ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на выполнение работ по созданию подсистемы защиты информации муниципальной автоматизированной системы централизованного оповещения населения на территории городского округа город-герой Волгоград

1. Общие сведения

1.1. Наименование

Выполнение работ по созданию подсистемы защиты информации муниципальной автоматизированной системы централизованного оповещения населения на территории городского округа город-герой Волгоград.

1.2. Наименование Заказчика работ

Публичное акционерное общество «Ростелеком»

Место нахождения заказчика: Юридический адрес: 191167, город Санкт-Петербург, вн.тер.г. муниципальный округ Смольнинское, Наб Синопская, д. 14 Литера А

Почтовый адрес: 400066, г. Волгоград, ул. Мира, дом 16.

Адрес электронной почты: vlg@south.rt.ru

Номер контактного телефона: 8 (8442) 30-40-92

1.3. Сроки выполнения работ

Выполнение Работ разделено на два этапа:

1 этап: с даты заключения Договора до 28.12.2023;

2 этап: с 29.12.2023 г. до 28.12.2024 г.

1.4. Основания для выполнения работ по созданию муниципальной автоматизированной системы централизованного оповещения

Указ Президента Российской Федерации от 13 ноября 2012 года № 1522 «О создании комплексной системы экстренного оповещения населения об угрозе возникновения или о возникновении чрезвычайных ситуаций».

Федеральные законы:

от 21 декабря 1994 г. № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера»;

от 12 февраля 1998 г. № 28-ФЗ «О гражданской обороне»;

от 7 июля 2003 г. № 126-ФЗ «О связи»;

от 6 октября 2003 г. № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации».

Постановления Правительства Российской Федерации:

от 30 декабря 2003 г. № 794 «О единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций»;

от 26 ноября 2007 г. № 804 «Об утверждении Положения о гражданской обороне в Российской Федерации»;

от 2 апреля 2020 г. № 417 «Об утверждении Правил поведения обязательных для исполнения гражданами и организациями, при введении режима повышенной готовности или чрезвычайной ситуации»;

от 22 мая 2008 г. № 381 «О порядке предоставления участков для установки и (или) установки специализированных технических средств оповещения и информирования населения в местах массового пребывания людей»;

от 17 мая 2023 г. № 769 «О порядке создания, реконструкции и поддержания в состоянии постоянной готовности к использованию систем оповещения населения».

Совместные приказы министерств и ведомств Российской Федерации:

Приказ МЧС России и Минкомсвязи России от 31 июля 2020 г. № 578/365 «Об утверждении Положения о системах оповещения населения» (Далее – Положение о системах оповещения населения);

Приказ МЧС России и Минкомсвязи России от 31 июля 2020 г. № 579/366 «Об утверждении Положения по организации эксплуатационно-технического обслуживания систем оповещения населения».

Приказы МЧС России, МВД России и ФСБ России:

от 31 мая 2005 г. №428/432/321 «О порядке размещения современных технических средств массовой информации в местах массового пребывания людей в целях подготовки населения в области гражданской обороны, защиты от чрезвычайных ситуаций, обеспечения пожарной безопасности и охраны общественного порядка, а также своевременного оповещения и оперативного информирования граждан о чрезвычайных ситуациях и угрозе террористических акций» (зарегистрирован в Минюсте России, регистрационный номер 6700 от 9 июня 2005 г.);

от 28 октября 2008 г. № 646/919/526 «Об утверждении Требований по установке специализированных технических средств оповещения и информирования населения в местах массового пребывания людей» (зарегистрирован в Минюсте России, регистрационный номер 13001 от 26 декабря 2008 г.).

Приказ Минтруда России от 15.12.2020 № 903н «Об утверждении Правил по охране труда при эксплуатации электроустановок" (зарегистрирован в Минюсте России 30.12.2020 № 61957).

Методические рекомендации:

Методические рекомендации по созданию (реконструкции) и совершенствованию систем оповещения населения, утвержденных протоколом заседания рабочей группы Правительственной комиссии по предупреждению и ликвидации чрезвычайных ситуаций и обеспечению пожарной безопасности по координации создания и поддержания в постоянной готовности систем оповещения населения от 19.02.2021 № 1 (далее – Методические рекомендации).

Национальный стандарт Российской Федерации ГОСТ Р 42.3.01-2021 «Гражданская оборона. Технические средства оповещения населения. Классификация. Общие технические требования»;

Межгосударственный стандарт ГОСТ 34.602-2020 "Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы";

Национальный стандарт Российской Федерации ГОСТ Р 55199-2012 «Гражданская оборона. Оценка эффективности топологии оконечных устройств оповещения населения. Общие требования».

1.5. Термины и определения

АРМ ОД – программно-аппаратный комплекс пункта управления оповещением РАСЦО;

АРМ ОД ЗПУ – программно-аппаратный комплекс запасного пункта управления оповещением;

АРМ ОД ОПУ ЕДДС – программно-аппаратный комплекс основного пункта управления оповещением РАСЦО в единой дежурно-диспетчерской службе;

АРМ ОД ОПУ – программно-аппаратный комплекс основного пункта управления оповещением РАСЦО;

ГО и ЧС – гражданская оборона и чрезвычайные ситуации;

ЕДДС – единая дежурно-диспетчерская служба;

ЗПУ – запасной пункт управления;

ИБ – информационная безопасность;

КГО – комплекс голосового оповещения населения;

КСЭОН – комплексная система экстренного оповещения населения;

МАСЦО - муниципальная автоматизированная система информирования и оповещения населения, создаваемая на территории одного муниципального района или городского округа Волгоградской области;

ОПУ – основной пункт управления;

ПО – программное обеспечение;

ПЗИ – подсистема защиты информации;

РАСЦО – региональная автоматизированная система централизованного оповещения Волгоградской области;

РСЧС – единая государственная система предупреждения и ликвидации чрезвычайных ситуаций;

СЗИ – программные и аппаратные средства защиты информации;

СКЗИ – средства криптографической защиты информации;

Система-112 – система обеспечения вызова экстренных оперативных служб по единому номеру «112» на территории Волгоградской области;

СОВ - система обнаружения и предотвращения вторжений;

ССОП – сеть связи общего пользования;

СПО – специальное программное обеспечение;

ТУ – технические условия;

Центральный сервер РАСЦО – специализированное программное обеспечение автоматизированной системы информирования и оповещения населения, установленное на сервере РАСЦО, расположенном в Едином центре обработке данных Волгоградской области по адресу г. Волгоград, ш. Авиаторов, 2;

IP/MPLS – механизм в высокопроизводительной телекоммуникационной сети, осуществляющий передачу данных от одного узла сети к другому с помощью меток;

VPN – виртуальная частная сеть.

2. Цель создания МАСЦО

Обеспечение доведения сигналов оповещения и экстренной информации до населения, органов управления и сил ГО и РСЧС городского округа город-герой Волгоград в автоматизированном режиме функционирования.

Обеспечение программного сопряжения комплексов оповещения МАСЦО и региональной автоматизированной системой централизованного оповещения населения (далее – РАСЦО) Волгоградской области.

Использование современных средств и технической аппаратуры оповещения, электронных средств информирования для своевременного и гарантированного доведения сигналов оповещения и экстренной информации до населения городского округа город-герой Волгоград или его отдельных территорий.

Управление оконечными средствами оповещения и информирования с пунктов управления РАСЦО и МАСЦО.

Обеспечение возможности дальнейшего развития МАСЦО на базе современных технических средств с использованием мультисервисных решений, учитывающих текущее состояние и дальнейшее развитие цифровых сетей связи и передачи данных.

3. Необходимые сведения о пунктах управления действующих РАСЦО и КСЭОН

РАСЦО Волгоградской области функционирует на базе оборудования П-166 ИТК ОС и П-166. В состав РАСЦО входит:

- Центральный сервер системы и расположен по адресу г. Волгоград, шоссе Авиаторов, дом 2;

- Пункт управления 1. АРМ ОД ОПУ дежурно-диспетчерской службы Волгоградской области, расположенное по адресу г. Волгоград, шоссе Авиаторов, дом 2;
- Пункт управления 2. АРМ ОД ЗПУ, расположенное в запасном пункте управления (адрес предоставляется по запросу);
- Пункт управления 3. АРМ ОД ОПУ ЕДДС расположенное по адресу, г. Волгоград, улица Канунникова, дом 16.

Действующие пункты управления РАСЦО Волгоградской области имеют сопряжение с телефонной сетью общего пользования через телекоммуникационную подсистему Системы-112 Волгоградской области.

Действующая РАСЦО построена с использованием средств защиты информации и соответствует требованиям, предъявляемым к государственным информационным системам класса защищенности К2 в соответствии с приказом ФСТЭК России от 11.02.2013 №17.

КСЭОН функционирует на базе оборудования построенного на базе оборудования КТСО П-166М АО «Калужский завод телеграфной аппаратуры». Пункт управления КСЭОН расположен по адресу, г. Волгоград, улица Канунникова, дом 16.

4. Требования к работам

4.1 Требования к содержанию работ.

МАСЦО должна быть создана в соответствии с этапами, указанными в пункте 6, и настоящим Техническим заданием. В том числе необходимо выполнить следующие работы:

- передача оборудования и ПО ИБ, необходимого для исполнения Договора;
- монтаж и подключение к электропитанию СЗИ по адресам, указанным в приложении №1;
- пуско-наладка оборудования;
- создание подсистемы защиты информации;
- аттестация МАСЦО по ИБ;
- разработка документации.

Для создания основного пункта управления МАСЦО необходимо использовать существующее автоматизированное рабочее место дежурного единой дежурно-диспетчерской службы городского округа город-герой Волгоград, расположенного по адресу г. Волгоград, улица Канунникова, дом 16 и функционирующего на базе оборудования П-166 ИТК ОС.

Подрядчик своими силами осуществляет необходимые дополнительные настройки программного обеспечения и оборудования для обеспечения возможности управления смонтированными комплексами оповещения с существующих пунктов управления, указанных в п.3.

Подрядчик обеспечивает наличие всех необходимых для выполнения работ материалов, инструментов, оборудования, комплектующих изделий и ПО (в том числе кабели, кабель-каналы, разъемы, крепежный материал и т.д.) без дополнительных затрат для Заказчика.

Согласование размещения и подключения СЗИ к сети электроснабжения находится в зоне ответственности Заказчика.

В рамках выполнения работ, при невозможности размещения и подключения СЗИ по адресам, указанным в адресном плане размещения КГО (приложение №1) места размещения СЗИ по согласованию Сторон могут быть перенесены.

Невозможность размещения СЗИ может быть обоснована отказом собственника недвижимости и отсутствием технической возможности. Под невозможностью подключения к электропитанию понимается отсутствие электросети с необходимой мощностью на расстоянии более 200 метров от точки подключения.

Ответственность за выполнение требований по охране труда и обеспечение пожарной безопасности при выполнении работ несёт Подрядчик.

4.2 Требования к оборудованию.

4.2.1 Общие требования к оборудованию.

Оборудование должно быть новым, не бывшим в употреблении/эксплуатации, не восстановленным, не переделанным, не поврежденным, не находиться под арестом, в залоге или иным обременением, изготовленным из 100 (ста) процентов новых компонентов, не иметь дефектов, связанных с материалами и качеством изготовления и конструкцией, материалами или работой по их изготовлению, либо проявляющихся в результате действия или упущения производителя и/или упущения Подрядчика, при соблюдении Заказчиком правил эксплуатации передаваемых товаров.

Оборудование не должно иметь дефектов, связанных с конструкцией, материалами или работой по их изготовлению, либо проявляющихся в результате действия или упущения производителя и/или упущения Подрядчика, при соблюдении Заказчиком правил эксплуатации оборудования.

Корпуса оборудования не должны иметь потертостей, царапин и следов вскрытия.

Оборудование должно соответствовать ГОСТам, ТУ, действующим на момент поставки в РФ, иметь торговую марку (товарный знак при наличии), сопровождаться необходимыми сертификатами.

В комплектации должны быть все необходимые интерфейсные шнуры и кабели, а также носители с драйверами, необходимыми для работы оборудования.

Оборудование должно сопровождаться технической документацией на русском языке, с приложением гарантийного талона с указанием на русском языке адреса и телефонов сервисного центра, даты производства оборудования, даты передачи оборудования Заказчику. Гарантийный талон должен быть заверен печатью Подрядчика (при наличии печати).

4.2.2 Требования к составу оборудования и ПО.

Таблица №1. Требования к составу оборудования и ПО.

№ п/п	– Наименование	– 1 этап	– 2 этап	– Всего
		– Кол-во комплектов	– Кол-во комплектов	– Итого, комплектов
1	– СЗИ. Неисключительные права на расширение функционала программного обеспечения, выполняющего функции системы централизованного управления политиками безопасности для отдельных узлов и групп узлов защищенной сети ViPNet	– 35	– 79	– 114
2	– СЗИ. Неисключительное право на использование модуля обнаружения и предотвращения вторжений Средства защиты информации Secret Net Studio	– 0	– 1	– 1
3	– СЗИ. Неисключительное право на использование средств анализа защищенности	– 0	– 1	– 1
4	– СЗИ. Установочный комплект права на использование средств анализа защищенности	– 0	– 1	– 1
5	– СЗИ. Права на использование средств антивирусной защиты информации	– 0	– 10	– 10

6	– СЗИ. Установочный комплект права на использование средств антивирусной защиты информации	– 0	– 1	– 1
7	– СЗИ. ПАК ViPNet Coordinator IG10 4.x	– 35	– 79	– 114

Таблица № 1.1. Класс программного обеспечения:

№ п/п	Наименование ПО	Класс ПО	
		приказ Минцифры от 22.09.2020 № 486	**приказ Минцифры от 31.12.2015 № 621**
1	Расширение функционала программного обеспечения, выполняющего функции системы централизованного управления политиками безопасности для отдельных узлов и групп узлов защищенной сети ViPNet (п.4.3 настоящего ООЗ)	02.08 Средства мониторинга и управления	
2	Модуль обнаружения и предотвращения вторжений Средства защиты информации Secret Net Studio (п.4.3 настоящего ООЗ)	03.01 Средства защиты от несанкционированного доступа к информации	
3	Программное обеспечение анализа защищенности (п.4.3 настоящего ООЗ)		02.01 Операционные системы 02.13 Средства обеспечения информационной безопасности
4	Программное обеспечение антивирусной защиты информации (п.4.3 настоящего ООЗ)	03.06 Средства антивирусной защиты	
5	ViPNet Coordinator IG10 4.x (п.4.3 настоящего ООЗ)	03.11 Средства защиты каналов передачи данных, в том числе криптографическими методами	

4.3 Требования к подсистеме защиты информации

– **Требования к Подрядчику:**

Подрядчик должен предоставить Заказчику сведения о наличии действующих лицензий:

1) лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации, полученной в соответствии с «Положением о лицензировании деятельности по технической защите конфиденциальной информации», утвержденным постановлением Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (далее - Положение) на следующие виды работ и услуг:

- услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации (подпункт "б" пункта 4 Положения);

– работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации средств и систем информатизации (подпункт "г" пункта 4 Положения);

– работы и услуги по проектированию в защищенном исполнении средств и систем информатизации (подпункт "д" пункта 4 Положения);

– - услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации,

программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации) (подпункт "е" пункта 4 Положения).

2) лицензии ФСБ России, полученной в соответствии с «Положением о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию 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)», утвержденным Постановлением Правительства РФ от 16 апреля 2012 г. N 313 на следующие виды выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, указанные в прилагаемом к указанному положению перечне (Приложение 1):

- разработка защищенных с использованием шифровальных (криптографических) средств информационных систем (пункт 2 Перечня);

- монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации, и шифровальных (криптографических) средств, разработанных для применения в составе технологии, реализуемой промежуточными элементами интеллектуальной системы учета электрической энергии (мощности) и приборами учета электрической энергии, сертифицированных Федеральной службой безопасности Российской Федерации (пункт 12 Перечня);

– 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 20 Перечня);

– - передача шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации, и шифровальных (криптографических) средств, разработанных для применения в составе технологии, реализуемой промежуточными элементами интеллектуальной системы учета электрической энергии (мощности) и приборами учета электрической энергии, сертифицированных Федеральной службой безопасности Российской Федерации (пункт 21 Перечня).

Указанные в настоящем пункте требования являются существенными в целях исполнения Договора

Требования к Системе:

Для Системы установлен класс защищенности государственных информационных систем К2 согласно приказу ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

ПЗИ должна обеспечивать соответствие МАСЦО требованиям к установленному классу защищенности.

Работы выполняются в несколько в соответствии с Таблицей 1.

Подрядчик вправе выполнить работы по этапам досрочно.

Таблица 1

№ п/п	Наименование этапов	Описание состава мероприятий, реализуемых в рамках этапа	Срок выполнения работ по этапу
	Разработка требований к ПЗИ Системы	− Уточнение и анализ угроз безопасности информации Системы; − Разработка модели угроз безопасности информации Системы.	не позднее 28.12.2023
	Разработка технических решений ПЗИ Системы	− Разработка (уточнение) технических решений ПЗИ Системы; − Разработка эксплуатационной документации и организационно-распорядительных документов по обеспечению безопасности.	не позднее 28.12.2023
	Передача средств защиты информации (I очередь)	− Комплектация ПЗИ программными и программно-техническими СрЗИ (Перечень передаваемых СрЗИ указан в Таблице № 4).	не позднее 28.12.2023
	Внедрение средств защиты информации (I очередь)	− Пусконаладочные работы (Сведения о составе СрЗИ, внедряемых в Систему, приведены в Таблице № 2)	не позднее 28.12.2023
	Передача средств защиты информации (II очередь)	− Комплектация ПЗИ программными и программно-техническими СрЗИ Перечень передаваемых СрЗИ указан в Таблице № 5)	с 29.12.2023 г. до 28.12.2024
	Внедрение средств защиты информации (II очередь)	− Пусконаладочные работы (Сведения о составе СрЗИ, внедряемых в Систему, приведены в Таблице № 3); − Внедрение организационных мер защиты информации; − Проведение предварительных испытаний.	с 29.12.2023 г. до 28.12.2024
	Аттестация Системы	− Проведение аттестационных испытаний	с 29.12.2023 г. до 28.12.2024

Этап №1. Разработка требований к ПЗИ Системы.

Уточнение и анализ угроз безопасности информации Системы

Угрозы безопасности информации определяются Подрядчиком по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей Системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

При определении угроз безопасности информации учитываются структурно-функциональные характеристики Системы, включающие структуру и состав Системы, физические, логические, функциональные и технологические взаимосвязи между сегментами Системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в Системе и в ее отдельных сегментах, а также иные характеристики Системы, применяемые информационные технологии и особенности ее функционирования.

1) В рамках выполнения работ Заказчик организует предоставление доступа на объекты, предназначенные для размещения Системы, а также информацию, необходимую для проектирования и разработки документации по запросу Подрядчика.

Анализ угроз безопасности информации должен включать:

1) уточнение (выявление) источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей;

2) анализ возможных уязвимостей программных и программно-аппаратных средств;

3) определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации;

4) оценку возможных последствий от реализации (возникновения) угроз безопасности информации.

В качестве исходных данных для анализа угроз безопасности информации используется банк данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, а также источники, содержащие иные сведения об уязвимостях и угрозах безопасности информации.

Разработка модели угроз безопасности информации Системы.

Подрядчик в соответствии с Методикой оценки угроз безопасности информации, утвержденной ФСТЭК России от 05.02.2021 г., разрабатывает проект модели угроз безопасности информации, обрабатываемой в Системе.

Модель угроз безопасности информации должна содержать описание информационной системы и их структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационных систем, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Модель угроз безопасности информации должна содержать обоснование необходимости использования СКЗИ для защиты информации, а также определение класса СКЗИ в соответствии с Приказом ФСБ России от 24.10.2022 г. № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств».

– Подрядчику также необходимо подготовить и предоставить Заказчику проект частного технического задания на создание подсистемы защиты информации Системы.

В результате выполнения работ по этапу № 1 Подрядчик предоставляет проекты:

– модели угроз безопасности информации Системы;

– частного технического задания на создание подсистемы защиты информации Системы.

Заказчик своими силами проводит согласование со ФСТЭК России проекта модели угроз безопасности информации и частного технического задания. В случае выявленных при согласовании со ФСТЭК России замечаний по содержанию разрабатываемых в рамках данного этапа документов Подрядчик дорабатывает документы в части выявленных замечаний и в течение 10 (десяти) рабочих дней предоставляет доработанные документы Заказчику.

–

Этап № 2. Разработка технических решений ПЗИ Системы.

Подрядчик, в целях определения технических решений ПЗИ:

– уточняет условия расположения Системы относительно границ контролируемой зоны;

– уточняет конфигурацию, компоненты и топологию Системы, ее физические, функциональные и технологические связи как внутри системы, так и с другими системами различного уровня и назначения;

– уточняет состав технических средств и систем, предполагаемых к использованию в Системе, условия их расположения, общесистемные и прикладные программные средства;

– уточняет режимы обработки информации в Системе;

– осуществляет анализ имеющихся у Заказчика документов, в частности: действующих политик информационной безопасности; документов, определяющих

организационную структуру Заказчика; сведений об ИТ-инфраструктуре; сведений о действующей ПЗИ.

Для выполнения вышеуказанных работ Подрядчиком:

1) уточняются соответствующие разделы технической документации с учетом результатов предыдущих этапов создания ПЗИ;

2) определяются (уточняются) субъекты доступа (пользователи, процессы и иные субъекты доступа) и объекты доступа Системы;

3) определяются политики управления доступом;

4) уточняются и обосновываются организационные и технические меры, подлежащие реализации в рамках ПЗИ;

5) определяются виды и типы СрЗИ, обеспечивающие реализацию всех технических мер по обеспечению безопасности Системы с учетом проводимых работ по анализу угроз безопасности информации;

6) уточняется архитектура ПЗИ, включающая состав, места установки, взаимосвязи СрЗИ;

7) определяются требования к параметрам настройки программных и программно-аппаратных средств, включая СрЗИ, обеспечивающие реализацию мер по обеспечению безопасности, блокирование (нейтрализацию) угроз безопасности информации и устранение уязвимостей Системы;

8) определяются меры по обеспечению безопасности при взаимодействии Системы с иными объектами информатизации или информационно-телекоммуникационными сетями.

На основании полученных сведений Подрядчик осуществляет:

1) разработку технического проекта на создание ПЗИ Системы в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и иным нормативными правовыми актами в области защиты информации.

Организационные и технические меры защиты информации, реализуемые в Системе в рамках ее ПЗИ, должны обеспечивать, в том числе:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- защиту среды виртуализации;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- доступность информации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных.

Для выбора мер защиты информации должны применяться методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

При разработке технических решений ПЗИ должно быть учтено использование для передачи информации средств криптографической защиты информации системы вызова экстренных оперативных служб через единый номер «112», используемых в пунктах управления органов повседневного управления звеньев территориальной подсистемы Волгоградской

области РСЧС (единые дежурно-диспетчерские службы), а также государственной информационной системы «Распределенная автоматизированная система информирования и оповещения населения Волгоградской области» – программно-аппаратных комплексов VipNet Coordinator HW 4 (сеть №4826, сеть №15228), а также обеспечено использование совместимых средств криптографической защиты информации в Системе.

Технические решения должны содержать требования к защите информации при информационном взаимодействии Системы с иными информационными системами и информационно-телекоммуникационными сетями.

Результаты разработки (доработки) технических решений отражаются в технической документации на систему защиты информации, разрабатываемой с учетом ГОСТ 34.201 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» и в соответствии с п 15.1 приказа ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2) разработку эксплуатационной документации и организационно-распорядительных документов по обеспечению безопасности:

- технический паспорт на Систему;
- организационно-распорядительные документы по защите информации, регламентирующие защиту информации в ходе эксплуатации Системы, в том числе план мероприятий по защите информации Системы, управлению (администрированию) ПЗИ, управлению конфигурацией Системы, реагированию на инциденты безопасности, информированию и обучению персонала, контролю за обеспечением уровня защищенности информации.

3) разработку программ и методик испытаний ПЗИ Системы на соответствие требованиям информационной безопасности в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и иным нормативными правовыми актами в области защиты информации.

В результате разработки технических решений ПЗИ Подрядчик предоставляет:

- технический проект на создание ПЗИ Системы, включающий:
  - ведомость технического проекта;
  - пояснительную записку с изложением решений по комплексу организационных мер и программно-техническим средствам обеспечения безопасности информации, составу средств защиты информации;
  - схему структурную ПЗИ Системы.
- проекты эксплуатационной документации и организационно-распорядительных документов по обеспечению безопасности;
- программу и методики предварительных испытаний ПЗИ Системы,
- программу и методики приемочных испытаний ПЗИ Системы;
- программу и методики аттестационных испытаний ПЗИ Системы.

Программы и методики испытаний ПЗИ, технический проект на создание ПЗИ Системы согласовываются Подрядчиком с Заказчиком и утверждаются до начала аттестационных испытаний в срок не более 5 рабочих дней после передачи Заказчику.

В ходе аттестационных испытаний Подрядчик может вносить изменения в программы и методики испытаний ПЗИ по согласованию с Заказчиком.

Этап № 3. Передача средств защиты информации (I очередь).

Комплектация ПЗИ Системы СрЗИ проводится в соответствии с разработанным техническим проектом на создание ПЗИ Системы и учетом имеющихся в наличии у Заказчика СрЗИ. Перечень передаваемых СрЗИ указан в Таблице № 4 настоящего ТЗ.

Неисключительные права (лицензии) на использование программного обеспечения средств защиты информации предоставляются в соответствии с действующим законодательством на основании сублицензионных договоров и актов приёма-передачи неисключительных прав.

Этап № 4. Внедрение средств защиты информации (I очередь).

Для установки и настройки СрЗИ используются СВТ Заказчика, которые в полном объеме обеспечивают соответствие характеристик СВТ рекомендациям производителей СрЗИ.

Внедрение ПЗИ включает пуско-наладку передаваемых СрЗИ:

- осуществляется монтаж и пусконаладочные работы технических и программных средств;
- проводятся испытания СрЗИ;
- устраняются неисправности и внесение изменений в документацию на Систему;
- оформляется акт о вводе СрЗИ в эксплуатацию.

Адреса размещения средств оповещения приведены в Приложении № 1. Сведения о составе СрЗИ, внедряемых в Систему, приведены в Таблице 2.

В рамках выполнения работ по установке и настройке Заказчик оказывает содействие в обеспечении доступа специалистов Подрядчика к объектам информатизации и инженерным коммуникациям, а также к средствам администрирования ViPNet-сети № 15228.

После внедрения СрЗИ Подрядчик предоставляет акт ввода в эксплуатацию каждого компонента ПЗИ (СрЗИ).

– Таблица 2 - Состав внедряемых СрЗИ

№ п/п	Наименование СВТ	Внедряемые
		Криптографический шлюз[1]
1	Оконечные устройства (комплексы голосового оповещения)	35
	Итого	35

Примечание:

[1]ПАК, указанные в строке 2 Таблицы 4.

Этап № 5. Передача средств защиты информации (II очередь).

Комплектация ПЗИ Системы СрЗИ проводится в соответствии с разработанным техническим проектом на создание ПЗИ Системы и учетом имеющихся в наличии у Заказчика СрЗИ. Перечень передаваемых СрЗИ указан в Таблице 5.

Неисключительные права (лицензии) на использование программного обеспечения средств защиты информации предоставляются в соответствии с действующим законодательством на основании сублицензионных договоров и актов приёма-передачи неисключительных прав.

Этап № 6. Внедрение средств защиты информации (II очередь).

Для установки и настройки СрЗИ используются СВТ Заказчика, которые в полном объеме обеспечивают соответствие характеристик СВТ рекомендациям производителей СрЗИ.

Внедрение ПЗИ включает:

1) Пуско-наладку передаваемых СрЗИ:
   - осуществляется монтаж и пусконаладочные работы технических и программных средств;
   - проводятся испытания СрЗИ;

– устраняются неисправности и внесение изменений в документацию на Систему;

– оформляется акт о вводе СрЗИ в эксплуатацию.

Адреса размещения средств оповещения приведены в Приложении № 1. Сведения о составе СрЗИ, внедряемых в Систему, приведены в Таблице 3.

В рамках выполнения работ по установке и настройке Заказчик оказывает содействие в обеспечении доступа специалистов Подрядчика к объектам информатизации и инженерным коммуникациям, а также к средствам администрирования ViPNet-сети № 15228.

После внедрения СрЗИ Подрядчик предоставляет акт ввода в эксплуатацию каждого компонента ПЗИ (СрЗИ).

Таблица 3 – Состав внедряемых СрЗИ

№ п/п	Наименование СВТ	Внедряемые			
		Криптографический шлюз[1]	**Антивирусные средства защиты[2]**	**Средства обнаружения вторжений[3]**	**Средство анализа защищенности[4]**
1	Оконечные устройства (комплексы голосового оповещения)	79	0	0	0
2	АРМ ЗИП	0	1	0	0
3	АРМ ЕДДС городского округа г. Волгоград	0	0	1	1
	Итого	79	1	1	1

Примечание:

[1]ПАК, указанные в строке 2 Таблицы 5.

[2]ПО, указанное в строке 3 Таблицы 5.

[3]ПО, указанное в строке 5 Таблицы 5.

[4]ПО, указанное в строке 6 Таблицы 5.

2) Внедрение организационных мер защиты информации

При внедрении организационных мер защиты информации осуществляется утверждение Заказчиком организационно-распорядительных документов и эксплуатационной документации ПЗИ, в т.ч. в целях реализации правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения.

В случае выявления недостатков в организационно-распорядительных документах по защите информации Подрядчиком осуществляется корректировка организационно-распорядительных документов ПЗИ.

3) Предварительные испытания объекта информатизации

Предварительные испытания проводятся согласно утвержденным программам и методикам.

Во время предварительных испытаний проводится:

– испытание ПЗИ на соответствие техническому заданию;

– устранение неисправностей и внесение изменений в документацию на ПЗИ, в том числе эксплуатационную, в соответствии с протоколами испытаний;

– оформление протокола предварительных испытаний.

Этап № 7. Аттестация Системы на соответствие требованиям о защите информации

Требования к мероприятиям по аттестации Системы на соответствие требованиям о защите информации описаны в Приложении № 2.

Таблица 4. Состав и характеристики программных средств защиты информации (I очередь)

№ п/п	Наименование	Характеристики программного обеспечения*	Ед. изм.	Кол-во
1.	Неисключительные права на расширение функционала программного обеспечения, выполняющего функции системы централизованного управления политиками безопасности для отдельных узлов и групп узлов защищенной сети ViPNet*	Предоставление прав на расширение функционала ПО ViPNet Policy Manager**, выполняющего функции системы централизованного управления политиками безопасности для отдельных узлов и групп узлов защищенной сети VipNet** №15228 на 1 узел управления. Срок действия неисключительных прав – бессрочно.	усл. ед.	35
2.	ПАК ViPNet Coordinator IG10 4.x (Utun) I1*	Форм-фактор - блок с креплением на DIN-рейку: наличие. Количество сетевых интерфейсов RJ45 10/100-BaseT: 3 шт. Среднее время наработки на отказ (MTBF): 350 000 часов Максимальная пропускная способность VPN (L3): 10 Мбит/с Максимальная производительность МЭ: 10 Мбит/с Встроенный DNS-сервер, NTP-сервер, DHCP-сервер: наличие Функция DHCP –Relay: наличие Работа в режиме 24x7: наличие Возможность создания кластера горячего резервирования: наличие Интерфейс GPIO 1 x In, 1 x Out : наличие Разъем для Sim-карты: 1 шт. Совместимость с VPN-узлами сети ViPNet №15228: наличие. Наличие следующего функционала: - межсетевой экран с контролем состояний сессий и инспекцией прикладных протоколов; - защита соединений сетевого уровня с шифрованием и аутентификацией - раздельная настройка правил фильтрации для открытого и шифруемого трафика; - NAT/PAT; - статическая и динамическая маршрутизация; - поддержка VLAN; - удаленное обновление программного обеспечения с помощью ViPNet Administrator; - дистанционное управление политиками безопасности с помощью ViPNet PolicyManager; Комплект передачи: – программно-аппаратный комплекс ViPNet Coordinator IG 10 I1; – эксплуатационная документация; – формуляр; – блок питания согласно эксплуатационной документации.	усл. ед.	35

*В соответствии с пунктом 1 части 1 статьи 33 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», в связи с необходимостью обеспечения совместимости передаваемых

средств защиты информации с используемыми Заказчиком средствами защиты информации, эквивалент на указанный объект закупки не предусмотрен.

**В описании требований к техническим характеристикам услуг используются товарные знаки программного обеспечения, используемого у Заказчика, совместимость с которым необходимо обеспечить.

Таблица 5. Состав и характеристики программных средств защиты информации (II очередь)

№ п/п	Наименование	Характеристики программного обеспечения*	Ед. изм.	Кол-во
1.	Неисключительные права на расширение функционала программного обеспечения, выполняющего функции системы централизованного управления политиками безопасности для отдельных узлов и групп узлов защищенной сети ViPNet*	Предоставление прав на расширение функционала ПО ViPNet Policy Manager**, выполняющего функции системы централизованного управления политиками безопасности для отдельных узлов и групп узлов защищенной сети VipNet** №15228 на 1 узел управления. Срок действия неисключительных прав – бессрочно.	усл. ед.	79
2.	ПАК ViPNet Coordinator IG10 4.x (Utun) I1*	Форм-фактор - блок с креплением на DIN-рейку: наличие. Количество сетевых интерфейсов RJ45 10/100-BaseT: 3 шт. Среднее время наработки на отказ (MTBF): 350 000 часов Максимальная пропускная способность VPN (L3): 10 Мбит/с Максимальная производительность МЭ: 10 Мбит/с Встроенный DNS-сервер, NTP-сервер, DHCP-сервер: наличие Функция DHCP –Relay: наличие Работа в режиме 24x7: наличие Возможность создания кластера горячего резервирования: наличие Интерфейс GPIO 1 x In, 1 x Out : наличие Разъем для Sim-карты: 1 шт. Совместимость с VPN-узлами сети ViPNet №15228: наличие. Наличие следующего функционала: - межсетевой экран с контролем состояний сессий и инспекцией прикладных протоколов; - защита соединений сетевого уровня с шифрованием и аутентификацией - раздельная настройка правил фильтрации для открытого и шифруемого трафика; - NAT/PAT; - статическая и динамическая маршрутизация; - поддержка VLAN; - удаленное обновление программного обеспечения с помощью ViPNet Administrator; - дистанционное управление политиками безопасности с помощью ViPNet PolicyManager; Комплект передачи: – программно-аппаратный комплекс ViPNet Coordinator IG 10 I1; – эксплуатационная документация;	усл. ед.	79

		– формуляр; – блок питания согласно эксплуатационной документации.		
3.	Права на использование средств антивирусной защиты информации	Компоненты САВЗ функционируют на следующих версиях ОС: • семейства Linux: ОС Astra Linux Special Edition 1.7. Компоненты САВЗ обеспечивают реализацию следующих функциональных возможностей: • резидентный антивирусный мониторинг; • антивирусное сканирование по команде пользователя или администратора; • антивирусное сканирование по расписанию; • антивирусное сканирование при определенных условиях: • после обновлений антивирусных баз данных; • каждый раз при запуске компьютера; • каждые сутки при первом запуске компьютера; • при успешном Интернет или VPN соединении; • вход пользователя; • при обнаружении подозрительной активности, в том числе и активным модулем «защита в режиме реального времени». • наличие задачи на выключение ПЭВМ по завершению сканирования • антивирусное сканирование трафика по следующим протоколам: FTP, HTTP и HTTPs, POP3 и POP3s, а также IMAP и IMAPs трафика. • защита от еще неизвестных вредоносных программ на основе эвристического анализа; • возможность добавлять в исключения только определенные угрозы, в независимости от их местонахождения на ПК: • обнаружение скрытых процессов; • возможность отключения антивирусной защиты при необходимости; • антивирусная проверка и лечение файлов, упакованных программами типа PKLITE, LZEXE, DIET, EXEPACK и пр.; • антивирусную проверку и лечение файлов в архивах форматов ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE; • наличие встроенного агента администрирования САВЗ, т.е. для возможности удаленного управления на клиентских рабочих станциях не нужно дополнительно устанавливать программное обеспечение для удаленного администрирования антивирусного программного обеспечения; • наличие планировщика; • ядро и все основные модули продукта не требуют перезагрузки и активны сразу	усл. ед.	10

		после установки; • настройка лимитов сканирования по параметрам – глубина вложенности (архивов), размера объекта и времени сканирования объекта; • наличие модуля, позволяющего проводить автоматическое сканирование содержания подключаемых внешних устройств хранения данных, а также применять расширенный анализ для запуска файлов с таких устройств; • возможность отката обновлений вирусных баз на предыдущие версии и приостановка их обновления с последующим автоматическим включением обновления через указанный промежуток времени; • настройка проверки исполняемых файлов и загрузочных областей компьютера в качестве отдельной задачи; • технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющих избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей; • наличие множества путей уведомления администраторов о важных событиях, происходящих на рабочих станциях (почтовое сообщение, всплывающее окно, запись в журнал событий); • обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на отчуждаемых носителях информации. САВЗ имеет сертификат соответствия ФСТЭК России, подтверждающий соответствие требованиям к средствам антивирусной защиты не ниже 5 класса. Срок действия неисключительных прав на использование САВЗ – не менее 12 месяцев. В комплект передачи входит: - установочный комплект. - формуляр на изделие. - сертификат соответствия ФСТЭК России.		
4.	Установочный комплект права на использование средств антивирусной защиты информации	В комплект передачи входит: - установочный комплект. - формуляр на изделие. - сертификат соответствия ФСТЭК России.	усл. ед.	1
5.	Неисключительное право на использование модуля обнаружения и предотвращения вторжений Средства защиты информации Secret Net Studio*	Модуль должен осуществлять обнаружение и предотвращение вторжений. Срок действия неисключительных прав – 1 год. Модуль обнаружения и предотвращения вторжений должен быть совместим с используемым Заказчиком СЗИ от НСД Secret Net Studio. **Требования к сертификации и применению в информационных системах:** СЗИ должно соответствовать требованиям документов:	усл. ед.	1

		• «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» по 4 уровню доверия (ФСТЭК России, 2020); • «Требования к системам обнаружения вторжений» не ниже 4 класса защиты» (ФСТЭК России, 2011); • «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты» ИТ.СОВ.У4.ПЗ (ФСТЭК России, 2012). СЗИ должно допускать использование в следующих информационных системах: • государственные информационные системы – до 2 класса защищенности (включительно).		
6.	Неисключительное право на использование средств анализа защищенности	Средство анализа защищенности (далее – САНЗ) обеспечивает выполнение следующих основных функций: – сканирование узлов и удалённая идентификация ОС; – в рамках одной задачи, обеспечивается сканирование не менее 4 узлов исследуемой сети; – сканирование и идентификация UDP и TCP –сервисов; – выявление уязвимостей в программном обеспечении (ПО) исследуемых сетей, обнаруживаются следующие уязвимости: – переполнение буфера; – уязвимость к DoS- атакам; – ошибочная конфигурация службы; – слабая парольная защита (при анализе стойкости паролей ПО должно иметь возможность подключения внешних словарей); – возможность повышения привилегий пользователя; – SQL-инъекция; – инъекция кода; – межсайтовое выполнение скриптов. По результатам санирования предусмотрена возможность формирования (генерации) отчётов. Генерация отчётов должна осуществляться по запросу пользователя из графического интерфейса пользователя. Представление выходных данных в отчётах должно осуществляться с использованием цветовой шкалы, отражающей уровень опасности каждой из выявленных уязвимостей. Отчёты должны содержать рекомендации по устранению уязвимостей. Предусмотрена возможность обновления баз данных и исполняемого кода. САНЗ при запуске должно обеспечивать аутентификацию пользователей по паролю. САНЗ должно быть сертифицировано ФСТЭК России на соответствие ТУ. Срок действия неисключительных прав на использование САНЗ – не менее 12 месяцев	усл. ед.	1
7.	Установочный комплект права на использование средств анализа защищенности	САНЗ передается в виде загрузочного носителя, который содержит набор предустановленного специализированного и системного программного обеспечения. В комплект должен входить формуляр на изделие.	усл. ед.	1

*В соответствии с пунктом 1 части 1 статьи 33 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», в связи с необходимостью обеспечения совместимости передаваемых средств защиты информации с используемыми Заказчиком средствами защиты информации, эквивалент на указанный объект закупки не предусмотрен.

**В описании требований к техническим характеристикам услуг используются товарные знаки программного обеспечения, используемого у Заказчика, совместимость с которым необходимо обеспечить

4.4.Требования к документации

По завершению работ по 2 этапу в срок не позднее 28.12.2024 должен быть разработан и передан Заказчику следующий комплект документов:

−руководства по эксплуатации оборудования, предусмотренные производителем;

−паспорта на оборудование, предусмотренные производителем;

−лицензии, сертификаты соответствия на оборудование и программное обеспечение;

−исполнительская документация.

Вся документация должна быть согласована и передана Заказчику в электронном виде, в формате PDF, на компакт-дисках (CD) или DVD-дисках.

5. Электропитание и заземление оборудования СЗИ

Электропитание подключаемого оборудования СЗИ должно осуществляться от существующих источников электропитания с номинальным напряжением 220 В.

Электропитание и заземление оборудования СЗИ должно быть предусмотрено от существующих источников электропитания и систем заземления. Оборудование СЗИ должно иметь защиту от перепадов электричества. Создание новых контуров заземления в обязанности Подрядчика не входит.

Оборудование СЗИ должно подключаться к существующим контурам заземления (при наличии).

6. Этапы выполнения работ. Содержание работ.

Номер п/п	Наименование мероприятия	Срок выполнения
1	- передача, монтаж и пусконаладка оборудования СЗИ по адресам согласно Приложению №1 к техническому заданию - создание подсистемы защиты информации в соответствии с требованиями п.4.3.	не позднее 28.12.2023
2	- передача, монтаж и пусконаладка оборудования СЗИ по адресам согласно Приложению №1 к техническому заданию - создание подсистемы защиты информации в соответствии с требованиями п.4.3. - аттестация МАСЦО - разработка документации	не позднее 28.12.2024

Работы по этапам выполняются последовательно. По соглашению Сторон работы, предусмотренные этапами, могут быть выполнены ранее установленного в п.6. технического задания срока.

7. Гарантии качества

Гарантийный срок на передаваемое оборудование должен составлять не менее 12 месяцев, на выполненные работы 2 (два) года.

Приложение №1 к техническому заданию

Адресный план размещения комплексов голосового оповещения

1. **Первый этап реализации 2023г.**

№ п/п	Адрес установки
Центральный район	
1	Муниципальное общеобразовательное учреждение лицей № 5 имени Ю.А. Гагарина , ул. Мира, 17
2	Муниципальное общеобразовательное учреждение гимназия № 3, ул. Пушкина, 7
3	Государственное бюджетное профессиональное образовательное учреждение Волгоградский строительный техникум, ул. Скосырева, 1 (Комитет образования ВО)
Тракторозаводский район	
4	Муниципальное общеобразовательное учреждение средняя школа № 87, ул. Колумба, 1 (пос. ГЭС)
5	Муниципальное общеобразовательное учреждение средняя школа № 3, пр-т Ленина, 197Б
6	Муниципальное общеобразовательное учреждение средняя школа имени 37-й Гвардейской стрелковой дивизии № 17, ул. Дзержинского, 40
7	Муниципальное дошкольное образовательное учреждение детский сад № 201, ул. Героев Шипки, 29А (пос. ГЭС)
Советский район	
8	Муниципальное общеобразовательное учреждение средняя школа № 54, ул. Казахская, 20
9	Муниципальное общеобразовательное учреждение средняя школа № 55 «Долина знаний», ул. Добрушина, 1
10	Муниципальное общеобразовательное учреждение средняя школа с углубленным изучением отдельных предметов № 106, ул. Ухтомского, 10
11	Муниципальное дошкольное образовательное учреждение детский сад № 21, ул. Богданова, 3А
Краснооктябрьский район	
12	Муниципальное общеобразовательное учреждение средняя школа № 95, пр-т Ленина, 151А
13	Муниципальное общеобразовательное учреждение гимназия № 14, пр-т Ленина, 121
14	Муниципальное общеобразовательное учреждение средняя школа с углубленным изучением отдельных предметов № 49, ул. Репина, 11
15	Муниципальное общеобразовательное учреждение средняя школа № 32, ул. Качалова, 58
16	Муниципальное общеобразовательное учреждение средняя школа с углубленным изучением отдельных предметов № 20, пр-т Ленина, 83
17	ГБУЗ Волгоградская областная детская клиническая больница, отделение медицинской реабилитации, ул. Асланова, 5А, (Комитет здравоохранения ВО)
Красноармейский район	
18	Муниципальное общеобразовательное учреждение средняя школа № 75, ул. Пролетарская, 9
19	Муниципальное общеобразовательное учреждение гимназия № 6, ул. Изобильная, 16
20	Государственное учреждение здравоохранения клиническая больница скорой медицинской помощи № 15, ул. Андижанская, 1А (Комитет здравоохранения ВО)
21	Муниципальное общеобразовательное учреждение средняя школа № 134 «Дарование», ул. Вучетича, 17

Ворошиловский район	
22	Муниципальное общеобразовательное учреждение гимназия № 5, ул. Пугачевская, 8
23	Муниципальное общеобразовательное учреждение гимназия № 4, ул. Иркутская, 1
24	Муниципальное общеобразовательное учреждение лицей № 11, ул. Елецкая, 9Б
25	Муниципальное общеобразовательное учреждение средняя школа № 105, ул. С. Филиппова, 1
Дзержинский район	
26	Муниципальное общеобразовательное учреждение средняя школа № 102, б-р 30 лет Победы, 66А
27	Государственное казенное образовательное учреждение Волгоградская школа-интернат № 2, ул. Хорошева, 18А (Комитет образования ВО)
28	Муниципальное общеобразовательное учреждение лицей № 7, ул. 51 Гвардейской, 59
29	Муниципальное общеобразовательное учреждение средняя школа с углубленным изучением отдельных предметов № 33, пос. Аэропорт, 23А
Кировский район	
30	Муниципальное общеобразовательное учреждение средняя школа № 77, ул. Маресьева, 4
31	Муниципальное общеобразовательное учреждение гимназия № 9, ул. Писемского, 38
32	Муниципальное общеобразовательное учреждение гимназия № 10, ул. 64 Армии, 63
33	Муниципальное общеобразовательное учреждение средняя школа № 24 имени Героя Советского Союза А.В. Федотова, ул. Кирова, 94Б
34	Муниципальное общеобразовательное учреждение средняя школа № 56, ул. Губкина, 2
35	Муниципальное дошкольное образовательное учреждение детский сад № 29, ул. Писемского, 1А

2. Второй этап реализации 2024г.

№ п/п	Адрес установки
Центральный район	
1	Муниципальное общеобразовательное учреждение средняя школа с углубленным изучением отдельных предметов № 44, ул. Рокоссовского, 40
2	12-ти этажный жилой дом, проспект Ленина, 56
3	Телерадиокомпания РТРС, ул. Рокоссовского, 98
Тракторозаводский район	
4	Муниципальное общеобразовательное учреждение средняя школа № 61, ул. Грамши, 39
5	Муниципальное общеобразовательное учреждение средняя школа № 88, ул. Богомольца, 15
6	Муниципальное общеобразовательное учреждение средняя школа № 1, ул. Ополченская, 42А
7	Муниципальное общеобразовательное учреждение гимназия № 13, ул. Быкова, 1
8	Муниципальное общеобразовательное учреждение средняя школа № 3, ул. Тракторостроителей, 15 (Нижний Тракторный)
9	Муниципальное общеобразовательное учреждение гимназия № 16, ул. Желудева, 5
10	Федеральное государственное бюджетное образовательное учреждение Волгоградский технический университет, факультет подготовки инженерных кадров, ул. Дегтярева, 2 (Комитет образования ВО)

11	Муниципальное общеобразовательное учреждение средняя школа № 27, ул. Мелиораторов, 9 (Водстрой)
12	Государственное бюджетное профессиональное образовательное учреждение Волгоградский технический колледж, корпус 1, ул. Шурухина, 59 (Комитет образования ВО)
Советский район	
13	Муниципальное общеобразовательное учреждение средняя школа с углубленным изучением отдельных предметов № 106, ул. Тормосиновская, 23
14	Федеральное государственное бюджетное образовательное учреждение высшего образования «Волгоградский государственный аграрный университет», пр-т Университетский, 26 (Комитет образования ВО)
15	Муниципальное общеобразовательное учреждение средняя школа № 93, ул. Тулака, 1
16	Федеральное государственное бюджетное образовательное учреждение высшего образования "Волгоградский государственный университет", пр-т Университетский, 100 (Комитет образования ВО)
17	Частное профессиональное образовательное учреждение «Газпром колледж Волгоград имени И.А. Матлашова», пр-т Университетский, 71 (Комитет образования ВО)
18	Муниципальное общеобразовательное учреждение средняя школа № 140, ул. Валентины Терешковой, 52
19	Государственное бюджетное профессиональное образовательное учреждение "Волгоградский техникум водного транспорта имени адмирала флота Н.Д. Сергеева", ул. Красноволжская, 1 (Комитет образования ВО)
20	Муниципальное общеобразовательное учреждение средняя школа № 15, пос. М. Горького, ул. Волгоградская, 156
21	Муниципальное общеобразовательное учреждение средняя школа № 15, пос. М.Горького, ул. Волгоградская, 172
22	Муниципальное общеобразовательное учреждение средняя школа № 46, пос. Песчанка, ул. Ольховская, 8
23	Муниципальное общеобразовательное учреждение средняя школа № 129, пос. Горный, ул. Семушкина, 2
24	Муниципальное дошкольное образовательное учреждение детский сад № 7 «Долина детства», ул. Добрушина, 27
25	Муниципальное дошкольное образовательное учреждение детский сад № 33, ул. Я. Купалы, 62
26	Муниципальное дошкольное образовательное учреждение детский сад № 287, пос. 8 кирпичного завода, 28
27	Государственное бюджетное учреждение здравоохранения клиническая больница скорой медицинской помощи № 7, ул. Казахская, 1 (детский корпус) (Комитет здравоохранения ВО)
28	Муниципальное дошкольное образовательное учреждение детский сад № 36, ул. Воронова, 16
29	Муниципальное дошкольное образовательное учреждение детский сад № 11, ул. Грибанова, 3
Краснооктябрьский район	
30	Муниципальное общеобразовательное учреждение гимназия № 12, ул. Прибалтийская, 1А
31	Муниципальное общеобразовательное учреждение средняя школа № 78, ул. Хользунова, 33
32	Муниципальное общеобразовательное учреждение средняя школа № 30, ул. Никопольская, 1
33	Отдел полиции № 2 Управления МВД России по г. Волгоград, ул. Тряскина, 11

34	Муниципальное общеобразовательное учреждение средняя школа № 76, ул. Созидательская, 27
35	Волгоградский институт управления Российской академии народного хозяйства и государственной службы, ул. Герцена, 10 (Комитет образования ВО)
36	5-ти этажное здание, АО "Партнер-Сервис", проспект Ленина, 94
Красноармейский район	
37	Волгоградский филиал Аккредитованного образовательного частного учреждения высшего образования «Московский финансово-юридический университет МФЮА», ул. Бахтурова, 25Г (Комитет образования ВО)
38	Муниципальное общеобразовательное учреждение средняя школа № 60, ул. Олимпийская, 33
39	Государственное бюджетное профессиональное образовательное учреждение “Волгоградский индустриальный техникум”, ул. Арсеньева, 8 (Комитет образования ВО)
40	Муниципальное общеобразовательное учреждение средняя школа № 134 «Дарование», ул. Георгиевская, 4
41	Муниципальное дошкольное образовательное учреждение детский сад № 221, ул. Водников, 10
42	Филиал муниципального унитарного предприятия Метроэлектротранс, Трамвайно-троллейбусное депо № 3, ул. 40 лет ВЛКСМ, 66
43	Муниципальное общеобразовательное учреждение средняя школа № 65, Бульвар Энгельса, 30
44	Муниципальное общеобразовательное учреждение средняя школа № 75, ул. Арсеньева, 32
45	Муниципальное дошкольное образовательное учреждение детский сад № 343, Веселый переулок, 12 (Волжский район гидросооружений и судоходства Федерального бюджетного учреждения «Администрация Волго-Донского бассейна внутренних водных путей», ул. Бутурлиновская, 24)
46	Муниципальное дошкольное образовательное учреждение детский сад № 223, ул. Куликовская, 9
47	Муниципальное общеобразовательное учреждение средняя школа № 117, Николаевская, 17А
48	Муниципальное общеобразовательное учреждение средняя школа с углубленным изучением отдельных предметов № 38, пр-т Столетова, 50А
Ворошиловский район	
49	Муниципальное общеобразовательное учреждение лицей № 11, 2 корпус № 2, ул. Елецкая, 20
50	Административное здание, ул. Азизбекова, 75
51	Муниципальное общеобразовательное учреждение средняя школа № 104, ул. Елецкая, 142
52	Федеральное государственное бюджетное учреждение здравоохранения «Волгоградский медицинский клинический центр Федерального медико-биологического агентства» (ФГБУЗ ВМКЦ ФМБА России), ул. Ким, 24 (Комитет здравоохранения ВО)
53	Муниципальное общеобразовательное учреждение средняя школа № 14, ул. Ставропольская, 71
54	Муниципальное общеобразовательное учреждение средняя школа № 11, ул. Комитетская, 58
55	Муниципальное общеобразовательное учреждение средняя школа № 105, ул. Ельшанская, 130

56	Общежитие Федерального государственного бюджетного образовательного учреждения высшего образования «Волгоградский государственный технический университет», Институт архитектуры и строительства, ул. Академическая, 1, к. В (Комитет образования ВО)
57	Частное учреждение здравоохранения «КБ «РЖД-Медицина» г. Волгоград», стационар, ул. Автотранспортная, 75 (РЖД)
58	Муниципальное казенное учреждение «Городской информационный центр», ул. Бобруйская, 7
Дзержинский район	
59	Муниципальное дошкольное образовательное учреждение детский сад № 23, ул. Охотская, 19
60	Государственное бюджетное образовательное учреждение школа-интернат «Созвездие», ул. Большая, 17 (Комитет образования ВО)
61	Муниципальное дошкольное образовательное учреждение детский сад № 31, ул. Покрышкина, 5
62	Муниципальное общеобразовательное учреждение средняя школа № 67 по адресу Ангарская, 15
63	Муниципальное общеобразовательное учреждение средняя школа № 89, ул. Республиканская, 5
64	Муниципальное общеобразовательное учреждение средняя школа № 50, пос. Гумрак, ул. Строителей, 4А
65	Муниципальное общеобразовательное учреждение средняя школа с углубленным изучением отдельных предметов № 97, ул. Пятиизбянская, 5
66	Государственное бюджетное учреждение здравоохранения клиническая больница скорой медицинской помощи № 25, ул. Землячки, 74 (Комитет здравоохранения ВО)
67	Муниципальное дошкольное образовательное учреждение детский сад № 123, ул. Рыбалко, 6А
68	Муниципальное дошкольное образовательное учреждение детский сад № 277, ул. Батумская, 1
69	Муниципальное дошкольное образовательное учреждение «Центр развития ребенка – детский сад № 6», ул. 8 воздушной армии, 23А
70	Муниципальное общеобразовательное учреждение средняя школа с углубленным изучением отдельных предметов № 96, пр-т Жукова, 13
Кировский район	
71	Государственное бюджетное учреждение здравоохранения Волгоградская областная клиническая больница № 1 (инфекционное отделение № 1), пер. Кленовый , 1Б (Комитет здравоохранения ВО)
72	Муниципальное общеобразовательное учреждение средняя школа с углубленным изучением отдельных предметов № 57, ул. Саши Чекалина, 10
73	Муниципальное общеобразовательное учреждение средняя школа № 56, ул. Кирова, 128Б
74	Почта России, отделение № 108, ул. Военный городок, 1 (Почта России)
75	Государственное казенное общеобразовательное учреждение "Волгоградская школа-интернат №4", ул. Лимоновая, 1 (Комитет образования ВО)
76	Муниципальное общеобразовательное учреждение «Основная школа № 59 имени полного кавалера ордена Славы Н.П. Красюкова», Веселая Балка, 62А
77	Государственное бюджетное учреждение здравоохранения "Волгоградский областной клинический центр медицинской реабилитации", ул. Санаторная, 29 (Комитет здравоохранения ВО)

78	Государственное бюджетное профессиональное образовательное учреждение «Волгоградский энергетический колледж», ул. Турбинная, 261 (Комитет образования ВО)
79	Государственное учреждение здравоохранения «Городская клиническая больница №1», Родильный дом № 3, ул. Федотова, 18 (Комитет здравоохранения ВО)

Приложение № 2 к техническому заданию

Аттестация Системы

Аттестация Системы включает:

1) Проведение испытаний ПЗИ объекта информатизации

В ходе испытаний объекта информатизации Исполнитель (при необходимости совместно с Заказчиком) проводит согласно утвержденным программам и методикам:

– опытную эксплуатацию ПЗИ Системы;

– анализ уязвимостей Системы;

– приемочные испытания ПЗИ Системы;

При проведении опытной эксплуатации проводится:

– опытная эксплуатация СрЗИ;

– устранение неисправностей и внесение изменений в документацию на ПЗИ, в том числе эксплуатационную, в соответствии с протоколами испытаний;

– оформление акта о завершении опытной эксплуатации;

Приемочные испытания ПЗИ проводятся с учетом ГОСТ 34.603 и включают проверку выполнения требований к ПЗИ в соответствии с требованиями на создание Системы.

При проведении приемочных испытаний проводится:

– испытания СрЗИ на правильность функционирования и соответствие техническому проекту;

– оформление протоколов приемочных испытаний.

2) Проведение аттестационных испытаний.

Проведение комплекса организационных и технических мероприятий (аттестационных испытаний) включает:

– оценку соответствия технического паспорта Системы, акта классификации Системы, состава и содержания эксплуатационной документации на ПЗИ и документов по защите информации Заказчика;

– оценку соответствия Системы и условий ее эксплуатации требованиям по защите информации;

– проверку наличия документов, содержащих результаты анализа уязвимостей, проведенного на этапах предварительных или приемочных испытаний ПЗИ;

– проверку наличия сведений об установленных СрЗИ в реестре сертифицированных СрЗИ, ведение которого осуществляет ФСТЭК России в соответствии с Положением о системе сертификации СрЗИ, утвержденным приказом ФСТЭК России от 3 апреля 2018 г. № 55, или документов, подтверждающих проведение оценки соответствия СрЗИ требованиям по безопасности информации в формах, отличных от сертификации;

– проверку наличия у Заказчика работников, ответственных за обеспечение защиты информации в ходе эксплуатации Системы, в том числе за проведение оценки угроз безопасности информации, управление (администрирование) системой защиты информации (администраторов безопасности), управление конфигурацией объекта информатизации, реагирование на инциденты, информирование и обучение персонала, контроль за обеспечением уровня защиты информации, а также проверку достаточности установленных для них обязанностей в соответствии с требованиями по защите информации;

– оценку уровня знаний и умений работников Заказчика, ответственных за обеспечение защиты информации, в соответствии с установленными для них обязанностями в эксплуатационной документации и документах по защите информации владельца объекта информатизации;

- оценку соответствия принятых организационных мер требованиям по защите информации и их достаточности для защиты от актуальных для Системы угроз безопасности информации;
- оценку соответствия принятых технических мер по защите информации от несанкционированного доступа (воздействия на информацию) требованиям по защите информации и их достаточности для защиты от актуальных для Системы угроз безопасности информации.

В результате аттестационных мероприятий Исполнителем подтверждается соответствие ПЗИ требованиям приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и иным нормативными правовыми актами в области защиты информации, в том числе в области защиты автоматизированных системах управления производственными и технологическими процессами.

Проведение аттестационных испытаний Системы лицами, осуществляющими проектирование и (или) внедрение ПЗИ, не допускается.

В соответствии с п .11 приказа ФСТЭК от 29.04.2021 г. № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну» (далее – Приказ № 77) в качестве исходных данных, необходимых для аттестации Системы, используются предоставляемые не позднее 30 дней с момента передачи Исполнителем разработанных проектов документов, утвержденные/согласованные Заказчиком следующие документы или их копии:

- технический паспорт на Системы;
- акт классификации Системы;
- утвержденная (согласованная) Заказчиком модель угроз безопасности информации;
- техническое задание создание (развитие, модернизацию) Системы и (или) частное техническое задание на создание (развитие, модернизацию) ПЗИ Системы;
- проектная документацию на ПЗИ Системы;
- эксплуатационная документация на ПЗИ Системы и применяемые СрЗИ;
- организационно-распорядительные документы по защите информации, регламентирующие защиту информации в ходе эксплуатации Системы, в том числе план мероприятий по защите информации Системы, документы по порядку оценки угроз безопасности информации, управлению (администрированию) ПЗИ, управлению конфигурацией Системы, реагированию на инциденты безопасности, информированию и обучению персонала, контролю за обеспечением уровня защищенности информации.
- документы, содержащие результаты анализа уязвимостей Системы и приемочных испытаний ПЗИ Системы;
- иные документы, разрабатываемые в процессе проектирования ПЗИ

По решению Заказчика вышеуказанные документы (их копии) представляются Исполнителю в виде электронных документов либо в бумажном виде.

Аттестация проводится в соответствии с утвержденной программой и методиками аттестационных испытаний. Для проведения аттестации Системы применяются национальные стандарты, а также методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. №1085.

При проведении аттестационных испытаний должны применяться следующие методы проверок (испытаний):

- экспертно-документальный метод, предусматривающий проверку соответствия ПЗИ установленным требованиям по защите информации, на основе оценки

эксплуатационной документации, организационно-распорядительных документов по защите информации, а также условий функционирования Системы;

- анализ уязвимостей Системы, в том числе вызванных неправильной настройкой (конфигурированием) программного обеспечения и СрЗИ;
- испытания ПЗИ путем осуществления попыток несанкционированного доступа (воздействия) к Системе в обход ее ПЗИ.

По результатам аттестационных испытаний оформляются:

- протоколы аттестационных испытаний;
- заключение по результатам аттестационных испытаний о соответствии Системы требованиям о защите информации;
- аттестат соответствия (в случае положительных результатов аттестационных испытаний). Аттестат соответствия выдается на весь срок эксплуатации Системы.

Заключение и протоколы в течение 5 рабочих дней после утверждения Исполнителем направляются Заказчику.

В случае выявления в ходе аттестационных испытаний недостатков, которые можно устранить в процессе аттестации Системы, Заказчик обеспечивает их устранение, а Исполнитель оценивает качество такого устранения.

В случае выявления при проведении аттестационных испытаний недостатков, которые невозможно устранить в процессе аттестации Системы, работы по аттестации Системы завершаются, аттестат соответствия не оформляется.

Срок выполнения работ по данному этапу не позднее 90 календарных дней после заключения Договора.

В соответствии с п. 27 Приказа № 77 Исполнитель обязан в течение 5 рабочих дней после подписания аттестата соответствия направить во ФСТЭК России копии следующих документов:

- аттестата соответствия;
- технического паспорта;
- акта классификации Системы;
- программы и методик аттестационных испытаний;
- заключения и протоколов.

Приложение № 3 к техническому заданию

Технические условия на сопряжение с РАСЦО Волгоградской области

ТЕХНИЧЕСКИЕ УСЛОВИЯ
на подключение (присоединение) муниципальной автоматизированной системы централизованного оповещения населения
городского округа города Волгограда
к региональной автоматизированной системе централизованного оповещения населения Волгоградской области

"__"_____20__г. № _____

1. Общая информация	
1.1. Заказчик технических условий (ТУ)	**Муниципальное казенное учреждение «Центр обеспечения мероприятий гражданской защиты Волгограда» (МКУ «ЦОМ ГЗ Волгограда»)**
1.2. Исходящий номер и дата заявки	
2. Технические условия на подключение (присоединение) МАСЦО к региональной автоматизированной системе централизованного оповещения населения Волгоградской области (далее - РАСЦО)	
2.1. Назначение МАСЦО	Присоединение осуществляется в соответствии с требованиями совместного Приказа МЧС России, Минцифры России 31.07.2020 № 578/365 "Об утверждении Положения о системах оповещения населения", "Методических рекомендаций по созданию и реконструкции систем оповещения населения", утвержденных МЧС РФ 19.02.2021.
2.2 Границы зоны оповещения	Перечень объектов экономики, населенных пунктов, подлежащих оповещению и попадающих в зону действия МАСЦО определяются в процессе проектирования и должен быть согласован с территориальным органом МЧС России и утвержден в порядке, установленном органом местного самоуправления.
2.3 Требования к оборудованию МАСЦО	Технические средства оповещения МАСЦО должны соответствовать следующим требованиям: 1. ГОСТ Р 42.3.01-2021 "Гражданская оборона. Технические средства оповещения населения. Классификация. Общие технические требования". 2. ГОСТ Р 22.1.12-2005 "Безопасность в чрезвычайных ситуациях. Структурированная система мониторинга и управления инженерными системами зданий и сооружений. Общие требования" 3. МАСЦО должна быть построена (реконструирована) на основе комплексов технических средств оповещения населения, прошедших государственные испытания в МЧС

	России и предназначенных для создания автоматизированных систем оповещения. Необходимые технические средства оповещения МАСЦО определяются в ходе разработки проектной документации из расчета показателей гарантированного оповещения органов управления, сил РСЧС (ГО) и населения, с учетом действующего оборудования в субъекте Российской Федерации в целях сопряжения автоматизированных систем оповещения на всех уровнях. 4. МАСЦО должна обеспечить техническую и программную совместимость с пунктами управления оповещением ДДС Волгоградской области, которые представляют собой комплекс технических средств оповещения П-166 ИТК ОС АРМ ОД и действующим оборудованием, входящим в состав РАСЦО. 5. Присоединяемая МАСЦО должна обеспечивать: - прием сигналов управления, передаваемых с основного и запасного пунктов управления РАСЦО, а также с автоматизированного рабочего места (далее АРМ) РАСЦО в зоне действия МАСЦО; - автоматическое индивидуальное/ избирательное/ циркулярное исполнение команд, передаваемых с основного и запасного пунктов управления РАСЦО, а также с АРМ РАСЦО в зоне действия МАСЦО; - ретрансляцию сигналов "Внимание всем" и последующего речевого сообщения в систему речевого оповещения МАСЦО, передаваемых с основного и запасного пунктов управления РАСЦО, а также с АРМ РАСЦО в зоне действия МАСЦО; - передачу в основной и запасной пункты управления РАСЦО, а также на АРМ РАСЦО в зоне действия МАСЦО, квитанций подтверждения выполнения команд всем оборудованием, входящим в состав МАСЦО; - индивидуальный/ избирательный/ циркулярный запуск оповещения дежурной сменой на территории, входящей в зону МАСЦО, включая запуск оборудования, входящего в состав МАСЦО и входящего в состав РАСЦО и обеспечивающего звукопокрытие зоны МАСЦО; - автоматическое доведение информации о запуске оповещения дежурной сменой и результатах отработки в РАСЦО основного и запасного пунктов управления, а также в АРМ РАСЦО в зоне действия МАСЦО;

	- дистанционную проверку работоспособности аппаратуры, каналов связи и систем управления (индивидуальной/ избирательной/ циркулярной) под управлением дежурной смены или по запросам основного и запасного пунктов управления РАСЦО, а также с АРМ РАСЦО в зоне действия МАСЦО; - цифровую диспетчерскую связь с записью переговоров с основного и запасного пунктов управления РАСЦО, а также с АРМ РАСЦО в зоне действия МАСЦО.
2.4 Требования к оконечным техническим средствам оповещения	Комплексы оповещения должны быть предназначены для построения систем озвучивания зданий, сооружений и открытых пространств, а также систем локального оповещения. Комплексы оповещения должны обеспечивать: автономное электропитание при отключении электросети не менее 6 ч в режиме ожидания и не менее 1 ч в рабочем режиме. Места установки, количество, мощность оконечных средств оповещения определяются в процессе проектирования.
2.5 Требования по подключению (присоединению) МАСЦО к РАСЦО	МАСЦО должна подключаться к РАСЦО через сопряжение с серверной группой оповещения, которая расположена по адресу: г. Волгоград, ш. Авиаторов, 2 в здании единого центра обработки данных Волгоградской области. От МАСЦО до серверной инфраструктуры РАСЦО должен быть организован защищенный канал связи не менее 10 Мб/с. Должна быть обеспечена возможность управления оконечными средствами оповещения в зоне действия МАСЦО осуществляться с АРМ РАСЦО в ДДС Волгоградской области. Владелец МАСЦО должен разработать и заключить с Администрацией Волгоградской области Соглашение об информационном обмене в случаях наступления ЧС и повседневной деятельности. Владелец МАСЦО должен разработать и утвердить Регламент действий дежурных смен МАСЦО в случаях наступления ЧС и повседневной деятельности. Регламент должен быть согласован с администрацией Волгоградской области.
2.6 Способ передачи сигналов и информации оповещения	автоматизированный
3. Требования по проведению организационно-технических мероприятий по исключению несанкционированного задействования систем оповещения населения	
Требования по проведению организационно-технических мероприятий по исключению несанкционированного	Все работы, проводимые по сопряжению МАСЦО с РАСЦО, должны выполняться таким образом, чтобы исключить несанкционированные доступ и задействование систем оповещения, как на этапе

доступа и задействования систем оповещения населения	проведения работ по присоединению (подключению), так и на этапе их эксплуатации. МАСЦО должна соответствовать следующим требованиям: 1. Подключаемая МАСЦО должна соответствовать требованиям, предъявляемым к государственным информационным системам не ниже класса защищенности К2 в соответствии с приказом ФСТЭК России от 11.02.2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах". 2. Подключение МАСЦО должно быть осуществлено по защищенным каналам связи с использованием средств криптографической защиты информации семейства ViPNet Coordinator HW 4 (класс не ниже КС3) с действующим сертификатом соответствия ФСТЭК и/или ФСБ. 3. При эксплуатации владелец МАСЦО обеспечивает наличие действующих сертификатов технической поддержки средств защиты информации для осуществления обновления программных и программно-технических средств защиты информации.
4.Требования по обеспечению готовности МАСЦО к действиям по предназначению	
Требования по обеспечению готовности МАСЦО к действиям по предназначению	Технические средства оповещения и линии связи (линии управления) МАСЦО должны находиться в режиме постоянной готовности к передаче сигналов и информации оповещения и обеспечивать возможность автоматизированного включение (запуска) оконечных средств оповещения МАСЦО по сигналам оперативного дежурного ДДС Волгоградской области.
5. Срок действия технических условий	
Срок действия технических условий	с даты выдачи настоящих технических условий по **31.12.2024**

СПЕЦИФИКАЦИЯ

№ п/п	Наименование	Ед. изм.	Кол-во
1	**Программное обеспечение, в составе:**		
1.1	СЗИ. Неисключительные права на расширение функционала программного обеспечения, выполняющего функции системы централизованного управления политиками безопасности для отдельных узлов и групп узлов защищенной сети ViPNet Policy Manager (Запись в реестре отечественного ПО №2470 от 23.12.2016)	Шт.	114
1.2	СЗИ. Неисключительное право на использование модуля обнаружения и предотвращения вторжений Средства защиты информации Secret Net Studio 8 (Запись в реестре отечественного ПО №№3855 от 16.08.2017)	Шт.	1
1.3	СЗИ. Неисключительное право на использование средств анализа защищенности «Сканер-ВС» (Запись в реестре отечественного ПО №231 от 18.03.2016)	Шт.	1
1.4	СЗИ. Установочный комплект права на использование средств анализа защищенности «Сканер-ВС»	Шт.	1
1.5	СЗИ. Права на использование средств антивирусной защиты информации Kaspersky Endpoint Security для бизнеса – Стандартный (Запись в реестре отечественного ПО №205 от 18.03.2016)	Шт.	10
1.6	СЗИ. Установочный комплект права на использование средств антивирусной защиты информации Kaspersky Endpoint Security для бизнеса – Стандартный	Шт.	1
2	**Работы, в составе:**		
2.1	Работы по 1 этапу	Шт.	1
2.2	Работы по 2 этапу	Шт.	1

ГРАФИК ИСПОЛНЕНИЯ ОБЯЗАТЕЛЬСТВ И СТОИМОСТЬ ЭТАПОВ

№	Наименование этапа	Сроки исполнения обязательств	НМЦ Этапа работ, руб.
1 этап	- передача, монтаж, подключение к электропитанию и пусконаладка оборудования и программного обеспечения СЗИ по адресам согласно Приложению №1 к техническому заданию - создание подсистемы защиты информации в соответствии с требованиями п.4.3. технического задания	не позднее 28.12.2023	6 955 250 руб. включает в себя: - стоимость лицензий 55 125 руб. (НДС не облагается в соответствии с пп. 26 п. 2 ст. 149 Налогового кодекса РФ) - 6 900 125 руб. с НДС
2 этап	- передача, монтаж, подключение к электропитанию и пусконаладка оборудования и программного обеспечения СЗИ по адресам согласно Приложению №1 к техническому заданию - создание подсистемы защиты информации в соответствии с требованиями п.4.3. технического задания - аттестация МАСЦО - разработка документации	не позднее 28.12.2024	15 958 204,88 руб. включает в себя: - стоимость лицензий 154 895,13 руб. (НДС не облагается в соответствии с пп. 26 п. 2 ст. 149 Налогового кодекса РФ) - 15 803 309,75 руб. с НДС
ИТОГО, руб.:			22 913 454,88