Приложение № 1 к Извещению

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

### Общие сведения

В ходе исполнения договора необходимо оказать услуги по созданию системы защиты информации в Государственном автономном учреждении Саратовской области «Комплексный центр социального обслуживания населения Краснокутского района» (далее – ГАУ СО КЦСОН Краснокутского района), а также провести аттестацию автоматизированных рабочих мест входящих в состав информационных систем (- далее ИС), обрабатывающих конфиденциальную информацию (персональные данные) и функционирующих в ГАУ СО КЦСОН Краснокутского района, по требованиям безопасности информации.

### Перечень объектов информатизации и состав ИС, обрабатывающих конфиденциальную информацию

Услуги оказываются для трех информационных систем:

1. Автоматизированная информационная система «Электронный социальный регистр населения» (АИС «ЭСРН») в составе 5 АРМ.

Все компоненты размещаются по адресу: 413235, Саратовская область, г. Красный Кут, ул. Садовая, дом 2

В информационных системах обрабатываются персональные данные граждан Российской Федерации. Режим обработки персональных данных в ИС – многопользовательский.

### Перечень документов, на основании которых оказываются услуги

1. Федеральный закон РФ от 27 июля 2006 г. №152-ФЗ «О персональных данных».
2. Федеральный закон РФ от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон РФ от 04 мая 2011 года № 99-ФЗ «О лицензировании отдельных видов деятельности».
4. Требования к защите персональных данных при их обработке в информационных системах персональных данных (утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119).
5. Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утверждены постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687).
6. Требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации (утверждены Постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676).
7. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21).
8. Приказ ФСБ России от 09 февраля 2005 г. №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».
9. Состав и содержание 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 (утверждены приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378).
10. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17).
11. Методический документ. Меры защиты информации в государственных информационных системах (утвержден ФСТЭК России 11 февраля 2014 г.).
12. ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения»
13. ГОСТ РО 0043-004-2012 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний»
14. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»
15. Методические документы. Профили средств защиты информации. Утверждены ФСТЭК России 2012-2017гг.

### Цели оказания услуг

Целями оказания услуг являются:

* выполнение требований Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных»;
* выполнение требований Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* выполнение требований иных нормативно-правовых актов Российской Федерации, документов ФСТЭК и ФСБ России, регламентирующих вопросы защиты персональных данных и иной конфиденциальной информации;
* обеспечение конфиденциальности, целостности и доступности, обрабатываемой в ИС ГАУ СО КЦСОН Краснокутского района информации;
* исключение несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать хищение, утрата, утечка, уничтожение, изменение, блокирование, копирование, распространение персональных данных;
* защита прав и законных интересов субъектов, чьи персональные данные обрабатываются в ИС ГАУ СО КЦСОН Краснокутского района

### Требования к порядку оказания услуг

Оказание услуг должно производиться этапами в следующем порядке:

1. Проведение предварительного анализа процессов обработки конфиденциальной информации и персональных данных в ГАУ СО КЦСОН Краснокутского района. Цель выполнения этапа – определение текущего состояния выполнения Заказчиком требований законодательства по защите конфиденциальной информации и персональных данных, определение состава технических и программных средств, функционирующих в ИС. Определение функционирующих средств защиты информации, их настроек и иных мер и методов, применяемых в целях обеспечения информационной безопасности.
	1. Определение состава защищаемой информации, а также перечня обрабатываемых персональных данных, целей и сроков обработки персональных данных, категорий обрабатываемых персональных данных, подразделений и должностных лиц, допущенных к обработке защищаемой информации.
	2. Определение порядка обработки защищаемой информации.
	3. Определение состава ИС, обрабатывающих защищаемую информацию, конфигурации компонентов ИС, их размещения относительно границ контролируемой зоны.
	4. Определение физических, функциональных и технологических связей между компонентами ИС.
	5. Проведение анализа мероприятий по организации обеспечения безопасности конфиденциальной информации и персональных данных в составе:
* анализ документации по вопросам обеспечения безопасности персональных данных, в т.ч. при их обработке в ИС.
* анализ мероприятий по размещению, специальному оборудованию, охране и режиму допуска в помещения, где ведется работа с персональными данными;
* анализ мероприятий по защите персональных данных от несанкционированного доступа;
1. Разработка необходимой организационно-распорядительной и эксплуатационной документации Заказчика, регламентирующей вопросы обработки и обеспечения безопасности конфиденциальной информации и персональных данных.
2. Определение актуальных угроз и возможностей нарушителя безопасности информации, обрабатываемой в информационных системах Заказчика. Определение угроз производится с учетом требований нормативных и руководящих документов ФСТЭК России с использованием Банка данных угроз. Поскольку в ряде ИС ГАУ СО КЦСОН Краснокутского района применяются криптографические средства защиты информации, определение возможностей нарушителя безопасности информации производится в том числе в соответствии с требованиями документов ФСБ России.
3. Создание системы защиты информации для информационных систем, указанных в разделе 2 настоящего технического задания.
	1. Формирование требований по защите информации в информационных системах (с учетом необходимости выполнения базового набора мер защиты, а также мер, направленных на нейтрализацию актуальных угроз безопасности информации)
	2. Формирование технического решения (в составе технического проекта), описывающего состав необходимых технических и организационных мер защиты, а также набора средств защиты информации, их функций и настроек, необходимых к использованию в информационных системах.
	3. Поставка недостающих у Заказчика средств защиты информации в соответствии с определенным в п.4.2 техническим решением.
	4. Установка, настройка, конфигурирование средств защиты информации (а также средств информатизации ИС) в соответствии с определенным в п.4.2 техническим решением. В случае необходимости в ходе проведения работ Исполнителем должна быть проведена коррекция настроек уже действующих на объекте информатизации средств защиты информации, в т.ч. криптографических (шифровальных) средств.
	5. Определение состава и методик проведения аттестационных испытаний по требованиям безопасности информации ИС ГАУ СО КЦСОН Краснокутского района.
	6. Проведение аттестационных испытаний ИС ГАУ СО КЦСОН Краснокутского района по требованиям безопасности информации.

**5.Параметры оказания услуг**

В результате оказания услуг, система защиты информации в целях получения оператором инструментов управления и контроля за процессами контроля информационной безопасности, а также нейтрализации угроз, должна быть оснащена необходимыми для этого подсистемами защиты информации и аттестована на соответствие требованиям к информационной безопасности.

Для оказания услуг Исполнителем Заказчик предоставляет автоматизированные рабочие места (АРМ) в количестве, определенном п.6 настоящего Технического задания, в состав которых входит оборудование, соответствующее характеристикам, не ниже следующих:

|  |  |
| --- | --- |
| **Оборудование, входящее в состав АРМ** | **Минимальные характеристики** |
| Процессор | Двухъядерный процессор с частотой ядра не менее 2 Ghz |
| Оперативная память | Не менее 4 Гб (в случае Windows 8/8.1), не менее 8 Гб (в случае Windows 10) |
| Жёсткий диск | Жесткий диск - не менее 160 Gb (файловая система NTFS), свободного места на системном разделе - не менее 25 процентов от общего объема |
| LAN интерфейс | 1 порт LAN 100mb/s |
| USB интерфейс | 1 свободный  порт USB |
| Видео | Наличие видеокарты стандарта VGA  |
| Клавиатура | Стандартная qwerty-клавиатура, совместимая с материнской платой системного блока АРМ |
| Мышь | Компьютерный манипулятор «мышь», совместимая с материнской платой системного блока АРМ |
| Монитор | Монитор стандарта VGA |
| Операционная система и ПО | Windows 10 (билд 1511,1607,1703,1709,1903,1909, 2004); Windows 8/8.1 Операционная система должна быть установленной не позднее 2021 года, не содержать вирусов и ошибок.  |

Заказчик до момента заключения Договора устанавливает на АРМ программное обеспечение (ПО), необходимое для работы сотрудников объекта. Установленное ПО не будет содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам.

Заказчик предоставляет:

* выход в интернет для данного АРМ (открытый порт UDP 55777) с минимальной скоростью подключения к сети интернет 256 kbit;
* источник бесперебойного питания, обеспечивающий работу АРМ при отключении электропитания в течение не менее 10 минут;
* документы, подтверждающие легальность установленной на АРМ операционной системы (Windows 10, 8, 8.1);
* План помещений, используемых Заказчиком, с указанием расположения АРМ;
* Юридический документ, подтверждающий право использования Заказчиком помещения, в котором расположено АРМ;
* Копию договора на обслуживание пожарной сигнализации помещения (здания);
* Документы, подтверждающие физическую охрану помещения (здания), в котором расположено АРМ;
* Состав технических средств, составляющих АРМ с указанием наименования и серийных номеров (Системный блок, клавиатура, мышь, принтер, монитор и т.д.);
* Перечень установленного программного обеспечения на АРМ;
* Перечень средств защиты с указанием номеров сертификатов, сроков действия сертификатов, регистрационных номеров средств защиты информации;
* Схему локально-вычислительной сети (взаимодействия АРМ с интернетом), с указанием установленных средств защиты информации на АРМ.

### Технические требования к разрабатываемой системе защиты информации

Точный состав и требования к функциям, реализуемым системой защиты информации, могут быть сформированы только по результатам определения актуальных угроз безопасности информации в соответствии с п. 3 раздела 5 настоящего технического задания. Однако, система защиты информации должна как минимум выполнять следующие базовые функции:

* Идентификация и аутентификация пользователей, являющихся работниками оператора.
* Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов.
* Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.
* Защита обратной связи при вводе аутентификационной информации.
* Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей.
* Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа.
* Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами.
* Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы.
* Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе).
* Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу.
* Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации.
* Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети.
* Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).
* Управление доступом к машинным носителям информации.
* Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания).
* Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения.
* Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти.
* Генерирование временных меток и (или) синхронизация системного времени в информационной системе.
* Защита информации о событиях безопасности.
* Реализация антивирусной защиты.
* Обновление базы данных признаков вредоносных компьютерных программ (вирусов).
* Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей.
* Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе.
* Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи.
* Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств.

Система защиты информации должна обеспечивать противодействие угрозам безопасности информации, определенным в Модели угроз. Компоненты системы защиты информации должны удовлетворять требованиям, предъявляемым к средствам защиты информации, используемым в ИСПДн с соответствующим уровнем защищенности обрабатываемых ПДн и государственных информационных системах соответствующего класса защищенности.

В соответствии с определенным классом и уровнем защищенности для ИС, в состав создаваемой системы защиты информации должны входить:

* подсистема защиты от несанкционированного доступа, регистрации и учета;
* подсистема криптографической защиты информации;
* подсистема межсетевого экранирования;
* подсистема антивирусной защиты;
* подсистема анализа и контроля защищенности.

### Требования по сертификации средств защиты информации

Средства защиты информации от несанкционированного доступа должны иметь действующий сертификат соответствия ФСТЭК России на соответствие требованиям документов «Защита от несанкционированного доступа к информации. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – не ниже 4 уровня контроля, «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – не ниже 5 класса защищенности, классу защиты не ниже СКН ИТ.СКН.П4.ПЗ.

Средства межсетевого экранирования должны иметь действующий сертификат на соответствие требованиям ФСТЭК России к межсетевым экранам типа «В» четвертого класса защиты.

Средства криптографической защиты информации должны иметь действующий сертификат на соответствие требованиям ФСБ России к шифровальным (криптографическим) средствам класса – не ниже КС2 и наличие возможности использования для криптографической защиты (шифрования и имитозащиты IP-трафика) информации.

Средства антивирусной защиты должны иметь действующий сертификат соответствия ФСТЭК России на соответствие требованиям документов не ниже «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа А второго класса защиты. ИТ.САВЗ.А2.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Б второго класса защиты. ИТ.САВЗ.Б2.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа В второго класса защиты. ИТ.САВЗ.В2.ПЗ» (ФСТЭК России, 2012) «Профиль защиты средств антивирусной защиты типа Г второго класса защиты. ИТ.САВЗ.Г2.ПЗ» (ФСТЭК России, 2012).

Средства анализа защищенности должны соответствовать требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – не ниже 4 уровня контроля при соблюдении технических условий.

### Сведения о разрабатываемой документации

В ходе оказания услуг должны быть разработаны следующие документы:

1. Проект организационно-распорядительной документации Заказчика, регламентирующей защиту информации и персональных данных в составе, как минимум для каждой ИС должен включать:
* Акт классификации.
* Акт определения уровня защищенности.
* Приказ о назначении ответственного за обеспечение безопасности и обработку персональных данных.
* Порядок резервного копирования персональных данных.
* Приказы о допуске сотрудников к обработке ПДн в ИСПДн.
* Порядок действия во внештатных ситуациях.
* Инструкция администратора.
* Инструкция пользователя.
* Инструкция по парольной защите.
* Инструкция по антивирусной защите.
* Технический паспорт.
1. Модель угроз и нарушителя безопасности информации, обрабатываемой в информационных системах:
* Описание методического подхода к моделированию угроз безопасности информации.
* Общий перечень угроз безопасности информации при их обработке в ИС.
* Результаты определения актуальности угроз безопасности информации.
* Описание методологии формирования модели нарушителя.
* Описание нарушителей.
* Предположения об имеющейся у нарушителя информации об объектах атак.
* Предположения об имеющихся у нарушителя средствах атак.
* Описание каналов атак.
* Предположения о потенциале нарушителя.
* Определение типа нарушителя.
1. Техническое задание на создание системы защиты информации.
2. Технический проект на систему защиты информации.
3. Программа и методики аттестационных испытаний ИС.
4. Протоколы проведения испытаний.
5. Заключения по результатам аттестационных испытаний.
6. Аттестаты соответствия.

Вся документация представляется Заказчику распечатанной и сброшюрованной, а также (дополнительно) в электронном виде в формате Microsoft Word. Документация выполняется на русском языке с учетом требований законодательства и государственных стандартов РФ.

### Требования по эксплуатации и техническому обслуживанию

Размещение оборудования, технических средств должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности.

Исполнитель обеспечивает гарантийное техническое обслуживание на протяжении 12 месяцев с момента ввода системы защиты информации в действие. Гарантийное техническое обслуживание включает в себя:

* Внесение необходимых изменений в документацию, подготовленную Исполнителем, а также в состав средств защиты информации, входящих в систему защиты информации, в случае наличия замечаний со стороны ФСТЭК или ФСБ России в рамках выполнения мероприятий, предусмотренных п. 3 части II Требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации (утверждены Постановлением Правительства Российской Федерации от 6 июля 2015 г. №676).
* Реагирование на сбои в работе СЗИ по заявке Заказчика в течение одного рабочего дня.

### Условия оказания услуг

Услуги оказываются в условиях постоянной эксплуатации существующих объектов Заказчика. Технология оказания услуг не должна существенно затруднять текущую работу Заказчика. При формировании требований к системе защиты персональных данных учитываются имеющиеся у Заказчика средства защиты, структура существующей инфраструктуры объекта.

Заказчик обязуется предоставить Исполнителю всю информацию, необходимую для оказания услуг согласно Технического задания, доступ специалистов Исполнителя к необходимому для оказания услуг оборудованию, программному обеспечению и техническим средствам на территории Заказчика и обеспечить контакт с техническими специалистами Заказчика.

### Порядок контроля и приёмки услуг

Испытания системы защиты информации ИС проводятся на объекте Заказчика. Заказчик вправе привлекать для оценки качества оказанных Исполнителем услуг третьих лиц, являющихся специалистами в области защиты информации. Подобная оценка качества осуществляется в рамках действующего законодательства РФ и проводится за счет Заказчика.

### 11. Требования по обеспечению режима конфиденциальности

### при оказании услуг

Информация и документация, получаемые в ходе оказания услуг, считаются конфиденциальными, и Исполнитель обязуется не разглашать их без согласия Заказчика третьим лицам кроме случаев, предусмотренных законодательством Российской Федерации.

### 12. Требования к исполнителю

1. Исполнитель должен иметь лицензии, предусмотренную Федеральным законом Российской Федерации 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»:

1.1. на осуществление деятельности по технической защите конфиденциальной информации с перечнем работ и услуг, на которые распространяется лицензия:

* установка, монтаж, испытания, ремонт средств защиты информации (программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации).
* аттестационные испытания и аттестация на соответствие требованиям по защите информации: средств и систем информатизации.

1.2. на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание 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) по следующим пунктам Приложения к Постановлению Правительства Российской Федерации от 16 апреля 2012 г. N 313 «Перечень выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств»:

* пункт 12. Монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств.
* пункт 20. Работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).
* пункт 21. Передача шифровальных (криптографических) средств.

2. Оказать услугу в полном объеме с обязательным выездом специалистов Исполнителя на объекты Заказчика.

3. Исполнитель обязуется:

* не проводить противозаконные действия по сбору, использованию и передаче третьей стороне информации, циркулирующей и хранящейся в ИС;
* не осуществлять НСД к информационным ресурсам ИС;
* не проводить незаконное копирование информации, циркулирующей или хранящейся в ИС;
* не предпринимать манипулирование информацией, циркулирующей или хранящейся в ИС (фальсифицировать, модифицировать, подделывать, блокировать, уничтожать или искажать информацию);
* не нарушать технологию сбора, накопления, хранения, обработки, преобразования, отображения и передачи информации, в результате чего может быть осуществлено искажение, потеря или незаконное использование информации;
* не устанавливать в ИС программы-вирусы (загрузочные, файловые и др.);
* не устанавливать программные и аппаратные закладные устройства в технические средства в ИС;
* не устанавливать в технические средства ИС программное обеспечение, зараженное вирусами;
* не распространять конфиденциальную информацию об оказанных услугах и полученных результатах.