Приложение № 12
к приказу областного
государственного казённого
учреждения «Центр по сопровождению
закупок»
от 27.10.2023 № 39

УТВЕРЖДАЮ

Директор
ОГКУ «Центр по сопровождению закупок»
_____ А.С. Ахметшин
«27» 10 2023 г.

Регламент
взаимодействия со сторонними информационными системами и внешними пользователями

Ульяновск
2023

Оглавление

Термины, определения и сокращения

Автоматизированная обработка – обработка информации с помощью средств вычислительной техники.

Автоматизированная система (АС) - система, состоящая из комплекса средств автоматизации, реализующего информационную технологию выполнения установленных функций, и персонала, обеспечивающего его функционирование (Межгосударственный стандарт ГОСТ 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»).

Автоматизированное рабочее место (АРМ) - Программно-технический комплекс АС, предназначенный для автоматизации деятельности определенной категории пользователей или определенного вида деятельности. (Межгосударственный стандарт ГОСТ 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»).

Администратор безопасности - лицо, ответственное за защиту автоматизированной системы от несанкционированного доступа к информации (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К).

Безопасность информации [данных] - состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Вспомогательные технические средства и системы (ВТСС) - технические средства исистемы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с основными техническими средствами и системами или в защищаемых помещениях (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К).

Защита информации от несанкционированного доступа (ЗИ от НСД) - защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Защита информации от разглашения - защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и

определения»).

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Носитель защищаемой информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Основные технические средства и системы (ОТСС) - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К).

Система защиты информации (СЗИ) - совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины иопределения»).

Средство защиты информации (СрЗИ) - техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Физическая защита информации - защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

1. Общие положения

1.1 Настоящий «Регламент о взаимодействии со сторонними информационными системами и внешними пользователями» ОГКУ «Центр по сопровождению закупок» определяет порядок взаимодействия информационных систем и внешних пользователей, принадлежащих иным ведомствам и организациям, с государственной информационной системой автоматизации процесса управления государственными закупками Ульяновской области «АЦК-Госзаказ» (далее – ГИС АЦК-Госзаказ») в соответствии с законодательством Российской Федерации.

1.2 Настоящий Регламент разработан в соответствии с Приказом Федеральной службы по техническому и экспортному контролю № 17 от 11 февраля 2013 года «Требования по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.3 Действие настоящего Регламента распространяется на работников ОГКУ «Центр по сопровождению закупок» и работников владельцев информационных систем, заинтересованных во взаимодействии с ГИС «АЦК-Госзаказ».

2 Порядок подключения к ГИС

Процедура подключения состоит из следующих шагов:

2.1. Предоставление Оператору ГИС заявки на подключении к ГИС. В заявке должна быть указана цель подключения, предполагаемый вариант подключения, описание информационной системы, ее класс защищенности, информация об используемых мерах защиты, включая информацию о выполнении требований по защите информации и используемых средствах криптографической защиты, информация об ответственных лицах и документ, подтверждающий выполнение требований безопасности информации.

2.2 Документом, подтверждающим выполнение требований безопасности информации, может быть

a. аттестат соответствия требованиям безопасности информации, предъявляемым к государственным информационным системам 3 класса защищенности (К3), с использованием сертифицированных СрЗИ по требованиям безопасности информации ФСТЭК России не ниже чем по 6 (шестому) уровню доверия и сертифицированных СКЗИ по требованиям безопасности информации ФСБ России – схема защищенного взаимодействия №1 с ГИС «АЦК-Госзаказ»;
b. заключение об оценке эффективности принимаемых мер защиты информации (далее – заключение), предъявляемым к государственным информационным системам третьего класса защищенности (К3), с использованием сертифицированных СрЗИ по требованиям

безопасности информации ФСТЭК России не ниже чем по 6 (шестому) уровню доверия и сертифицированных СКЗИ по требованиям безопасности информации ФСБ России – схема защищенного взаимодействия №2 с ГИС «АЦК-Госзаказ»;

c. документ, подтверждающий соответствие подключаемой информационной системы типовому сегменту «Внешний пользователь (вариант подключения №1)» или типовому сегменту «Внешний пользователь (вариант подключения №2) – схема защищенного взаимодействия №3 с ГИС «АЦК-Госзаказ».

В данном документе должны быть перечислены:

1. используемые технические средства подключаемой информационной системы (далее – ИС);
2. сертифицированные средства защиты информации с серийными номерами (знаками соответствия), используемые для защиты информации в ИС;
3. копии актов установок средств защиты информации ИС;
4. скриншоты настроек средств защиты информации ИС;
5. протоколы по анализу защищенности ИС, полученные с помощью сертифицированного средства анализа защищенности. Из протоколов должно следовать, что в ИС отсутствуют критические и высокие информационные уязвимости, либо должны быть представлены компенсирующие меры, снижающие вероятность эксплуатации данных уязвимостей;
6. протоколы инвентаризации, полученные с помощью сертифицированного средства анализа защищенности;
7. утвержденный пакет организационно-распорядительной документации, реализующий организационные меры, необходимые при обеспечении безопасности информации в ГИС «АЦК-Госзаказ».

2.3. Требования к реализации защищенного взаимодействия.

2.3.1. Требования к реализации защищенного взаимодействия в соответствии со схемой защищенного взаимодействия №1.

1) Подключаемая ИС должна иметь действующий аттестат соответствия требованиям безопасности информации, предъявляемым к государственным информационным системам 3 класса защищенности (К3) с использованием сертифицированных СрЗИ по требованиям ФСТЭК России не ниже чем по 6 (шестому) уровню доверия и сертифицированных СКЗИ по требованиям безопасности информации ФСБ России.

2) Подключаемая ИС должна использовать СКЗИ, совместимые со средствами, применяемыми в ГИС «АЦК-Госзаказа» (ПАК «ViPNet Coordinator HW» или ViPNet

Client). В целях организации защищенного канала связи с ГИС «АЦК-Госзаказа» должно быть использовано сертифицированное или имеющее положительное заключение ФСБ России СКЗИ с классом криптографической защиты не ниже КС3. Подключение ИС к ГИС «АЦК-Госзаказа» должно быть реализовано только посредством данного СКЗИ.

3) С целью обеспечения безопасного межсетевого взаимодействия ИС с ГИС «АЦК-Госзаказа» должно быть использовано средство МЭ, имеющее сертификат соответствия требованиям документов: Требования доверия (4), Требования к МЭ, Профиль защиты МЭ(А четвертого класса защиты. ИТ.МЭ.А4.ПЗ), Профиль защиты МЭ (Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ).

4) Помещения для размещения технических средств СКЗИ и средства МЭ должны удовлетворять требованиям ТУ и ЭД на данные средства.

6)Установка, монтаж, запуск и первоначальная настройка СКЗИ и средства МЭ должны быть проведены в заданных помещениях в соответствии с требованиями ТУ и ЭД на данные средства.

7) Эксплуатация СКЗИ и средств МЭ должна осуществляться в соответствии с требованиями ЭД на данные средства.

8) Среди средств защиты информации, используемых ИС, обязательно должны быть сертифицированные СрЗИ по требованиям ФСТЭК России не ниже чем по 6 (шестому) уровню доверия:

1. антивирусное средство;
2. средство защиты от несанкционированного доступа (если защита от несанкционированного доступа не реализована в рамках сертифицированной информационной системы);
3. средство анализа защищенности;
4. межсетевой экран.

2.3.2. Требования к реализации защищенного взаимодействия в соответствии со схемой защищенного взаимодействия №2.

1) Подключаемая ИС должна иметь заключение об оценке эффективности принимаемых мер защиты информации (далее – заключение), предъявляемым к государственным информационным системам третьего класса защищенности (К3). Заключение об оценке эффективности принятых мер защиты информации может быть оформлен владельцем ИС. В случае отсутствия у владельца ИС необходимых специалистов по защите информации, он может привлекать организации, имеющие лицензию ФСТЭК России по технической защите информации, для выполнения необходимых работ и оформлению данного

документа.

2) Подключаемая ИС должна использовать СКЗИ, совместимые со средствами, применяемыми в ГИС «АЦК-Госзаказа» (ПАК «ViPNet Coordinator HW» или ViPNet Client). В целях организации защищенного канала связи с ГИС «АЦК-Госзаказа» должно быть использовано сертифицированное или имеющее положительное заключение ФСБ России СКЗИ с классом криптографической защиты не ниже КС3. Подключение ИС к ГИС «АЦК-Госзаказа» должно быть реализовано только посредством данного СКЗИ.

3) С целью обеспечения безопасного межсетевого взаимодействия ИС с ГИС «АЦК-Госзаказа» должно быть использовано средство МЭ, имеющее сертификат соответствия требованиям документов: Требования доверия (4), Требования к МЭ, Профиль защиты МЭ (А четвертого класса защиты. ИТ.МЭ.А4.ПЗ), Профиль защиты МЭ (Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ).

4) Помещения для размещения технических средств СКЗИ и средства МЭ должны удовлетворять требованиям ТУ и ЭД на данные средства.

6)Установка, монтаж, запуск и первоначальная настройка СКЗИ и средства МЭ должны быть проведены в заданных помещениях в соответствии с требованиями ТУ и ЭД на данные средства.

7) Эксплуатация СКЗИ и средств МЭ должна осуществляться в соответствии с требованиями ЭД на данные средства.

8) Среди средств защиты информации, используемых ИС, обязательно должны быть сертифицированные СрЗИ по требованиям ФСТЭК России не ниже чем по 6 (шестому) уровню доверия:

1. антивирусное средство;
2. средство защиты от несанкционированного доступа (если защита от несанкционированного доступа не реализована в рамках сертифицированной информационной системы);
3. средство анализа защищенности;
4. межсетевой экран.

2.3.3. Требования к реализации защищенного взаимодействия в соответствии со схемой защищенного взаимодействия №3.

Возможны два варианта защищенного взаимодействия ИС с ГИС «АЦК-Госзаказ» в соответствии со схемой защищенного взаимодействия №3.

2.3.3.1. Вариант подключения № 1

Обеспечивается защищенное взаимодействия ИС с ресурсами ГИС «АЦК-Госзаказ» со стационарных АРМ в рамках локально-вычислительной сети (сегмента ЛВС), расположенной в

пределах контролируемой зоны ИС.

Данный вариант предполагает подключение ЛВС внешнего пользователя (сегмента ЛВС) к защищенной сети, к которой подключена ГИС «АЦК-Госзаказ» (сеть ViPNet № 10883) через программно-аппаратный комплекс «ViPNet Coordinator HW x» (далее – ПАК «ViPNet Coordinator HW x»), устанавливаемый на стороне ИС.

ПАК «ViPNet Coordinator HW x» должен обладать действующим сертификатом соответствия требованиям по безопасности ФСБ России. Выбор модели ПАК «ViPNet Coordinator HW x» для подключения ЛВС (сегмента ЛВС) к защищенной сети ГИС «АЦК-Госзаказ» осуществляется владельцем ИС с учетом пропускной способности канала связи и требуемой производительности.

Администрирование ПАК «ViPNet Coordinator HW x» на стороне ИС осуществляется его специалистами, назначенными приказом руководителя.

Для настройки обмена данными между ИС и ресурсами ГИС «АЦК-Госзаказ», ИС должна соответствовать сегменту ГИС «АЦК-Госзаказ», прошедшему аттестационные испытания (сегмент «Внешний пользователь (вариант подключения №1»). ИС считается соответствующая сегменту «Внешний пользователь (вариант подключения №1», если для ИС и сегмента «Внешний пользователь (вариант подключения №1» установлены одинаковые классы защищенности, угрозы безопасности информации, реализованы одинаковые проектные решения по информационной системе и ее системе защиты информации.

Соответствие ИС, на которую распространяется аттестат соответствия, сегменту «Внешний пользователь (вариант подключения №1», подтверждается в ходе приемочных испытаний ИС.

В ИС должно обеспечивается соблюдение эксплуатационной документации на систему защиты информации ГИС «АЦК-Госзаказ» и организационно-распорядительных документов по защите информации.

Требования средствам защиты информации ИС:

1) Средство защиты информации от несанкционированного доступа, имеющее сертификат ФСТЭК по требованиям безопасности информации Secret Net Studio;
2) Межсетевой экран, имеющий сертификат ФСТЭК или ФСБ Secret Net Studio;
3) Сертифицированное антивирусное средство Dr.Web Enterprise Security Suite;
4) Сертифицированное средство анализа защищенности RedCheck или xSpider;

Данный вариант подключения не подходит при наличии на стороне внешнего пользователя мобильных устройств пользователей (смартфоны, планшетные ПК) или АРМ пользователей, расположенных за пределами контролируемой зоны, для которых требуется обеспечить защищенную работу с ресурсами ГИС АЦК-Госзаказ.

2.3.3.2. Вариант подключения № 2

Обеспечивается защищенное взаимодействия ИС с ресурсами ГИС «АЦК-Госзаказ» со стационарных АРМ.

Данный вариант предполагает подключение стационарных АРМ при помощи программного обеспечения СКЗИ «ViPNet Client» в целях защиты канала связи до центрального узла доступа ГИС «АЦК-Госзаказ» (ПАК «ViPNet Coordinator HW 4»).

Для настройки обмена данными между ИС и ресурсами ГИС «АЦК-Госзаказ», ИС должна соответствовать сегменту ГИС «АЦК-Госзаказ», прошедшему аттестационные испытания (сегмент «Внешний пользователь (вариант подключения №2»). ИС считается соответствующая сегменту «Внешний пользователь (вариант подключения №2», если для ИС и сегмента «Внешний пользователь (вариант подключения №1» установлены одинаковые классы защищенности, угрозы безопасности информации, реализованы одинаковые проектные решения по информационной системе и ее системе защиты информации.

Соответствие ИС, на которую распространяется аттестат соответствия, сегменту «Внешний пользователь (вариант подключения №2», подтверждается в ходе приемочных испытаний ИС.

В ИС должно обеспечивается соблюдение эксплуатационной документации на систему защиты информации ГИС «АЦК-Госзаказ» и организационно-распорядительных документов по защите информации.

Требования средствам защиты информации ИС:

5) Средство защиты информации от несанкционированного доступа, имеющее сертификат ФСТЭК по требованиям безопасности информации Secret Net Studio;
6) Межсетевой экран, имеющий сертификат ФСТЭК или ФСБ, Secret Net Studio;
7) Антивирусное средство - модуль антивирусной защиты Secret Net Studio;
8) Сертифицированное средство анализа защищенности RedCheck;

2.4. Информация, содержащаяся в заявке, проверяется ответственными лицами ОГКУ «Центр по сопровождению закупок», которые принимают решение о возможности взаимодействия с внешней информационной системой

2.5. Выполняется организация защищенного канала связи с использованием сертифицированных СКЗИ VipNet (класс криптографической защиты не ниже КС3)

2.6. Производится тестирование защищенного канала связи, по результатам которого оформляется акт технической готовности к защищенному взаимодействию.

2.7. Производится организация подключения к ГИС внешней информационной системой в тестовом режиме, включая формирование временных пар «логин-пароль» к ГИС. При этом администраторы ГИС проводят постоянный контроль запросов внешней информационной

системы и передаваемых данных.

2.8. При отсутствии инцидентов информационной безопасности и подозрений в нарушении политики информационной безопасности ОГКУ ««Центр по сопровождению закупок»» принимается решение о взаимодействии с ГИС внешней информационной системы в рабочем режиме.

3 Порядок взаимодействия с ГИС

3.1. Работа пользователей ИС с ресурсами ГИС производится только через штатный WEB интерфейс ГИС «АЦК-Госзаказ», доступный в защищенной сети по ip адресу: 192.168.0.103 или соответствующий ему виртуальный адрес сети ViPNet.

3.2. При работе со штатным WEB интерфейсом ГИС «АЦК-Госзаказ» пользователи ИС руководствуются «Инструкцией пользователя ГИС» и актуальными эксплуатационными документами ГИС «АЦК-Госзаказ».

3.3. ОГКУ «Центр по сопровождению закупок» в лице администратора безопасности организует ознакомление под роспись пользователей ИС с необходимыми организационными документами и особенностями взаимодействия с программными и аппаратными средствами ГИС.

3.4. ОГКУ «Центр по сопровождению закупок» имеет право осуществлять необходимый контроль деятельности внешних пользователей и прекращать их деятельность в случае выявления обоснованных подозрений в нарушении мер безопасности. В этом случае ОГКУ Центр по сопровождению закупок» и владелец ИС организовывают совместную комиссию по расследованию возможного инцидента информационной безопасности, руководствуясь в т.ч. регламентом по расследованию инцидентов ОГКУ «Центр по сопровождению закупок».

3.5. В целом ОГКУ «Центр по сопровождению закупок»» и владелец ИС обязуются обмениваться любой информацией о возможных инцидентах информационной безопасности зоне их совместной ответственности.

4 Порядок отключения информационной системы

4.1 Процедура отключения ИС состоит из следующих шагов:

4.1.1. Предоставление Оператору ГИС заявки на отключение ИС, подписанной руководителем владельца ИС.

4.1.2. Удаление идентификационной и авторизационной информации ИС из базы данных ГИС.

4.1.3. Удаление информации (маршрутов) о подключении ИС по защищенной сети VipNet.

4.2. Отключение ИС может быть произведено администраторами ГИС принудительно при наличии обоснованных подозрений о возможности совершения компьютерных атак в отношении ГИС с использованием ресурсов внешней системы.

5. Порядок внесения изменений

5.1. Регламент подлежит полному пересмотру при изменении актуальных угроз безопасности информации в ГИС «АЦК-Госзаказ», при проведении дополнительных аттестационных испытаниях или повторной аттестации ГИС «АЦК-Госзаказ».

5.2. Регламент подлежит частичному пересмотру в следующих случаях:

- в целях повышения эффективности мероприятий, определенных в настоящем Регламенте;

-при изменении состава, обязанностей и полномочий должностных лиц ОГКУ «Центр по сопровождению закупок», которые задействованы в мероприятиях настоящему Регламенту.

5.3. Полный пересмотр данного документа проводится администраторами безопасности, руководителем ОГКУ «Центр по сопровождению закупок» с целью проверки соответствия определенныхданным документом мер защиты реальным условиям применения их в ГИС «АЦК-Госзаказ».

5.4. Частичный пересмотр данного документа проводится администраторами безопасности. Частичный пересмотр не должен затрагивать вопросов, касающихся применения в ИС средств защиты информации, условий соответствия ИС типовым сегмента ГИС «АЦК-Госзаказ», описанных в аттестационных документах. При частичном пересмотре могут быть добавлены, удалены или изменены приложения Регламента с обязательным указанием оснований и внесенных изменений в «Листе регистрации изменений в Регламенте» (Приложение 2) без переутверждения всего Регламента.

Приложение № 1

Лист ознакомления

№ п/п	Ф.И.О.	Роспись	Дата
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			
26.			
27.			
28.			
29.			

30.			
31.			
32.			
33.			
34.			
35.			
36.			

Приложение № 2

Лист регистрации изменений

№ п/п	Описание внесенного изменения	ФИО лица	Роспись	Дата
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				

20.				
21.				
22.				
23.				
24.				
25.				
26.				
27.				
28.				
29.				
30.				
31.				
32.				
33.				
34.				
35.				
36.				