|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

ЧАСТЬ V.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на выполнение работ по созданию Информационной системы «Система обмена информацией»

На 30 листах

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Содержание

[Перечень сокращений 3](#_Toc158982575)

[Используемые нормативные правовые акты 5](#_Toc158982576)

[1 Полное наименование работ 7](#_Toc158982577)

[2 Цели выполнения работ по Контракту 7](#_Toc158982578)

[3 Состав и содержание работ по созданию ИС СОИ 8](#_Toc158982579)

[3.1 Состав работ в рамках 1-ого этапа создания ИС СОИ 8](#_Toc158982580)

[3.1.1 Содержание работ по разработке плана 1-ого этапа создания ИС СОИ 9](#_Toc158982581)

[3.1.2 Содержание работ по созданию Центрального узла ИС СОИ, включая Комплексную систему обеспечения информационной безопасности 11](#_Toc158982582)

[3.1.3 Содержание работ по аттестации ИС СОИ 14](#_Toc158982583)

[3.2 Состав работ в рамках 2-ого этапа создания ИС СОИ 15](#_Toc158982585)

[3.2.1 Содержание работ по разработке плана 2-ого этапа создания ИС СОИ 15](#_Toc158982586)

[3.2.2 Содержание работ по созданию резервного узла ИС СОИ, включая Комплексную систему обеспечения информационной безопасности 16](#_Toc158982587)

[3.2.3 Содержание работ по аттестации ИС СОИ 18](#_Toc158982588)

[4 Срок, место и условия выполнения работ 19](#_Toc158982589)

[4.1 Сроки выполнения работ 19](#_Toc158982590)

[4.2 Место и условия выполнения работ 19](#_Toc158982591)

[5 Требования к реализации основного функционала ИС СОИ 20](#_Toc158982592)

[5.1 Требования к функциям, выполняемым СОИ 20](#_Toc158982593)

[5.2 Требования к функциям, выполняемых КСОИБ СОИ 21](#_Toc158982594)

[6 Оказание услуг 22](#_Toc158982595)

[6.1 Оказание услуг по сопровождению Центрального узла ИС СОИ 22](#_Toc158982596)

[6.1.1 Общие требования к услуге по сопровождению Центрального узла ИС СОИ 23](#_Toc158982597)

[6.2 Оказание услуг по мониторингу состояния защищенности и обеспечению кибербезопасности ИС СОИ 24](#_Toc158982598)

[6.2.1 Требования к услуге по мониторингу состояния защищенности и обеспечению кибербезопасности ИС СОИ 25](#_Toc158982599)

[7 Порядок приемки работ, требования к результатам работ и отчетным документам 28](#_Toc158982600)

[7.1 Общие требования к приемке работ 28](#_Toc158982601)

[7.2 Требования к документации на ИС СОИ 28](#_Toc158982602)

[8 Требования к Исполнителю работ и услуг 30](#_Toc158982603)

Перечень сокращений

Сокращения, используемые в документе, приведены в Табл. 1.

Табл. 1 Перечень сокращений

|  |  |
| --- | --- |
| ACL | Access Control List |
| CP | Certified Professional; |
| IDS | Intrusion Detection System |
| IP | Internet Protocol |
| IRP | Incident Response Platform |
| NAT | Network Address Translation |
| SIEM | Security information and event management |
| SLA | Service-Level Agreement |
| SSH | Secure Shell |
| АРМ | Автоматизированное рабочее место; |
| Заказчик | Автономная некоммерческая организация «Международный учебно-методический центр финансового мониторинга» (далее – МУМЦФМ); |
| ИБ  ИС | Информационная безопасность;  Информационная система; |
| Исполнитель | Участник закупки, определенный конкурентным способом; |
| КСОИБ | Комплексная система обеспечения информационной безопасности; |
| ЛВС | Локальная вычислительная сеть; |
| НСД | Несанкционированный доступ; |
| ПОД/ФТ | Противодействие отмыванию денег и финансированию терроризма; |
| ОРД | Организационно-распорядительная документация; |
| ОС | Операционная система; |
| ПО | Программное обеспечение; |
| РФ | Российская Федерация; |
| СКЗИ | Средства криптографической защиты информации; |
| СОИ | Система обмена информацией; |
| СРПФР СНГ | Совет руководителей подразделений финансовой разведки – государств участников Содружества независимых государств; |
| ФАТФ | Группа разработки финансовых мер по борьбе с отмыванием денег – Financial Action TaskForce (FATF); |
| ФЗ | Федеральный закон; |
| ФРОМУ | Финансирование распространения оружия массового уничтожения; |
| ФСБ России | Федеральная служба безопасности Российской Федерации; |
| ФСО России | Федеральная служба охраны Российской Федерации; |
| ФСТЭК России | Федеральная служба по техническому и экспортному контролю Российской Федерации; |
|  |  |
|  |  |
|  |  |

Используемые нормативные правовые акты

* + Поручение Президента Российской Федерации Пр-249 от 07.02.2023;
  + Концепция развития национальной системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (утв. Президентом РФ 30.05.2018);
  + Концепция сотрудничества государств-участников Содружества Независимых Государств в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения (одобрена Решением Совета глав государств Содружества Независимых Государств «О Концепции сотрудничества государств-участников Содружества Независимых Государств в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения» от 11.10.2017);
  + Соглашение об образовании Совета руководителей подразделений финансовой разведки государств – участников Содружества Независимых Государств от 05.12.2012;
  + Федеральный закон от 28.06.2013 № 134–ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия незаконным финансовым операциям»;
  + постановление Правительства Российской Федерации от 06.07.2015 № 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»;
  + Указ Президента Российской Федерации от 13.06.2012 № 808 «Вопросы Федеральной службы по финансовому мониторингу» (вместе с «Положением о Федеральной службе по финансовому мониторингу»);
  + Указ Президента Российской Федерации от 18.11.2015 № 562 «О Межведомственной комиссии по противодействию финансированию терроризма» (вместе с «Положением о Межведомственной комиссии по противодействию финансированию терроризма»);
  + постановление Правительства РФ от 24.07.2021 № 1264 «Об утверждении Правил обмена документами в электронном виде при организации информационного взаимодействия»;
  + Приказ Минцифры России № 667, ФСО России № 233 от 04.12.2020 «Об утверждении Требований к организационно-техническому взаимодействию государственных органов и государственных организаций»;
  + Методология оценки технического соответствия рекомендациям ФАТФ и эффективности систем ПОД/ФТ системы (октябрь 2019 года);
  + Руководящие указания ФАТФ «Оценка рисков ОД/ФТ на национальном уровне» (февраль 2013 года);
  + Международные стандарты по противодействию отмыванию доходов, финансированию терроризма и финансированию распространения оружия массового уничтожения – Рекомендации ФАТФ (октябрь 2020 года);
  + Национальные стандарты электронного взаимодействия стран-участниц СРПФР СНГ;
  + постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
  + постановление Правительства Российской Федерации от 16.02.2008 № 87 «О составе разделов проектной документации и требованиях к их содержанию»;
  + Приказ ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;
  + Приказ ФСТЭК России № 17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
  + ГОСТ Р 59793–2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;
  + ГОСТ 34.201–2020 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;
  + ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний»;
  + ГОСТ 34.602–2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
  + ГОСТ Р 59792-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды испытаний автоматизированных систем»;
  + ГОСТ 19.101–77 «Единая система программной документации. Виды программ и программных документов»;
  + ГОСТ 19.503–79 «Единая система программной документации. Руководство системного программиста. Требования к содержанию и оформлению»;
  + ГОСТ 7.79–2000 «Система стандартов по информации, библиотечному и издательскому делу. Правила транслитерации кирилловского письма латинским алфавитом»;
  + ГОСТ Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;
  + ГОСТ Р ИСО 15704-2022 «Моделирование и архитектура предприятия. Требования к стандартным архитектурам и методологиям предприятия»;
  + ГОСТ Р 57193-2016 «Системная и программная инженерия. Процессы жизненного цикла систем»;
  + ГОСТ 19.102–77 «Единая система программной документации. Стадии разработки»;
  + ГОСТ Р ИСО 21500-2014 «Руководство по проектному менеджменту»;
  + ГОСТ Р 54871–2011 «Проектный менеджмент. Требования к управлению программой»;
  + ГОСТ Р 54869–2011 «Проектный менеджмент. Требования к управлению проектом»;
  + ГОСТ 12.1.030–81 «Система стандартов безопасности труда. Электробезопасность. Защитное заземление. Зануление»;
  + ГОСТ 15150–69 «Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды»;
  + ГОСТ 21958–76 «Система "Человек-машина". Зал и кабины операторов. Взаимное расположение рабочих мест. Общие эргономические требования»;
  + ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения»;
  + ГОСТ 27331–87 «Пожарная техника. Классификация пожаров»;
  + ГОСТ 32396–2021 «Устройства вводно-распределительные для жилых и общественных зданий. Общие технические условия»;
  + ГОСТ Р ИСО 9001–2015 «Системы менеджмента качества. Требования»;
  + ГОСТ 10434–82 «Соединения контактные электрические. Классификация. Общие технические требования»;
  + ГОСТ 32397–2020 «Щитки распределительные для производственных и общественных зданий. Общие технические условия»;
  + ГОСТ Р ИСО 14001–2016 «Системы экологического менеджмента. Требования и руководство по применению»;
  + ГОСТ 12.2.003–91 «Система стандартов безопасности труда. Оборудование производственное. Общие требования безопасности»;
  + ГОСТ Р 50571.22–2000 «Электроустановки зданий. Часть 7. Требования к специальным электроустановкам. Раздел 707. Заземление оборудования обработки информации»;
  + «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР–К) (утв. Приказом Председателя Гостехкомиссии России от 30.08.2002 № 282);
  + Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. решением Председателя Гостехкомиссии России от 30.03.1992);
  + Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением Председателя Гостехкомиссии России от 30.03.1992);
  + Нормативно–технический документ «Требования к системам обнаружения вторжений» (утв. приказом ФСТЭК России от 6.12.2011 № 638);
  + Нормативно–технический документ «Требования к средствам антивирусной защиты» (утв. приказом ФСТЭК России от 20.03.2012 № 28);
  + Нормативно–технический документ «Требования к средствам электронной подписи» (утв. приказом ФСБ России от 27.12. 2011 № 796);
  + Рекомендация Коллегии Евразийской экономической комиссии от 12.03.2019 № 9 «О перечне стандартов и рекомендаций в области информационной безопасности, применяемых в рамках реализации цифровой повестки Евразийского экономического союза».

1. Полное наименование работ

Работы по созданию информационной системы «Система обмена информацией» (далее – ИС СОИ).

1. Цели выполнения работ

Работы по созданию ИС СОИ направлены на достижение Международным учебно-методическим центром финансового мониторинга (далее – МУМЦФМ) цели по оказанию технического содействия государствам-партнёрам Российской Федерации с использованием защищенной телекоммуникационной сети с применением сертифицированных СКЗИ и обеспечения импортонезависимости.

1. Состав и содержание работ по созданию ИС СОИ

Работы по созданию ИС СОИ выполняются на основании проектной документации, указанной в п.3.1.1.

ИС СОИ состоит из прикладных компонентов (далее – СОИ) и Комплексной системы обеспечения информационной безопасности ИС СОИ (далее – КСОИБ СОИ). Для достижения цели, указанной в разделе 2 планируется проведение работ в 2 этапа:

Состав работ в рамках 1-ого этапа:

1. Разработка плана 1-ого этапа создания ИС СОИ;
2. Создание Центрального узла ИС СОИ, включая Комплексную систему обеспечения информационной безопасности:
   1. Актуализация комплекта проектной документации (технический проект) на создание СОИ и КСОИБ СОИ;
   2. Разработка и согласование рабочей (исполнительной) документации на СОИ и КСОИБ СОИ;
   3. Реализация технических решений в рамках создания Центрального узла ИС СОИ;
   4. Проведение опытной эксплуатации 1-ого этапа создания ИС СОИ (СОИ и КСОИБ СОИ);
   5. Проведение приёмочных испытаний 1-ого этапа создания ИС СОИ (СОИ и КСОИБ СОИ).
3. Аттестация ИС СОИ;

Состав работ в рамках 2-ого этапа:

1. Разработка плана 2-ого этапа создания ИС СОИ;
2. Создание Резервного узла ИС СОИ, включая Комплексную систему обеспечения информационной безопасности:
   1. Актуализация комплекта проектной (технический проект) и рабочей (исполнительной) документации на создание СОИ и КСОИБ СОИ;
   2. Реализация технических решений в рамках создания Резервного узла ИС СОИ;
   3. Проведение опытной эксплуатации 2-ого этапа создания СОИ и КСОИБ СОИ;
   4. Проведение приёмочных испытаний 2-ого этапа создания СОИ и КСОИБ СОИ;
3. Аттестация ИС СОИ.
   1. Состав работ в рамках 1-ого этапа создания ИС СОИ

В 1-ом этапе планируется реализация технических решений в составе Центрального узла ИС СОИ:

* Компонент сетевого взаимодействия;
* Компонент авторизации пользователей;
* Компонент учета взаимодействующих организаций, объединений и их представителей;
* Компонент оповещения пользователей о значимых событиях (перечень событий определяется на этапе проектирования);
* Компонент логирования действий пользователей;
* Средство защиты каналов связи;
* Средство межсетевого экранирования;
* Средство контроля защищённости и соответствия стандартам;
* Средство сбора и анализа событий;
* Средство обнаружения вторжений;
* Средство доверенной загрузки;
* Средство антивирусной защиты;
* Средство защиты от несанкционированного доступа.

По результатам выполнения работ 1-ого этапа Исполнитель предоставляет Заказчику комплект документации, приведенный в Календарном плане выполнения работ по созданию ИС СОИ (Приложение № 2 к Договору).

* + 1. Содержание работ по разработке плана 1-ого этапа создания ИС СОИ

Заказчик предоставляет следующую проектную документацию, содержащую информацию о текущем состоянии программной и технической составляющей, целевой архитектуре, процессах и технологиях обеспечения информационной безопасности в СОИ и КСОИБ СОИ:

* Техническое задание на СОИ;
* Техническое задание на КСОИБ СОИ;
* Модель угроз и нарушителя безопасности информации СОИ;
* ОРД на СОИ;
* Комплект проектной документации СОИ:
  + Ведомость технического проекта (ТП);
  + Ведомость покупных изделий (ВП);
  + Схема организационной структуры (С0);
  + Схема структурная комплекса технических средств (С1);
  + Схема функциональной структуры (С2);
  + Пояснительная записка к техническому проекту (П2);
  + Описание автоматизируемых функций (П3);
  + Описание информационного обеспечения системы (П5);
  + Описание организации информационной базы (П6);
  + Описание комплекса технических средств (П9);
  + Описание программного обеспечения (ПА).
* Комплект проектной документации КСОИБ СОИ:
  + Ведомость технического проекта (ТП);
  + Ведомость покупных изделий (ВП);
  + Схема организационной структуры (С0);
  + Схема структурная комплекса технических средств (С1);
  + Схема функциональной структуры (С2);
  + Пояснительная записка к техническому проекту (П2);
  + Описание комплекса технических средств (П9);
  + Описание программного обеспечения (ПА).

На основании вышеуказанной документации и информации, а также с учетом изменений проектных решений и требований к ИС СОИ, должно быть актуализовано техническое задание на СОИ и КСОИБ СОИ в соответствии с нижеперечисленными стандартами и нормативными документами:

* + ГОСТ Р 59793–2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;
  + ГОСТ 34.201–2020 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;
  + ГОСТ РО 0043-004–2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний»;
  + ГОСТ 34.602–2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
  + ГОСТ Р 59792-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды испытаний автоматизированных систем»;
  + ГОСТ 19.101–77 «Единая система программной документации. Виды программ и программных документов»;
  + ГОСТ 19.503–79 «Единая система программной документации. Руководство системного программиста. Требования к содержанию и оформлению»;
  + ГОСТ 7.79–2000 «Система стандартов по информации, библиотечному и издательскому делу. Правила транслитерации кирилловского письма латинским алфавитом»;
  + ГОСТ Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;
  + ГОСТ Р ИСО 15704-2022 «Моделирование и архитектура предприятия. Требования к стандартным архитектурам и методологиям предприятия»;
  + ГОСТ Р 57193-2016 «Системная и программная инженерия. Процессы жизненного цикла систем»;
  + ГОСТ 19.102–77 «Единая система программной документации. Стадии разработки»;
  + ГОСТ Р ИСО 21500-2014 «Руководство по проектному менеджменту»;
  + ГОСТ Р 54871–2011 «Проектный менеджмент. Требования к управлению программой»;
  + ГОСТ Р 54869–2011 «Проектный менеджмент. Требования к управлению проектом»;
  + ГОСТ 12.1.030–81 «Система стандартов безопасности труда. Электробезопасность. Защитное заземление. Зануление»;
  + ГОСТ 15150–69 «Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды»;
  + ГОСТ 21958–76 «Система "Человек-машина". Зал и кабины операторов. Взаимное расположение рабочих мест. Общие эргономические требования»;
  + ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения»;
  + ГОСТ 27331–87 «Пожарная техника. Классификация пожаров»;
  + ГОСТ 32396–2021 «Устройства вводно-распределительные для жилых и общественных зданий. Общие технические условия»;
  + ГОСТ Р ИСО 9001–2015 «Системы менеджмента качества. Требования»;
  + ГОСТ 10434–82 «Соединения контактные электрические. Классификация. Общие технические требования»;
  + ГОСТ 32397–2020 «Щитки распределительные для производственных и общественных зданий. Общие технические условия»;
  + ГОСТ Р ИСО 14001–2016 «Системы экологического менеджмента. Требования и руководство по применению»;
  + ГОСТ 12.2.003–91 «Система стандартов безопасности труда. Оборудование производственное. Общие требования безопасности»;
  + ГОСТ Р 50571.22–2000 «Электроустановки зданий. Часть 7. Требования к специальным электроустановкам. Раздел 707. Заземление оборудования обработки информации»;
  + «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР–К) (утв. Приказом Председателя Гостехкомиссии России от 30.08.2002 № 282);
  + Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. решением Председателя Гостехкомиссии России от 30.03.1992);
  + Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением Председателя Гостехкомиссии России от 30.03.1992);
  + Нормативно–технический документ «Требования к системам обнаружения вторжений» (утв. приказом ФСТЭК России от 6.12.2011 № 638);
  + Нормативно–технический документ «Требования к средствам антивирусной защиты» (утв. приказом ФСТЭК России от 20.03.2012 № 28);
  + Нормативно–технический документ «Требования к средствам электронной подписи» (утв. приказом ФСБ России от 27.12. 2011 № 796);
  + Рекомендация Коллегии Евразийской экономической комиссии от 12.03.2019 № 9 «О перечне стандартов и рекомендаций в области информационной безопасности, применяемых в рамках реализации цифровой повестки Евразийского экономического союза».

В рамках разработки плана 1-ого этапа создания ИС СОИ должно быть актуализировано Техническое задание на создание ИС СОИ.

При необходимости Техническое задание на создание ИС СОИ должно быть актуализировано в части технических решений, обеспечивающих информационную безопасность инфраструктурных и общесистемных подсистем ИС СОИ в соответствии с требованиями по импортонезависимости.

В рамках разработки плана 1-ого этапа создания ИС СОИ необходимо определить итоговый перечень ОРД и согласовать с Заказчиком Ведомость покупных изделий.

По результатам выполнения работ по 1-ому этапу Исполнитель предоставляет комплект документации, указанный в Календарном плане выполнения работ по созданию ИС СОИ (Приложение № 2 к Договору).

* + 1. Содержание работ по созданию Центрального узла ИС СОИ, включая Комплексную систему обеспечения информационной безопасности

Результатом данных работ должен являться ввод в действие Центрального узла ИС СОИ, разработанный комплект проектной и рабочей документации согласно п. 7.2.1. настоящего Технического задания, включая разработанный комплект ОРД на ИС СОИ и Модель угроз и нарушителя безопасности информации ИС СОИ.

* + - 1. Актуализация комплекта проектной документации (технический проект) на создание СОИ и КСОИБ СОИ

Технический проект должен быть актуализирован в соответствии с требованиями, указанными в настоящем Техническом задании.

Технический проект должен отражать реализуемые решения в рамках целевой архитектуры ИС СОИ.

В техническом проекте должны быть описаны режимы функционирования.

Исполнителем должно быть выполнено: уточнение места и плана размещения оборудования на площадках, а также уточнение следующих параметров:

* + подключения ЛВС к смежным и внешним системам;
  + инженерных систем по месту подключения;
  + текущей системы мониторинга и управления;
  + настройки АРМ.

По результатам выполнения работ Исполнитель предоставляет:

* Комплект проектной документации СОИ (состав проектной документации приведен в п 7.2.1. подпункт 4 настоящего Технического задания).
* Комплект проектной документации КСОИБ СОИ (состав проектной документации приведен в п 7.2.1. подпункт 5 настоящего Технического задания).
  + - 1. Разработка и согласование рабочей (исполнительной) документации на СОИ и КСОИБ СОИ

По результатам выполнения работ Исполнитель предоставляет:

* Комплект рабочей (исполнительной) документации на СОИ (состав рабочей (исполнительной) документации на ИС СОИ приведен в п 7.2.1. подпункт 6 настоящего Технического задания).
* Комплект рабочей (исполнительной) документации на КСОИБ СОИ (состав рабочей (исполнительной) документации на КСОИБ СОИ приведен в п 7.2.1. подпункт 7 настоящего Технического задания).
  + - 1. Реализация технических решений в рамках 1-ого этапа

В рамках 1-ого этапа реализации технических решений ИС СОИ должны быть проведены работы по созданию Центрального узла ИС СОИ. В составе Центрального узла ИС СОИ должны быть реализованы основные функции компонентов СОИ и КСОИБ СОИ.

* + - * 1. Состав работ по внедрению компонентов СОИ:
* В состав работ на каждый компонент СОИ, указанный в п. 3.1 настоящего Технического задания, входит:

1. Установка компонента;
2. Настройка компонента в соответствии с проектной и рабочей документацией;
3. Интеграция компонентов со смежными системами согласно проектной и рабочей документации.
   * + - 1. Состав работ по внедрению средства защиты каналов связи:

* монтаж оборудования, установка и коммутация;
* настройка кластеризации;
* настройка IP-адресации, туннелируемых ресурсов, связей с ПО администратора;
* установка лицензий.
  + - * 1. Состав работ по внедрению средства межсетевого экранирования:
* настройка маршрутизации в рамках инфраструктуры 1-ого этапа создания ИС СОИ;
* настройка сегментации в рамках инфраструктуры 1-ого этапа создания ИС СОИ;
* настройка ACL, NAT.
  + - * 1. Состав работ по внедрению средства контроля защищённости и соответствия стандартам:
* тиражирование функционала средства контроля защищённости и соответствия стандартам на конечные устройства 1-ого этапа создания ИС СОИ
  + - * 1. Состав работ по внедрению средства сбора и анализа событий
* установка ОС;
* установка и базовая настройка агентов средства сбора и анализа событий;
* подключение источников.
  + - * 1. Состав работ по внедрению средства антивирусной защиты:
* установка антивирусного ПО на конечные устройства 1-ого этапа создания ИС СОИ;
* подключение к серверу централизованного управления;
* настройка групп и политик защищаемых устройств для ИС СОИ.
  + - * 1. Состав работ по настройке средства защиты от несанкционированного доступа:
* конфигурация средств защиты от НСД в соответствии с требованиями приказа ФСТЭК России № 17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» Класс защищенности информационной системы К1.
  + - * 1. Состав работ по внедрению средства доверенной загрузки:
* настройка общих параметров модулей на конечных устройствах 1-ого этапа создания ИС СОИ;
* настройка журналов на конечных устройствах 1-ого этапа создания ИС СОИ;
* регистрация токенов на конечных устройствах 1-ого этапа создания ИС СОИ.
  + - * 1. Состав работ по внедрению средства обнаружения вторжений:
* монтаж, подключение, проверка, первоначальная инициализация на площадке Центрального узла ИС СОИ;
* скачивание и обновление сигнатур;
* настройка политик IDS;
* отладка политик;
* постановка решения на мониторинг.
  + - 1. Проведение опытной эксплуатации 1-ого этапа создания ИС СОИ

Опытная эксплуатация проводится по разработанной и согласованной программе и методике опытной эксплуатации. Задачей на данном этапе является выявление дефектов работы системы и последующее их устранение. По результатам опытной эксплуатации принимают решение о готовности предъявления компонентов ИС СОИ в рамках создания Центрального узла ИС СОИ на приемочные испытания, или о необходимости доработки. Завершение опытной эксплуатации фиксируется подписанием протокола опытной эксплуатации.

* + - 1. Проведение приёмочных испытаний 1-ого этапа создания ИС СОИ

Приемочные испытания проводят в соответствии с разработанной и согласованной программой и методикой приемочных испытаний. Приемочные испытания проводятся для определения соответствия ИС СОИ в рамках 1-ого этапа создания Центрального узла ИС СОИ техническому заданию и решения вопроса о возможности приемки в постоянную эксплуатацию.

Результаты испытаний, предусмотренных программой и методикой испытаний, фиксируют в протоколах.

Приемочные испытания завершаются оформлением и утверждением заключения о возможности приемки Центрального узла ИС СОИ в постоянную эксплуатацию.

По результатам выполнения работ Исполнитель предоставит Заказчику полный комплект документации СОИ и КСОИБ СОИ (в соответствии с этапом 1.2 «Создание Центрального узла ИС СОИ, включая Комплексную систему обеспечения информационной безопасности» Календарного плана выполнения работ по созданию ИС СОИ, приведённого в Приложении № 2 к Договору) и систему в целом, реализующую утверждённый функционал 1-ого этапа создания ИС СОИ в полном объёме и отвечающую требованиям технического задания.

* + 1. Содержание работ по аттестации ИС СОИ

Работы по аттестации ИС СОИ в объёме 1-ого этапа создания ИС СОИ (объекта информатизации) должны включать:

1. Проведение обследования объекта информатизации.
2. Подготовка объекта информатизации к аттестационным испытаниям.
3. Проведение аттестации и разработка аттестационной документации для ИС СОИ в объёме 1-ого этапа создания ИС СОИ.

В ходе обследования Исполнитель должен уточнить (проанализировать) для ИС СОИ в объёме 1-ого этапа создания ИС СОИ следующую информацию:

* технологические процессы обработки информации;
* состав программного обеспечения, используемого при обработке информации;
* общесистемные и прикладные программные средства;
* состав средств и размещения объекта информатизации относительно контролируемой зоны;
* физические и логические связи между компонентами ИС СОИ в объёме 1-ого этапа создания ИС СОИ;
* физические и логические связи между ИС СОИ в объёме 1-ого этапа создания ИС СОИ и другими информационными системами, в том числе с сетями общего пользования;
* провести анализ состава организационно-распорядительной и нормативной документации, а также проверить наличие установленных сертифицированных средств защиты информации и их настроек.

В рамках подготовки ИС СОИ в объёме 1-ого этапа создания ИС СОИ к аттестационным испытаниям, Исполнитель должен разработать (актуализировать) Технический паспорт для ИС СОИ. Технический паспорт должен быть разработан в соответствии с Приказом ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

В ходе аттестации на соответствие требованиям безопасности информации ИС СОИ в объёме 1-ого этапа создания ИС СОИ, Исполнитель обязан:

1. Разработать документ «Программа и методики аттестационных испытаний».
2. Провести аттестационные испытания в соответствии с разработанной Программой и методикой испытаний.
3. Оформить Протокол по результатам аттестационных испытаний.
4. Оформить заключение по результатам аттестационных испытаний.

Программа и методика проведения аттестационных испытаний должна быть разработана в соответствии с Приказом Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну», ГОСТ РО 0043-004-2013 и согласована с Заказчиком до начала проведения аттестационных испытаний системы на соответствие требованиям безопасности информации.

Аттестация на соответствие требованиям безопасности информации ИС СОИ в объёме 1-ого этапа создания ИС СОИ должна выполняться в соответствии со следующими нормативными документами:

* Приказ ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;
* Приказ ФСТЭК России № 17 от 11.02.2013 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

По результатам выполнения работ по аттестации ИС СОИ в объёме 1-ого этапа создания ИС СОИ, должны быть разработаны следующие документы:

* Технический паспорт;
* Программа и методика аттестационных испытаний;
* Протокол проведения аттестационных испытаний;
* Заключение по результатам аттестационных испытаний;
* Аттестат соответствия требованиям по безопасности информации  
  (Аттестат выдается только при успешном прохождении аттестационных испытаний и положительном Заключении. При отрицательном результате проведения аттестационных испытаний выдаётся Заключение с соответствующими выводами).
* Акт о приемке ИС СОИ в объёме 1-ого этапа создания ИС СОИ в постоянную эксплуатацию (выдается только при успешном прохождении аттестационных испытаний и положительном Заключении).
  1. Состав работ в рамках 2-ого этапа создания ИС СОИ

Во 2-ом этапе планируется реализация технических решений в составе Резервного узла ИС СОИ:

* Компонент сетевого взаимодействия;
* Компонент авторизации пользователей;
* Компонент учета взаимодействующих организаций, объединений и их представителей;
* Компонент оповещения пользователей о значимых событиях (перечень событий определяется на этапе проектирования);
* Компонент логирования действий пользователей.
* Средство защиты каналов связи;
* Средство межсетевого экранирования;
* Средство контроля защищённости и соответствия стандартам;
* Средство сбора и анализа событий;
* Средство обнаружения вторжений;
* Средство доверенной загрузки;
* Средство антивирусной защиты;
* Средство защиты от несанкционированного доступа.

По результатам выполнения работ 2-ого этапа Исполнитель предоставляет Заказчику комплект документации, приведенный в Календарном плане выполнения работ по созданию ИС СОИ (Приложение № 2 к Договору).

* + 1. Содержание работ по разработке плана 2-ого этапа создания ИС СОИ

С учетом специфики архитектурных решений и систем Резервного узла ИС СОИ и определения план 2-ого этапа создания ИС СОИ должно быть актуализовано техническое задание на СОИ и КСОИБ СОИ.

В рамках разработки плана 2-ого этапа создания ИС СОИ должно быть актуализировано Техническое задание на создание ИС СОИ в части плана 2-ого этапа создания ИС СОИ.

В рамках разработки плана 2-ого этапа создания ИС СОИ необходимо согласовать с Заказчиком Ведомость покупных изделий.

По результатам выполнения работ по 2-ому этапу Исполнитель предоставляет комплект документации, указанный в Календарном плане выполнения работ по созданию ИС СОИ (Приложение № 2 к Договору).

* + 1. Содержание работ по созданию Резервного узла ИС СОИ, включая Комплексную систему обеспечения информационной безопасности

Результатом данных работ должен являться ввод в действие Резервного узла ИС СОИ, разработанный комплект проектной и рабочей документации согласно настоящему Техническому заданию.

* + - 1. Актуализация комплекта проектной документации (технический проект) и рабочей (исполнительной) документации на создание СОИ и КСОИБ СОИ

По результатам выполнения работ Исполнитель предоставляет актуализированный комплект документов в соответствии с реализуемыми техническими решениями 2-ого этапа создания ИС СОИ:

* Комплект проектной документации СОИ (состав проектной документации приведен в п 7.2.1. подпункт 4 настоящего Технического задания);
* Комплект проектной документации КСОИБ СОИ (состав проектной документации приведен в п 7.2.1. подпункт 5 настоящего Технического задания);
* Комплект рабочей (исполнительной) документации на СОИ (состав рабочей (исполнительной) документации приведен в п 7.2.1. подпункт 6 настоящего Технического задания);
* Комплект рабочей (исполнительной) документации на КСОИБ СОИ (состав рабочей (исполнительной) документации приведен в п 7.2.1. подпункт 7 настоящего Технического задания).
  + - 1. Реализация и развитие технических решений в рамках 2-ого этапа

В рамках 2-ого этапа реализации технических решений ИС СОИ должны быть проведены работы по созданию Резервного узла ИС СОИ. В составе Резервного узла ИС СОИ должны быть реализованы основные функции компонентов СОИ и КСОИБ СОИ.

* + - * 1. Состав работ по внедрению компонентов СОИ:
* В состав работ на каждый компонент СОИ, указанный в п. 3.2 настоящего Технического задания, входит:

1. Установка компонента;
2. Настройка компонента в соответствии с проектной и рабочей документацией;
3. Интеграция компонента со смежными системами согласно проектной и рабочей документации.
   * + - 1. Состав работ по развитию средства защиты каналов связи:

* монтаж оборудования, установка и коммутация на площадках Резервный узел ИС СОИ;
* настройка кластеризации;
* настройка IP-адресации, туннелируемых ресурсов, связей с ПО администратора;
* установка лицензий.
  + - * 1. Состав работ по развитию средства межсетевого экранирования:
* настройка маршрутизации в рамках инфраструктуры 2-ого этапа создания ИС СОИ;
* настройка сегментации в рамках инфраструктуры 2-ого этапа создания ИС СОИ;
* настройка ACL, NAT.
  + - * 1. Состав работ по развитию средства контроля защищённости и соответствия стандартам:
* тиражирование функционала средства контроля защищённости и соответствия стандартам на конечные устройства 2-ого этапа создания ИС СОИ
  + - * 1. Состав работ по внедрению средства сбора и анализа событий
* установка ОС;
* установка и базовая настройка агентов средства сбора и анализа событий;
* подключение источников.
  + - * 1. Состав работ по внедрению средства антивирусной защиты:
* установка антивирусного ПО на конечные устройства 2-ого этапа создания ИС СОИ;
* подключение к серверу централизованного управления;
* настройка групп и политик защищаемых устройств для ИС СОИ.
  + - * 1. Состав работ по настройке средства защиты от несанкционированного доступа:
* конфигурация средств защиты от НСД в соответствии с требованиями приказа ФСТЭК России № 17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» Класс защищенности информационной системы К1.
  + - * 1. Состав работ по внедрению средства доверенной загрузки:
* настройка общих параметров модулей на конечных устройствах 2-ого этапа создания ИС СОИ;
* настройка журналов на конечных устройствах 2-ого этапа создания ИС СОИ;
* регистрация токенов на конечных устройствах 2-ого этапа создания ИС СОИ.
  + - * 1. Состав работ по внедрению средства обнаружения вторжений:
* монтаж, подключение, проверка, первоначальная инициализация на площадках Резервного узла ИС СОИ;
* скачивание и обновление сигнатур;
* настройка политик IDS;
* отладка политик;
* постановка решения на мониторинг.
  + - 1. Проведение опытной эксплуатации 2-го этапа создания ИС СОИ

Опытная эксплуатация проводится по разработанной и согласованной программе и методике опытной эксплуатации. Задачей на данном этапе является выявление дефектов работы системы и последующее их устранение. По результатам опытной эксплуатации принимают решение о готовности предъявления компонентов ИC СОИ в рамках создания Резервного узла ИС СОИ на приемочные испытания, или о необходимости доработки. Завершение опытной эксплуатации фиксируется подписанием протокола опытной эксплуатации.

* + - 1. Проведение приёмочных испытаний 2-го этапа создания ИС СОИ

Приемочные испытания проводят в соответствии с разработанной и согласованной программой и методикой приемочных испытаний. Приемочные испытания проводятся для определения соответствия ИС СОИ в рамках 2-ого этапа создания Резервного узла ИС СОИ техническому заданию и решения вопроса о возможности приемки в постоянную эксплуатацию.

Результаты испытаний, предусмотренных программой и методикой испытаний, фиксируют в протоколах.

Приемочные испытания завершаются оформлением и утверждением заключения о возможности приемки Резервного узла ИС СОИ в постоянную эксплуатацию.

По результатам выполнения работ Исполнитель предоставит Заказчику полный комплект документации СОИ и КСОИБ СОИ (в соответствии с этапом 2.2 «Создание Резервного узла ИС СОИ, включая Комплексную систему обеспечения информационной безопасности» Календарного плана выполнения работ по созданию ИС СОИ, приведённого в Приложении № 2 к Договору) и систему в целом, реализующую утверждённый функционал 2-ого этапа создания ИС СОИ в полном объёме и отвечающую требованиям технического задания.

* + 1. Содержание работ по аттестации ИС СОИ

Работы по аттестации ИС СОИ в объёме 2-ого этапа создания ИС СОИ (объекта информатизации) должны включать:

1. Проведение обследования объекта информатизации.
2. Подготовка объекта информатизации к аттестационным испытаниям.
3. Проведение аттестации и разработка аттестационной документации для ИС СОИ в объёме 2-ого этапа создания ИС СОИ.

В ходе обследования Исполнитель должен уточнить (проанализировать) для ИС СОИ в объёме 2-ого этапа создания ИС СОИ следующую информацию:

* технологические процессы обработки информации;
* состав программного обеспечения, используемого при обработке информации;
* общесистемные и прикладные программные средства;
* состав средств и размещения объекта информатизации относительно контролируемой зоны;
* физические и логические связи между компонентами ИС СОИ в объёме 2-ого этапа создания ИС СОИ;
* физические и логические связи между ИС СОИ в объёме 2-ого этапа создания ИС СОИ и другими информационными системами, в том числе с сетями общего пользования;
* провести анализ состава организационно-распорядительной и нормативной документации, а также проверить наличие установленных сертифицированных средств защиты информации и их настроек.

В рамках подготовки ИС СОИ в объёме 2-ого этапа создания ИС СОИ к аттестационным испытаниям, Исполнитель должен разработать (актуализировать) Технический паспорт для ИС СОИ. Технический паспорт должен быть разработан в соответствии с Приказом ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

В ходе аттестации на соответствие требованиям безопасности информации ИС СОИ в объёме 2-ого этапа создания ИС СОИ, Исполнитель обязан:

1. Разработать документ «Программа и методики аттестационных испытаний».
2. Провести аттестационные испытания в соответствии с разработанной Программой и методикой испытаний.
3. Оформить Протокол по результатам аттестационных испытаний.
4. Оформить заключение по результатам аттестационных испытаний.

Программа и методика проведения аттестационных испытаний должна быть разработана в соответствии с Приказом Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну», ГОСТ РО 0043-004-2013 и согласована с Заказчиком до начала проведения аттестационных испытаний системы на соответствие требованиям безопасности информации.

Аттестация на соответствии требованиям безопасности информации ИС СОИ должна выполняться в соответствии со следующими нормативными документами:

* Приказ ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;
* Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

По результатам выполнения работ по аттестации ИС СОИ в объёме 2-ого этапа создания ИС СОИ, должны быть разработаны следующие документы:

* Технический паспорт;
* Программа и методики аттестационных испытаний;
* Протокол проведения аттестационных испытаний;
* Заключение по результатам аттестационных испытаний;
* Аттестат соответствия требованиям по безопасности информации  
  (Аттестат выдается только при успешном прохождении аттестационных испытаний и положительном Заключении. При отрицательном результате проведения аттестационных испытаний выдаётся Заключение с соответствующими выводами).
* Акт о приемке ИС СОИ в объёме 2-ого этапа создания ИС СОИ в постоянную эксплуатацию (выдается только при успешном прохождении аттестационных испытаний и положительном Заключении).

1. Срок, место и условия выполнения работ
   1. Сроки выполнения работ

Сроки выполнения работ определены в Календарном плане выполнения работ по созданию ИС СОИ (Приложение № 2 к Договору).

Срок оказания услуг определен в Календарном плане оказания услуг (Приложение № 3 к Договору).

* 1. Место и условия выполнения работ

Работы по актуализации технического задания, проектной и рабочей документации на создание ИС СОИ, разработке и модификации ПО выполняются на территории Исполнителя, за исключением работ, связанных с обработкой сведений ограниченного распространения. Перечень таких работ определяется Заказчиком.

Заказчик согласовывает доступ специалистов Исполнителя на территорию выполнения работ в соответствии с установленным в Федеральной службе по финансовому мониторингу и МУМЦФМ порядком на основании обоснованного письменного запроса Исполнителя.

Для допуска каждого специалиста Исполнитель предоставляет Заказчику следующие сведения: фамилия, имя, отчество, копия паспорта.

Специалисты Исполнителя в составе, согласованном Заказчиком, в течение 3 (трех) рабочих дней с момента согласования проходят ознакомление с нормативными правовыми актами, устанавливающими правила обращения со сведениями (информацией) на площадках Заказчика.

Для выполнения работ по актуализации технического задания, проектной и рабочей документации на создание ИС СОИ, разработке и модификации ПО на территории Заказчика, Заказчик предоставляет Исполнителю обоснованное количество рабочих мест, инфраструктуру (программные и технические средства разработки и документирования) и документацию на создаваемые программные компоненты.

Место выполнения работ:

* Здание Центрального узла ИС СОИ по адресу: 107450, г. Москва, ул. Мясницкая, дом 39, стр. 1;
* Здание Резервного узла ИС СОИ по адресу: 119017, г. Москва, Старомонетный пер., д. 31, стр. 1.

1. Требования к реализации основного функционала ИС СОИ
   1. Требования к функциям, выполняемым СОИ

В рамках создания ИС СОИ планируется реализация базового функционала компонентов:

* Компонент сетевого взаимодействия;
* Компонент авторизации пользователей;
* Компонент учета взаимодействующих организаций, объединений и их представителей;
* Компонент оповещения пользователей о значимых событиях (перечень событий определяется на этапе проектирования);
* Компонент логирования действий пользователей.

Компонент сетевого взаимодействия

Компонент сетевого взаимодействия ИС СОИ должен обеспечивать Зашифрованный сетевой обмен между абонентским пунктом (конечным устройством в стране-участнике взаимодействия с установленным ПО для сетевого взаимодействия с Центральным/Резервным узлом ИС СОИ) и Центральным/Резервным узлом (главным компонентом ИС СОИ, расположенным на площадках Заказчика и являющимся точкой подключения абонентских пунктов).

Компонент авторизации пользователей

Компонент авторизации пользователей должен обеспечивать:

* управление учетными записями участников, подключенных к ИС СОИ;
* управление доступом ИС СОИ.

Компонент учета взаимодействующих организаций и объединений

Компонент учета взаимодействующих организаций и объединений ИС СОИ должен обеспечивать:

* учет перечня взаимодействующих организаций, объединений и их представителей;
* учет возможностей маршрутизации сообщений между участниками информационного обмена.

Компонент оповещения пользователей о значимых событиях

Компонент оповещения пользователей о значимых событиях ИС СОИ должен обеспечивать:

* формирование событий и направление информации о событии путем оповещения пользователя о произошедших значимых событиях в ИС СОИ;
* визуальное оповещение пользователя о значимых событиях в ИС СОИ, при наличии подключения пользователя к ИС СОИ в текущий момент.

Компонент логирования действий пользователей.

Компонент логирования действий пользователей ИС СОИ должен обеспечивать отслеживание и запись активности, совершаемой пользователями во время работы с ИС СОИ.

* 1. Требования к функциям, выполняемых КСОИБ СОИ

Требования к функциям средства защиты каналов связи

Средство защиты каналов связи должно реализовывать следующие функции обеспечения ИБ:

* шифрование/расшифрование сетевых пакетов или сетевого трафика;
* передача информации по защищенным каналам связи c использованием криптографических протоколов;
* идентификация и аутентификация пользователей при доступе к сети ИС СОИ;
* обмен сообщениями и шифрованными файлами по криптографически защищённым каналам связи;
* создание криптографически защищенных каналов между объектами и пользователями для защиты передаваемой информации за пределами контролируемой зоны;
* контроль целостности передаваемой информации на основе использования криптографических методов защиты информации;
* обеспечение целостности файлов (данных), передаваемых между защищаемыми сегментами сети;
* регистрация попыток доступа к сетевым компонентам сегмента ИС СОИ.

Требования к функциям средства межсетевого экранирования.

Средство межсетевого экранирования должно реализовывать следующие функции обеспечения ИБ:

* сегментирование сети ИС СОИ;
* фильтрация потоков информации на границе ИС СОИ с использованием информации в полях заголовков сетевого и транспортного уровней;
* поддержка возможности отказоустойчивой конфигурации (кластеризация) с объединением в кластер в режиме Active/Standby;
* поддержка трансляции сетевых адресов (NAT);
* поддержка возможности администрирования на основе ролей;
* поддержка протоколов динамической маршрутизации;
* управление функциями системы посредством веб-интерфейса;
* поддержка возможности удаленного управления посредством протокола SSH;
* обеспечение сокрытия структуры и топологии внутренней сети;
* протоколирование событий сетевого доступа;
* регистрация попыток доступа к сетевым компонентам ИС СОИ.

Требования к функциям средства контроля защищённости и соответствия стандартам.

Средство контроля защищённости и соответствия стандартам должно реализовывать следующие функции обеспечения ИБ:

* инвентаризация ресурсов локальной вычислительной сети и обнаружение новых сетевых узлов;
* сканирование сети в целях выявления уязвимостей;
* генерация отчетов по результатам сканирования.

Требования к функциям средства сбора и анализа событий

Средство сбора и анализа событий должно реализовывать следующие функции обеспечения ИБ:

* централизованное хранение событий ИБ;
* сбор событий ИБ от средств защиты информации, а также информационной и телекоммуникационной инфраструктуры;
* нормализация данных (приведение данных к единому виду);
* фильтрация данных по заданным критериям и сохранение результатов фильтрации для последующего быстрого доступа к интересующим событиям ИБ;
* Бесшовные интеграции с различными системами (SIEM, IRP и пр.);
* Визуализация.

Требования к функциям средства защиты от несанкционированного доступа

Средство защиты от несанкционированного доступа должно реализовывать следующие функции обеспечения ИБ:

* Регистрация изменений полномочий доступа субъектов;
* Регистрация событий ИБ;
* Реализация замкнутой программной среды;
* Идентификация и аутентификация администраторов;
* Управление подключаемыми съемными носителями информации;
* Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти;
* Контроль доступа к защищаемой информации в соответствии с матрицей доступа;
* Идентификация узлов сети по логическим именам.

Требования к функциям средства доверенной загрузки.

Средство доверенной загрузки должно реализовывать следующие функции обеспечения ИБ:

* идентификация и аутентификация;
* проверка целостности ПО на основе использования криптографических методов защиты информации;
* обеспечение целостности программной среды;
* регистрация событий ИБ;
* регистрация изменений полномочий доступа субъектов.

Требования к функциям средства антивирусной защиты.

Средство антивирусной защиты должно реализовывать следующие функции обеспечения ИБ:

* централизованная защита от вредоносного ПО АРМ и хостов виртуальной инфраструктуры;
* сигнализация обнаружения вредоносного ПО;
* периодическое обновление средств антивирусной защиты и описаний известного вредоносного ПО;
* регистрация событий ИБ;
* автоматизированное оповещение ответственных лиц;
* регистрация событий вирусного заражении.

Требования к функциям средства обнаружения вторжений.

Средство обнаружения вторжений должно реализовывать следующие функции обеспечения ИБ:

* обнаружение сетевых атак на ИС СОИ;
* сигнализация обнаружения атаки;
* периодическое обновление баз сигнатур атак;
* построение отчетов об обнаруженных атаках в табличной форме.

1. Оказание услуг
   1. Оказание услуг по сопровождению Центрального узла ИС СОИ

Услуги должны оказываться в течении одного календарного года, начиная с 01.01.2025г.

Состав элементов Центрального узла ИС СОИ согласуется на 1-ом этапе создания ИС СОИ.

По завершению 1-ого этапа работ по созданию ИС СОИ с Заказчиком должно быть согласовано:

* Состав элементов Центрального узла ИС СОИ;
* Требования по SLA в рамках сопровождения Центрального узла ИС СОИ;
* Параметры определения Приоритета заявок на работы;
* Сроки реагирования и устранения неисправностей по каждому из элементов Центрального узла ИС СОИ;
* Требования к обеспечению бесперебойной работы по каждому элементу Центрального узла ИС СОИ;
* Требования к регламентно-профилактическим мероприятиям по каждому элементу Центрального узла ИС СОИ;
* Требования к мероприятиям по мониторингу здоровья элементов Центрального узла ИС СОИ.

Оказание услуг по сопровождению Центрального узла ИС СОИ должно осуществляться в соответствии с проектной документацией на СОИ и КСОИБ СОИ.

* + 1. Общие требования к услуге по сопровождению Центрального узла ИС СОИ

Исполнитель предоставляет сервис-менеджера по сопровождению ПО компонентов и подсистем ИС СОИ (далее – сервис-менеджер), являющегося для Заказчика единой точкой входа по следующим вопросам:

* обеспечение бесперебойной работы прикладного программного обеспечения компонентов и подсистем ИС СОИ;
* выполнение регламентно-профилактических мероприятий по обслуживанию прикладного программного обеспечения компонентов и подсистем ИС СОИ;
* обслуживание и сопровождения программно-технических средств, обеспечивающих работу компонентов и подсистем ИС СОИ.

В компетенцию сервис-менеджера не входят вопросы развития ПО компонентов и подсистем ИС СОИ.

К сопровождению подсистем и компонентов ИС СОИ, работе с оборудованием и ПО допускаются специалисты Исполнителя, ознакомленные с документацией на подсистемы и компоненты ИС СОИ, инструкциями на оборудование и методиками, принципами, правилами производителя оборудования.

Заказчик, при необходимости, может предоставить не более 3 рабочих мест работникам Исполнителя.

По согласованию с Заказчиком услуги могут оказываться без выезда специалиста на объект обслуживания.

* + - 1. Требования к обеспечению бесперебойной работы

Устранение нештатных ситуаций в функционировании системы должно выполняться с 9-00 до 18-00 по рабочим дням (если иное время не указано в соответствующих разделах настоящих технических требований) в соответствии с Регламентом по обеспечению бесперебойной работы ИС СОИ и проведению регламентно-профилактических мероприятий.

Устранение нештатных ситуаций в функционировании программно-технических средств, обеспечивающих работу компонента должно выполняться 24 часа в сутки, 7 дней в неделю.

* + - 1. Требования к регламентно-профилактическим мероприятиям

Исполнитель должен обеспечить выполнение регламентно-профилактических мероприятий на компонентах, подсистемах ИС СОИ, соответствующих базах данных и программно-технических средствах, обеспечивающих функционирование и доступность компонентов, подсистем ИС СОИ с 9.00 до 18.00 по рабочим дням в соответствии с настоящими Техническим заданием и эксплуатационной документацией на каждый компонент/подсистему ИС СОИ.

* + - 1. Требования к мероприятиям по обслуживанию и сопровождению

Мероприятия по обслуживанию и сопровождению программно-технических средств, обеспечивающих работу компонентов и предназначенных для неавтоматизированной обработки сведений, должны включать в себя следующие мероприятия, выполняемые специалистами Исполнителя:

* обновление по запросу Заказчика ПО, в том числе предоставляемого Заказчиком;
* регулярное поддержание в актуальном состоянии данных, и содержащих перечень и характеристики обслуживаемых программно-технических средств, и ежеквартальное предоставление этих данных Заказчику;
* ежедневные мониторинг, тестирование, диагностика оборудования и ПО, обеспечивающих работу компонентов;
* по необходимости оптимизация производительности программно-технических средств;
* ежедневный контроль настроек, в том числе и в части защиты информации;
* ежедневный контроль технического состояния и конфигураций поддерживаемого ПО и программно-технических средств;
* ежедневный анализ корректности работы поддерживаемой конфигурации оборудования и ПО;
* оказание услуг по сопровождению (включая внесение изменений в программный код) программно-технических средств, настройке новых схем и конфигураций, повышающих производительность и отказоустойчивость.
  1. Оказание услуг по мониторингу состояния защищенности и обеспечению кибербезопасности ИС СОИ

Услуги должны оказываться в течении одного календарного года, начиная с 01.01.2025г.

В рамках данного Технического задания осуществляется оказание Услуг по мониторингу состояния защищенности и обеспечению кибербезопасности ИС СОИ, включая реагирование на инциденты ИБ Заказчика путем непрерывного мониторинга и выявления инцидентов ИБ, оперативного реагирования, проведения технического анализа выявленных инцидентов ИБ, выяснения причин возникновения инцидентов ИБ, составления периодической отчётности, реализация обмена информацией о компьютерных инцидентах с ГосСОПКА, а также прогнозирование компьютерных атак на ИС СОИ.

В состав работ входит:

* мониторинг инцидентов ИБ;
* информационный обмен с ГосСОПКА;
* расследование инцидентов ИБ;
* реагирование на выявленные инциденты ИБ;
* предоставление оперативной и регулярной плановой отчетности;
* разработка отчета о состоянии защищенности Центрального узла ИС СОИ;
* подготовка отчетных документов, необходимых для закрытия этапа;
* отправка Заказчику документов, необходимых для закрытия этапа.
  + 1. Требования к услуге по мониторингу состояния защищенности и обеспечению кибербезопасности ИС СОИ
       1. Мониторинг событий ИБ.

При мониторинге инцидентов ИБ, зафиксированных центром мониторинга Исполнителя должно осуществляться:

* выявление и регистрация инцидентов ИБ в соответствии с SLA, зафиксированных центром мониторинга Исполнителя на основании сценариев обнаружения. Список сценариев и критичность согласовывается с Заказчиком на этапе подключения;
* выявление основных точек мошенничества и злоупотребления полномочиями, зафиксированными в ключевых бизнес-системах;
* первичная обработка выявленного инцидента ИБ: регистрация инцидента, базовая диагностика (обработка ложных срабатываний сценария), уточнение критичности, информирование Заказчика о факте обнаружения инцидента;
* анализ инцидента ИБ: установление причин и источника инцидента, передача информации Заказчику.

При реагировании на выявленные инциденты ИБ должно осуществляться:

* информирование ответственного специалиста (группы) Заказчика о факте обнаружения инцидента;
* разработка технических мер по блокированию инцидента (при технической возможности);
* сбор и обработка дополнительной информации по запросу уполномоченных специалистов Заказчика в рамках расследования инцидентов;
* участие в процессе нейтрализации последствий инцидента (при необходимости и технической возможности).

Экспертный анализ событий ИБ объекта Заказчика, переданных в центр мониторинга Исполнителя включает в себя, но не ограничивается следующими критериями:

* анализ событий, обрабатываемых центром мониторинга Исполнителя, для выявления аномалий, потенциально являющихся инцидентами, но не соответствующих текущим сценариям обнаружения инцидентов;
* доработка существующих сценариев обнаружения инцидентов для снижения количества ложных срабатываний;
* ретроспективный анализ событий и выявленных инцидентов для оценки общего уровня защищенности объекта Заказчика;
* расширение списка контролируемых сценариев обнаружения инцидентов в рамках внутренних исследований Исполнителя.

Изменение профиля Услуг по запросам Заказчика включает в себя:

* подключение/отключение источников, в случае необходимости;
* разработка новых коннекторов для подключения источников;
* выполнение запросов на реализацию новых сценариев обнаружения инцидентов, нетиповых отчетов или dashboard;
* изменение показателей критичности для сценариев обнаружения инцидентов.

Оказание Услуг по сопровождению и обеспечению доступности ядра средства сбора и анализа событий ИБ включает в себя, но не ограничивается:

* обеспечение работоспособности и доступности средства сбора и анализа событий ИБ;
* обеспечение совместно с Заказчиком, работоспособности и доступности сервера сбора событий на площадке Заказчика;
* обеспечение совместно с сотрудниками Заказчика, работоспособности канала передачи информации между сервером сбора событий и ядром средства сбора и анализа событий ИБ;
* администрирование средства сбора и анализа событий ИБ Заказчика, в том числе базы данных инцидентов.
  + - 1. Информационный обмен с ГосСОПКА:

Круглосуточное оперативное двухстороннее взаимодействие с Главным центром ГосСОПКА по следующим направлениям:

* + Выполнение реагирования и расследования выявляемых на инфраструктуре инцидентов совместно с Главным центром ГосСОПКА;
  + Обработка запросов Главного центра ГосСОПКА по проверке состояния инфраструктуры и выдаче рекомендаций по превентивному противодействию атаке – в течение 3-х часов с момента поступления запроса при наличии технической возможности;
  + Выдача рекомендаций по адаптации механизмов защиты инфраструктуры согласно информации о возможных векторах атаки, получаемой из Главного центра ГосСОПКА – в течение 2-х часов с момента поступления информации при наличии технической возможности.
    - 1. Расследование инцидентов ИБ:
* Глубокий анализ инцидентов:
  + Уточнение границ инцидента – задействованных активов и систем;
  + Идентификация и уточнение информации об атакующем;
  + Восстановление и уточнение хронологии инцидента;
  + Установление возможных причин инцидента;
* Формирование рекомендаций по дальнейшему реагированию (сдерживанию, устранению и восстановлению) на инциденты и недопущению их повторений.
  + - 1. Реагирование на выявленные инциденты ИБ:
* Изоляция инцидента на подконтрольных СЗИ с целью предотвращения дальнейшего распространения и подавление причин возникновения инцидента;
* Восстановление штатного режима работы подконтрольных СЗИ после успешного устранения инцидента ИБ – отмена выполненных темпоральных настроек в рамках реагирования на инцидент ИБ;
* Сбор и обработка дополнительной информации по запросу уполномоченных специалистов Заказчика.

Табл. Параметры оказания Услуг

|  |  |  |
| --- | --- | --- |
| 1. **Мониторинг инцидентов ИБ** | | |
| Количество одновременно подключенных к SIEM источников | Количество источников (серверов, АРМ, сетевых устройств, СЗИ) и бизнес-приложений уточняется по результатам 1-ого этапа создания ИС СОИ | |
| Длительность хранения собранных событий | активный поиск – 3 месяца  исторический архив – 1 год | |
| Аппаратная платформа для подсистемы сбора событий | предоставляется Заказчиком, требования к программно-аппаратному обеспечению:  - SIEM Agent – 8 vCPU / 32GB RAM / 1200GB HDD (из образа) | |
| Отказоустойчивость подсистемы сбора событий | обеспечивается Заказчиком | |
| Аппаратная платформа и лицензии на ПО для SIEM-системы в рамках услуги | предоставляется Исполнителем | |
| Отказоустойчивость для SIEM-системы | предоставляется Исполнителем | |
| **Время реакции в зависимости от критичности** | | |
| Время реакции на инцидент ИБ с момента его фиксации SIEM | Высокая критичность | не более 20 минут |
| Средняя критичность | не более 30 минут |
| Низкая критичность | не более 60 минут |
| Время базовой диагностики инцидента ИБ, выработки рекомендаций для нейтрализации инцидента и информирования Заказчика | Высокая критичность | не более 30 минут |
| Средняя критичность | не более 60 минут |
| Низкая критичность | не более 120 минут |
| Режим предоставления услуги | 24\*7 | |
| **Изменение профиля услуг** | | |
| Время выполнения работ по подключению новых типовых источников | 36 часов | |
| Время выполнения запроса на доработку политики выявления инцидентов ИБ | 84 часа | |
| **Обеспечение работоспособности платформы** | | |
| Период обслуживания платформы | 24\*7 | |
| Доступность ядра SIEM | Разовый простой | не более 16 часов |
| Доступность за квартал | не менее 98,5% |
| Количество технологических окон за квартал | не более 1 |
| Максимальная длительность технологического окна | не более 6 часов |
| Доступность системы сбора событий ИБ | Разовый простой | не более 24 часов |
| Доступность за квартал | не менее 97% |
| 1. **Расследование инцидентов ИБ** | | |
| Время реакции на инцидент ИБ с момента информирования Заказчика | Высокая критичность | не более 60 минут |
| Средняя критичность | не более 120 минут |
| Низкая критичность | не более 360 минут |
| Режим предоставления услуги | 24\*7 | |
| Условия обработки инцидентов в зависимости от уровня критичности | Высокий по умолчанию  Средний, Низкий по запросу | |
| 1. **Реагирование на инциденты ИБ** | | |
| Режим предоставления услуг | 24\*7 | |
| Параметр предоставления услуг | По запросу | |

1. Порядок приемки работ, требования к результатам работ и отчетным документам
   1. Общие требования к приемке работ

Приемка работ осуществляется по этапам Календарного плана выполнения работ по созданию ИС СОИ (Приложение № 2 к Договору).

Приемка работ по окончанию 1-ого этапа создания ИС СОИ осуществляется Комиссией в порядке, предусмотренном Договором.

Приемка работ по окончанию 2-ого этапа создания ИС СОИ осуществляется Комиссией в порядке, предусмотренном Договором.

* 1. Требования к документации на ИС СОИ

В рамках создания ИС СОИ должны быть разработаны/актуализированы следующие документы:

1. Техническое задание на создание ИС СОИ (включая КСОИБ СОИ);
2. Модель угроз и нарушителя безопасности информации ИС СОИ;
3. ОРД на ИС СОИ;
4. Комплект проектной документации ИС СОИ:
   1. Ведомость технического проекта (ТП);
   2. Ведомость покупных изделий (ВП);
   3. Схема организационной структуры (С0);
   4. Схема структурная комплекса технических средств (С1);
   5. Схема функциональной структуры (С2);
   6. Пояснительная записка к техническому проекту (П2);
   7. Описание информационного обеспечения системы (П5);
   8. Описание комплекса технических средств (П9);
   9. Описание программного обеспечения (ПА).
5. Комплект проектной документации КСОИБ СОИ:
   1. Ведомость технического проекта (ТП);
   2. Ведомость покупных изделий (ВП);
   3. Схема организационной структуры (С0);
   4. Схема структурная комплекса технических средств (С1);
   5. Схема функциональной структуры (С2);
   6. Пояснительная записка к техническому проекту (П2);
   7. Описание комплекса технических средств (П9);
   8. Описание программного обеспечения (ПА).
6. Комплект рабочей (исполнительной) документации на СОИ в составе:
   1. Ведомость эксплуатационной документации;
   2. Руководство пользователя (И3);
   3. Руководство администратора;
   4. Руководство администратора информационной безопасности;
   5. Технологическая инструкция (И2);
   6. Общее описание системы;
   7. Программа и методика опытной эксплуатации;
   8. Протокол опытной эксплуатации;
   9. Программа и методика приемочных испытаний;
   10. Протокол приемочных испытаний;
   11. Таблица доменных имен и IP-адресов.
7. Комплект рабочей (исполнительной) документации на КСОИБ СОИ в составе:
   1. Ведомость эксплуатационной документации;
   2. Руководство пользователя (И3);
   3. Руководство администратора;
   4. Руководство администратора информационной безопасности;
   5. Технологическая инструкция (И2);
   6. Общее описание системы;
   7. Программа и методика опытной эксплуатации;
   8. Протокол опытной эксплуатации;
   9. Программа и методика приемочных испытаний;
   10. Протокол приемочных испытаний;
   11. Таблица доменных имен и IP-адресов.
8. По результатам выполнения работ по аттестации ИС СОИ, должны быть предоставлены документы в составе:
   1. Технический паспорт;
   2. Программа и методики аттестационных испытаний;
   3. Протокол проведения аттестационных испытаний;
   4. Заключение по результатам аттестационных испытаний;
   5. Аттестат соответствия требованиям обеспечения информационной безопасности регуляторов и законодательства Российской Федерации (Аттестат выдается только при успешном прохождении аттестационных испытаний и положительном Заключении. При отрицательном результате проведения аттестационных испытаний выдаётся Заключение с соответствующими выводами);
   6. Акт о приемке ИС СОИ в объёме 1-ого (2-ого) этапа создания ИС СОИ в постоянную эксплуатацию (выдается только при успешном прохождении аттестационных испытаний и положительном Заключении).

Разрабатываемая техническая документация должна быть выполнена на русском языке.

Структура и содержание Технического задания на создание СОИ и КСОИБ СОИ должна соответствовать требованиям ГОСТ 34.602–2020 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

Структура и содержание технической документации на компоненты должны удовлетворять требованиям Приложения № 2 к Регламенту внедрения и сопровождения программных систем Федеральной службы по финансовому мониторингу № 02-00-06/13505 от 29.06.2015 (предоставляется Заказчиком).

Документы должны быть оформлены на листах формата А4 без рамки, основной надписи и дополнительных граф к ней, без шифра (номера документа).

Правила оформления документов должны быть предварительно согласованы с Заказчиком.

Документы предоставляются Заказчику в бумажном (2 экземпляра), а также в электронном виде на оптическом носителе (1 экземпляр).

1. Требования к Исполнителю работ и услуг

Деятельность по защите информации должна быть определена в Уставе (учредительных документах) Исполнителя как один из основных видов деятельности организации.

Исполнитель должен обладать следующими лицензиями ФСТЭК России:

1. на деятельность по технической защите конфиденциальной информации;
2. на деятельность по разработке и (или) производству средств защиты конфиденциальной информации.

Исполнитель должен обладать следующими лицензиями ФСБ:

На осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

Исполнитель должен иметь сертифицированную систему менеджмента качества в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО 9001-2015.

Исполнитель должен иметь в структуре компании выделенное подразделение, отвечающее за работы в области информационной безопасности.

Исполнитель должен иметь в структуре компании выделенное подразделение, отвечающее за поддержку и обслуживание внедряемых средств защиты в режиме 24/7.

Исполнитель должен иметь техническую лабораторию для моделирования проблемных ситуаций, которые могут возникнуть на программно-аппаратных комплексах, установленных у Заказчика.

Исполнитель должен иметь в штате сертифицированных специалистов, обладающих сертификатом Администратора системы защиты информации ViPNet

Исполнитель должен иметь в штате сертифицированных специалистов, обладающих сертификатом Kaspersky Certified System Engineer Level 1.2 (не менее двух).

Исполнитель должен иметь в штате сертифицированных специалистов, обладающих сертификатом ALCSA-1.7 Сертифицированный системный администратор Astra Linux Special Edition 1.7 (не менее трёх).

Исполнитель должен иметь в штате сертифицированных специалистов, обладающих сертификатом Certified Professional (CP) по продукту MaxPatrol SIEM (не менее пяти).