанных с продуктивными данными.

Все системное и вспомогательное прикладное ПО, устанавливаемое в Облаке, должно быть лицензировано – лицензии предоставляются ФОИВ-ом или получаются в рамках предоставления услуг у ПАО «Ростелеком».

ПО должно быть актуальной версии и включать обновления, опубликованные и рекомендованные производителем.

Первоначальную установку системного ПО производит сервисное подразделение ПАО «Ростелеком» с официальных дистрибутивов, полученных от вендоров, либо разработчиков ИС ФОИВ.

Администрирование системного ПО в тестовой зоне производит разработчик или администратор ИС.

Администрирование системного ПО в предпродуктивной и продуктивной зонах производит сервисное подразделение ПАО «Ростелеком».

Установку и администрирование прикладного ПО в тестовой зоне производит разработчик или администратор ИС.

Установку и администрирование прикладного ПО в предпродуктивной и продуктивной зонах производит администратор ИС.

В комплект документации на ИС должна входить документация на подсистему безопасности, включающая:

- инструкцию по безопасности системы;
- настройки операционной системы и СУБД (необходимые сервисы, используемые сетевые порты, права пользователей, права доступа к файлам и каталогам, аудит и т.п.);

- руководство администратора системы (предоставление прав пользователям, включая запрещенные комбинации прав и ролей пользователей в системе; перечень критичных операций, совершение которых одним лицом должно быть исключено);
- описание ключевой системы и правил работы с ней;
- описание технологических учетных записей, необходимых для работы ИС (перечень прав данных пользователей, для чего они используются и способ их заведения);
- спецификацию функциональных возможностей пакета MS Office, необходимых для работы ИС (в случае использования данного пакета).

Выгрузка из ИС информации категории ДСП, ПДн должна производиться при обязательном согласовании с подразделением ФОИВ - владельцем информации.

Возможность фактической выгрузки информации должна предоставляться пользователю только после подтверждения владельцем информации права на осуществление выгрузки для этого пользователя, для чего в системе должен быть предусмотрен алгоритм согласования и предоставления пользователям полномочий на выгрузку.

При проведении критичной операции[14] в ИС должна быть исключена возможность единоличного проведения данной операции от начала до конца. Пользователь, вводящий данные в систему, не должен осуществлять функции, относящиеся к компетенции пользователя, контролирующего введенную информацию (принцип «two persons»). Пользователь, подтверждающий информацию, не должен вносить в нее изменения; при необходимости он может только вернуть информацию на предыдущий этап обработки.

[14] Определение перечня операций, относящихся к критичным, с точки зрения бизнес-функций ИС, выполняется подразделением ФОИВ – заказчика ИС.

5.7 Условия, определяющие возможность проведения аттестации ИС ФОИВ

Для проведения аттестационных испытаний ГИС и/или ИСПДн в качестве исходных данных должны быть представлены:

- модель угроз безопасности информации;
- акт классификации информационной системы;
- техническое задание на создание (модернизацию) информационной системы и (или) техническое задание (частное техническое задание) на создание (модернизацию) системы защиты информации информационной системы;
- проектная и эксплуатационная документация на систему защиты информации информационной системы;
- организационно-распорядительные документы по защите информации;
- результаты анализа уязвимостей информационной системы;
- материалы предварительных и приемочных испытаний системы защиты информации информационной системы;

А также, иные документы, разрабатываемые в соответствии с применимыми НПА в области защиты информации.

Приложение А

(обязательное)

Приложение Б

(справочное)

Условия обеспечения ИБ в WEB-приложениях

Б.1 Требования к подсистеме управления сессиями пользователей

Авторизованному пользователю должна быть предоставлена возможность самостоятельного завершения сеанса работы. По завершению сеанса работы ИС должна удалить идентификатор соответствующей сессии и считать данного клиента неавторизованным.

Б.2 Требования к подсистеме разграничения доступа

Необходимо исключить возможность прямого обращения неавторизованного пользователя к защищенным ресурсам по известному URL. Доступ к защищенным ресурсам должен быть возможен только после проведения процедуры аутентификации.

Учетные данные пользователей должны храниться в защищенном виде. Хранение учетных данных в файлах, доступных путем обращения к ним через Web-сервер по URL, должно быть исключено.

Хранение критичной информации (учетные записи, пароли, пути к конфигурационным файлам и пр.) в HTML-страницах должно быть исключено.

В случае если в ИС предусматривается возможность внесения изменений пользователем в собственный профиль, внесенные изменения необходимо подтверждать проведением дополнительной процедуры аутентификации.

Использование заголовка REFERER, указывающего Web-серверу URL того ресурса, с которого пользователь попал на текущую страницу, в качестве основного механизма авторизации недопустимо.

Б.3 Защита от внедрения управляющих SQL-команд

Для построения в ИС SQL-запросов должны использоваться параметризованные запросы (например, хранимые процедуры).

В случае если применение параметризованных запросов невозможно, получаемые от пользователя данные должны проходить процедуру предварительной обработки, в ходе которой из них необходимо удалять метасимволы « ` -- /*», а также следующие SQL-операторы «SELECT, UNION, ALTER, UPDATE, EXEC, DROP, DELETE, INSERT». Контентная фильтрация может быть реализована с помощью специализированных регулярных выражений.

Б.4 Защита от атак «Cross-site scripting»

Для защиты от подобных атак передаваемые данные должны быть представлены текст или применены описанные ниже методы защиты.

Приведение данных к каноническому виду, а затем в случае обнаружения в них HTML-тегов выполнить следующие преобразования:

- заменить < > на &lt и >
- заменить ( ) на &#40 и)
- заменить # на #
- заменить & на &#38.

Обработка выходного потока данных – например, с использованием методов Server.HTMLEncode и HttpServerUtility.HTMLEncode в ASP и ASP.NET, преобразующие потенциально опасные символы, в том числе HTML-теги, во внутреннее безопасное представление.

Вставка данных в свойство innerText, которое обрабатывает любую информацию как текст (пассивная информация). При этом использование свойства innerHTML является недопустимым, так как данное свойство возвращает текст в виде HTML-кода.

Использование метода ValidateRequest, который осуществляет проверку записи HTML кода или сценариев в cookie-файлы (HttpRequest.Cookies), строки запросов (HttpRequest.QueryString) и HTML-формы (HttpRequest.Form).

Запретить пользователю ввод данных, в которых допустимы HTML-теги <IMG> или <TABLE>. Безопасными можно считать тэги: <PRE>,
, <P>,

<I></I>, <B></B>, в случае если дополнительно используются регулярные выражения (например, (/^(?:[\s\w\?\!\,\.\'\»]*|(?:\<\/?(?:i|b|p|br|em|pre)\>))*$/i).

При этом защитой не является перевод полученных данных в верхний регистр, а также фильтрация тэгов jscript, vbscript и т.д.

Б.5 Вывод сообщений об ошибках в Web-приложениях

ИС должна обрабатывать все сообщения об ошибках, полученные от сервера, и возвращать клиенту минимальное количество информации об ошибочных ситуациях, возникающих на сервере. При возникновении ошибки пользователю должна предоставляться только общая информация и идентификатор записи в журнале аудита с расшифровкой ошибки.

В случае нарушения работоспособности приложения следующую информацию запрещено предоставлять пользователю:

- данные о структуре файловой системы (информация о версии операционной системы, директориях с системными файлами и системным программным обеспечением, включая пути к директориям и файлам);
- фрагменты программного или конфигурационного кода;
- сообщения об ошибках при передаче запросов в СУБД;
- SQL-выражения, используемые при доступе к базе данных.

В случае выявления в приложении критичной ошибки, рекомендуется перенаправлять пользователя на HTML-страницу, при этом статус HTTP-ответа Web-сервера должен соответствовать «200».

Полный текст сообщения об ошибке, включая системные сообщения, должен сохраняться в журнале аудита так, чтобы администратор ИС мог отыскать его по идентификатору записи, сообщенной пользователю, а также посредством указания комбинации учетной записи пользователя (выполнявшего операции) и интервала времени возникновения ошибки.

Пользователю должны выводиться исчерпывающие и понятные сообщения об ошибках, когда невозможно записать текст сообщения в журнал аудита серверной части. Это касается ошибок, связанных с некорректным

функционированием клиентского приложения и невозможностью установления полноценной связи с сервером.

Б.6 Безопасность Web-сервисов

В Web-сервисах должны быть реализованы механизмы аутентификации вызывающей системы, а также механизмы разграничения доступа к Web-сервисам и их методам. Анонимные вызовы Web-сервисов запрещены.

В процессе обработки сообщения, полученного Web-сервисом, в системе-получателе необходимо проверить:

- соответствие структуры полученного сообщения утвержденной XML-схеме обмена сообщениями;
- наличие разрешения у системы-отправителя на выполнение операций, указанных в сообщении.

Помимо этого, в системе-получателе сообщения должен быть реализован аудит сообщений, полученных соответствующим Web-сервисом. В журнале аудита должно быть отражено: время, идентификатор ИС, отправившей сообщение, IP-адрес сервера-отправителя, запрошенная операция и её результат, а также результат проверки контрольного значения процедуры проверки ЭП.

Публикация UDDI-каталогов и WSDL-схем разрешается только при условии проведения аутентификации и авторизации пользователей при доступе к указанным объектам с использованием защищенных протоколов (NTLM, Kerberos).

Б.7 Требования к Web-приложениям по протоколам аутентификации

Для аутентификации пользователей должны использоваться защищенные протоколы аутентификации, допускающие передачу информации только в зашифрованном виде. Для этих целей могут использоваться, например, протоколы аутентификации NTLM/Kerberos (при интегрированной доменной аутентификации) или криптографический протокол TLSv1.2 (и выше).

При аутентификации на основе форм ввода регистрационную информацию (например, имя пользователя и его пароль) необходимо передавать в POST-запросах.

Б.8 Безопасность XML-документов и XML-схемы

Использование при обработке данных в формате XML внешних сущностей (External Entity), внешних параметров сущностей (External Parameter Entity) и внешних описаний типа документа (External Doctype) должно быть исключено.

Должна быть обеспечена защита XML-схемы от несанкционированного изменения.

Б.9 Защита данных Web-приложений

В параметрах веб-формы, предназначенных для ввода конфиденциальной информации, должны присутствовать директивы, запрещающие кеширование данных.

У параметров cookie, значения которых не должны быть доступны сценариям, выполняемым веб-браузером, должен быть выставлен атрибут HTTPOnly.

У параметров cookie, содержащих чувствительную информацию, должен быть выставлен атрибут secure.

Б.10 Обработка ввода и вывода

Должна выполняться проверка корректности вводимых пользователем данных, причем не только на стороне клиента (с использованием сценариев, исполняемых веб-браузерам), но и на стороне сервера.

В заголовках сообщений HTTP должны использоваться директивы, определяющие используемую кодировку. Использование разных кодировок для разных источников входных данных должно быть исключено.

Приложение В

(справочное)

Условия обеспечения аудита действий в ИС

В.1 Требования общего назначения

В ИС должен быть реализован механизм аудита с протоколированием следующих действий и событий:

- действий администратора системы; событий, связанных с выполнением технологических процессов внутри системы, и событий безопасности;
- действий пользователей, связанных с выполнением бизнес-операций (фискальные события);
- изменений состояния каждого документа, включая возврат документа на предыдущий этап обработки. Аудит по документам является обязательным элементом для ИС, обрабатывающих финансовые документы.

Протоколирование действий администратора системы и событий безопасности должно осуществляться средствами ИС в соответствии с требованиями данного раздела.

Должна осуществляться визуализация информации из журнала аудита в соответствии с требованиями данного раздела.

В.2 Невозможность несанкционированной модификации данных аудита

Журнал подсистемы аудита должен вестись таким образом, чтобы исключить возможность его несанкционированной модификации как путем штатных действий в рамках системы, так и извне ее.

Необходимо исключить возможность редактирования, отключения и удаления журнала аудита средствами системы, а также его импортирования в систему из какого-либо источника.

B.3 Данные журнала аудита

Наличие в журнале аудита чувствительных данных (пароли пользователей, ПДн и т.п.) должно быть исключено.

B.4 Централизованное ведение журнала аудита

Регистрация отдельных событий только составными частями ИС, потенциально доступными нарушителю (например, АРМ пользователя, общедоступные веб-серверы), должна быть исключена.

B.5 Обязательные реквизиты данных аудита

Информация в журнале подсистемы аудита должна представляться в структурированном виде в терминах прикладной области, т.е. фиксироваться должны события с бизнес-сущностями, а не с объектами баз данных. В журнале в обязательном порядке указываются следующие реквизиты события: дата и время; идентификатор пользователя, действия которого привели к возникновению события; наименование; идентификатор/наименование данных, на которые происходило воздействие; параметры; результат (успешный/неуспешный).

B.6 Время, фиксируемое в данных аудита

При протоколировании событий в журнале аудита ИС должно фиксироваться время (в формате UTC с точностью до секунды) прикладного сервера, т.е. сервера приложений.

B.7 Синхронизация времени операционной системы

Отсутствие или отключение средств синхронизации времени операционной системы на АРМ или сервере ИС должно быть исключено.

В.8 Разграничение доступа к данным аудита

Возможность доступа к данным аудита должна предоставляться только уполномоченным пользователям. Для выполнения данного требования работа с журналами в самой ИС должна осуществляться через прикладной уровень, а не через технологические интерфейсы Web-серверов, СУБД, серверов приложений.

В.9 Очистка данных аудита

Должны быть предусмотрены средства системы для очистки журнала аудита за определенный промежуток времени (за исключением как минимум шести последних месяцев) с фиксацией данного события в журнале аудита.

Должна быть исключена возможность очистки, в том числе средствами системы, журнала аудита до его архивирования или распечатки.

В.10 Возможность подключения архивных данных аудита

Журналы аудита на внешнем накопителе должны храниться не менее трех лет.

Для обеспечения работы с журналами аудита за предыдущие периоды должна быть реализована функция подключения, выгруженного на внешний накопитель журнала, при котором загружаемые данные только дополняют существующий журнал аудита, но не изменяют уже хранящейся в нем информации.

В.11 Обеспечение целостности архивных данных аудита

Должен обеспечиваться контроль целостности архивных журналов аудита, в том числе защита от ошибочных или преднамеренных действий администраторов ИС.

Например, реализация механизма периодического автоматического сброса журнала на внешние носители с помощью роботизированных средств. При этом

желательно использовать носители, не допускающие перезапись (CD-ROM с однократной записью и т.п.).

B.12 Действия при переполнении журнала аудита

При достижении журналом первого порогового значения объема, определенного параметрами ИС, администратору ИС должно выдаваться соответствующее предупреждение. При превышении журналом второго порогового значения объема, определенного параметрами ИС, администратору ИС должно выдаваться повторное предупреждение, а при записи в журнал сначала должны перезаписываться наиболее «старые» данные.

B.13 Параметры для анализа данных аудита

В системе должен быть реализован фильтр, позволяющий производить выборку и печать/выгрузку информации из журнала аудита по следующим параметрам:

- событию (например, нарушение контрольного значения процедуры ключевания);
- действиям конкретного пользователя;
- действиям над конкретным пользователем;
- действиям над конкретным документом/объектом, с разделением понятий создавшего и подтвердившего документ пользователя;
- дате (периоду дат);
- времени (периоду времени);
- комбинации вышеперечисленных параметров.

B.14 Комбинация параметров для анализа данных аудита

Должна предоставляться возможность произвольной группировки задаваемых параметров, например, получения выборки по документам, ввод и подтверждение которых совершались одним пользователем (нарушение принципа разделения полномочий). Названия событий и пользователей могут вводиться вручную либо выбираться из списка.

B.15 Управление журналом аудита

Управление журналом аудита (очистка за определенный промежуток времени, настройка списка протоколируемых операций и т.д.) должно осуществляться администратором системы. При этом все действия администратора (успешные и неуспешные) по управлению журналом аудита, включая также пассивные операции (просмотр данных), должны фиксироваться в этом же журнале.

B.16 Перечень фискальных событий журнала аудита

Для ИС в документации или условиях эксплуатации должен быть определен минимально необходимый перечень фискальных событий, которые заносятся в журнал аудита. Желательно наличие возможности настройки в системе перечня фискальных событий, подлежащих аудиту. При этом протоколирование расчетно-денежных операций является обязательным и должно осуществляться постоянно (возможность отключения их протоколирования должна отсутствовать в системе).

B.17 Протоколирование пассивных бизнес-операций

Целесообразно реализовать в ИС протоколирование пассивных бизнес-операций (просмотр данных).

B.18 Степень видимости данных журнала аудита

Область видимости данных журнала аудита (для случая иерархического администрирования) не должна превышать области видимости журналируемых данных ИС, определенной для пользователя его правами доступа. При выборке на просмотр информации из журнала аудита должны проверяться права доступа пользователей к данным; информация, доступ к которой пользователю запрещен, в выборку входить не должна.

B.19 Передача событий аудита в систему управления событиями ИБ (SIEM)

Должна быть возможность передачи событий аудита по протоколу Syslog.

Должна быть обеспечена возможность задать одного или нескольких получателей, как по IP адресу, так и по DNS имени, указать порт назначения, выбрать протокол (udp\tcp).

Должна быть возможность задать порт назначения.

Должна быть возможность выбора протокола работы Syslog (udp\tcp).

Опционально должна быть возможность для каждого получателя задать свой набор передаваемых событий.

Опционально должна быть возможность повторной отправки событий аудита по заданным диапазону времени и типам событий на указанного получателя.

B.20 Требования к журналу аудита

B.20.1 Регистрация события создания нового пользователя

Должны фиксироваться все атрибуты создаваемого пользователя.

B.20.2 Регистрация назначения/изменения пользовательских прав

Должно фиксироваться назначение пользователю прав доступа к данным и функциям системы, а также изменение прав доступа. Должна фиксироваться полная информация по назначаемым или изменяемым правам.

B.20.3 Регистрация блокирования пользователя

Должны фиксироваться все атрибуты блокируемого пользователя.

В.20.4 Регистрация входов пользователей в систему

Должны фиксироваться как входы пользователей в систему, так и выходы из нее. Должна фиксироваться информация по компьютеру, с которого осуществлен вход (IP-адрес или имя).

В.20.5 Регистрация попыток совершения НСД

Должны фиксироваться попытки совершения НСД (неправильный ввод пароля) или превышения полномочий. Должна фиксироваться информация по компьютеру, с которого был выполнен вход или была осуществлена попытка входа (IP-адрес или имя).

В.20.6 Регистрация изменений параметров и настроек

Должны фиксироваться изменения параметров и системных настроек ИС с указанием старых и новых значений параметров и настроек.

В.20.7 Регистрация нарушений целостности

Должны фиксироваться отрицательные результаты проверок целостности данных в системе, включая базы открытых ключей ЭП.

В.20.8 Регистрация случаев недоступности интерфейсов составных частей ИС

Должны фиксироваться все случаи недоступности интерфейсов составных частей ИС.

В.20.9 Регистрация автоматического завершения пользовательской сессии

Должны фиксироваться все атрибуты пользователя, сессия которого была автоматически завершена по истечении установленного периода времени.

Приложение Г

(справочное)

Критерии качества паролей

Пароль для входа в ИС считается качественным, если он удовлетворяет следующим условиям:

- длина пароля пользователя составляет не менее 8 символов;
- длина пароля администратора составляет не менее 14 символов;
- длина пароля технологической учетной записи составляет не менее 14 символов;
- в качестве пароля не используется имя учётной записи;
- пароль образован из цифр, строчных и прописных букв;
- в пароле используется минимум 6 разных символов;
- в пароле отсутствуют три рядом стоящих знака из следующих последовательностей (как слева направо, так и справа налево):
  - 1234567890-=
  - йцукенгшщзхъфывапролджэячсмитьбю
  - qwertyuiop[]asdfghjkl;’zxcvbnm,./
  - qazwsxedcrfvtgbyhnujmik,ol.p;/[‘]
  - йфяцычувскамепинртгоьшлбщдюзж.хэъ
  - 741852963
  - ЙЦУКЕНГШЩЗХЪФЫВАПРОЛДЖЭЯЧСМИТЬБЮ.
  - QWERTYUIOP[]ASDFGHJKL;’ZXCVBNM,./
  - QAZWSXEDCRFVTGBYHNUJMIK,OL.P;/[‘]
  - ЙФЯЦЫЧУВСКАМЕПИНРТГОЬШЛБЩДЮЗЖ.ХЭЪ.
  - 1йфя2цыч3увс4кам5епи6нрт7гоь8шлб9щдю0зж.-хэ=ъ
  - 1ЙФЯ2ЦЫЧ3УВС4КАМ5ЕПИ6НРТ7ГОЬ8ШЛБ9ЩДЮ0ЗЖ.-ХЭ
  - 1QAZ2WSX3EDC4RFV5TGB6YHN7UJM8IK,9OL.0P;/-[‘=]
  - 1qaz2wsx3edc4rfv5tgb6yhn7ujm8ik,9ol.0p;/-[‘=]
  - 1q2w3e4r5t6y7u8i9o0p-[=]azsxdcfvgbhnjmk,l.;/’qawsedrftgyhujikolp;[‘]

- 1Q2W3E4R5T6Y7U8I9O0P-[=]AZSXDCFVGBHNJMK,L.;/’QAWSEDRFTGYHUJIKOLP;[‘]
- 1Й2Ц3У4К5Е6Н7Г8Ш9Щ0З-Х=ЪФЯЫЧВСАМПИРТОЬЛБДЮЖ.ЭЙФЦЫУВКАЕПНРГОШЛЩДЗЖХЭЪ
- 1й2ц3у4к5е6н7г8ш9щ0з-х=ъфяычвсампиртоьлбдюж.эйфцыувкаепнргошлщдзжхэъ

Приложение Д

(справочное)

Перечень принятых сокращений

PPD	–	Предпродуктивная зона ИС
PRD	–	Продуктивная зона ИС
PREP	–	Подготовительная зона ИС
TST	–	Зона разработки и тестирования ИС
VPN	–	Virtual Private Network, Виртуальная частная сеть
АВПО	–	Антивирусное программное обеспечение
АРМ	–	Автоматизированное рабочее место
ВМ	–	Виртуальная машина
ГИС	–	Государственная информационная система
ДСП	–	Для служебного пользования
ЗК	–	Закрытый контур
ЗНО	–	Заявка на обслуживание
ИБ	–	Информационная безопасность
ИС	–	Информационная система
ИСПДн	–	Информационная система персональных данных
ИТ	–	Информационные технологии
КИИ	–	Критическая информационная инфраструктура
ЛВС	–	Локальная вычислительная сеть
МСЭ	–	Межсетевой экран
НДВ	–	Недокументированные возможности
НПА	–	Нормативный правовой акт
ОК	–	Открытый контур
ОС	–	Операционная система
ОЦОД		Объединённый центр обработки данных
ПК	–	Правительственной комплекс
ПДн	–	Персональные данные
ПО	–	Программное обеспечение
РК	–	Резервное копирование
СЗИ	–	Средства защиты информации
СКЗИ	–	Средства криптографической защиты информации
СКС	–	Структурированная кабельная сеть
СКУД	–	Система контроля и управления доступом
СТРК	–	Система технологического резервного копирования
СУБД	–	Система управления базами данных
СХД	–	Система хранения данных
ТРП	–	Техно-рабочий проект
ТУ	–	Технические условия
ФКУ	–	Федеральное казённое учреждение
ФОИВ	–	Федеральные органы исполнительной власти
ФПД	–	Фонд программной документации

ФСТЭК – Федеральная служба по техническому и экспортному контролю

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					

Подп. и дата

Инв. № дубл.

Взам. инв. №

Подп. и дата

Инв. № подл.

Изм.	Лист	№ докум.	Подп.	Дата	АГРВ.466459.301-01ТУ	Лист 71

Копировал

Формат А4