

Государственное казенное учреждение Сахалинской области
«Центр региональной цифровой трансформации»
(лицензия на деятельность по технической защите конфиденциальной информации № 2629 от 10.06.2015)

УТВЕРЖДАЮ

Руководитель государственного
казенного учреждения Сахалинской
области «Центр региональной
цифровой трансформации»


Р.В. Чужинов
«15» _____ 2021 г.

Технические условия

**подключения информационных систем
к государственной информационной системе
«Автоматизированная информационная система «Предоставление
государственных и муниципальных услуг в электронной форме»**

Введение

Государственная информационная система «Автоматизированная информационная система «Предоставление государственных и муниципальных услуг в электронной форме» (далее – ГИС) соответствует требованиям безопасности информации, предъявляемым к государственным информационным системам **третьего** класса защищенности, а также требованиям, предъявляемым к информационным системам персональных данных для которых необходимо обеспечить **третий** уровень защищенности персональных данных.

Требования настоящих технических условий устанавливают состав, содержание, а также порядок выполнения работ по подключению внешних пользователей и информационных систем (далее – ИС) сторонних организаций, а также состав программно-технических средств, в том числе средств защиты информации, необходимых для организации защищенного взаимодействия с ГИС.

Предоставление доступа к техническим и программным средствам ГИС возможно только после выполнения требований, указанных в настоящем документе.

1. Основные положения

1.1 Общее описание информационного обмена

Обмен информацией между ГИС и ИС сторонних организаций осуществляется в электронной форме с использованием шифрованного канала связи (VPN-сетей).

В ГИС для защиты информации конфиденциального характера используются сертифицированные криптографические средства на базе продуктов семейства ViPNet Coordinator. Для организации защищенного взаимодействия используется ViPNet-сеть № 2593. Владелец ViPNet-сети является государственным казенным учреждением Сахалинской области «Центр региональной цифровой трансформации» (далее – ГКУ СО «ЦРЦТ»).

1.2 Общие требования по защите информации

Хранение, обработка и обмен информацией, содержащейся в ГИС должны осуществляться после принятия необходимых мер по защите информации от компрометации, повреждения или утраты, предусмотренных нормативными правовыми актами Российской Федерации в области защиты информации.

Руководителями сторонних организаций должны быть назначены лица, ответственные за внесение сведений в ГИС, а также лица, ответственные за обеспечение организации защищенного взаимодействия с ГИС.

Для организации защищенного взаимодействия ИС сторонней организации с ГИС, в ИС должны быть выполнены организационные и технические мероприятия, подтверждающие соответствие системы защиты информации ИС сторонней организации требованиям безопасности информации.

2. Организационные требования

Организация подключения к ГИС должна осуществляться в соответствии с:

- требованиями нормативно-правовых актов Российской Федерации в сфере защиты информации;
- требованиями нормативно-технических и методических документов уполномоченных органов исполнительной власти Российской Федерации в сфере обеспечения безопасности информации (федеральная служба по техническому и экспортному контролю (далее - ФСТЭК) России, федеральная служба безопасности (далее - ФСБ) России;
- требованиями настоящих технических условий.

До начала выполнения работ по подключению ИС сторонней организации к ГИС схема защищенного взаимодействия должна быть согласована с ГКУ СО «ЦРЦТ».

Для организации взаимодействия, подключаемая организация предоставляет в ГКУ СО «ЦРЦТ» официальное письмо, содержащее запрос на подключение к ГИС, в составе которого отражено:

- наименование подключаемой системы с указанием ip-адресов подключаемых серверов/АРМ;
- сведения о контактном лице для организации канала связи;
- информация о наличии действующего аттестата соответствия требованиям безопасности информации, подтверждающий ее соответствие требованиям, предъявляемым к ГИС **третьего** класса защищенности, а также требованиям, предъявляемым к информационным системам персональных данных для которых необходимо обеспечить **третий** уровень защищенности персональных данных.

В случае отсутствия аттестата соответствия требованиям безопасности для подключаемой ИС, необходимо самостоятельно или с привлечением

сторонней организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации, провести мероприятия по оценке соответствия ИС изложенным в настоящем документе требованиям. По результатам оценки должен быть составлен акт в соответствии с формой в Приложении 1 к текущему документу.

В случае проведения повторной аттестации ИС, подключенной к ГИС, владелец ИС обязан предоставить в ГКУ СО «ЦРЦТ» скан-копию действующего аттестата соответствия.

3. Технические требования

Взаимодействие ИС сторонней организации с ГИС должно осуществляться с использованием программно-аппаратного средства криптографической защиты информации семейства ViPNet Coordinator, имеющего доступ к ViPNet-сети № 2593.

Автоматизированные рабочие места (далее - АРМ) и сервера, входящие в состав подключаемой ИС, должны быть оснащены сертифицированными ФСТЭК России по требованиям безопасности информации средствами защиты, удовлетворяющими требованиям части 2 текущего документа:

- средство защиты от несанкционированного доступа;
- средство межсетевого экранирования;
- средство антивирусной защиты.

Параметры настройки средств защиты информации должны обеспечивать:

- идентификацию и аутентификацию пользователей системы с использованием персональных логина и пароля, либо персонального аппаратного идентификатора и пароля;
- разграничение доступа пользователей по работе в ИС;
- регистрацию событий безопасности;

- контроль подключения устройств. Определение разрешенных для подключения к ИС устройств;
- фильтрацию входящего и исходящего сетевого трафика в соответствии с заданными правилами.

Базы антивирусных сигнатур должны находиться в актуальном состоянии. Обновление антивирусных баз должно производиться на постоянной периодической основе, обеспечивающей реагирования на актуальные вредоносные программы.

Режим доступа в помещения, в которых расположены технические средства, входящие в состав ИС, подключаемой к ГИС, должен исключать возможность бесконтрольного пребывания лиц, не имеющих права самостоятельного доступа в данные помещения.

4. Контроль реализации подключения к ГИС

Ответственность за соблюдение требований настоящих технических условий, обеспечение защиты информации в ходе эксплуатации подключаемой ИС сторонней организации, АРМ и серверов, входящих в состав ИС, а также ответственность за соблюдение требований к эксплуатации средств защиты информации и средств криптографической защиты информации в составе системы защиты информации, лежит на владельце подключаемой ИС.

ГКУ СО «ЦРЦТ» имеет право проводить проверки реализации схем подключения к защищаемой ГИС.

В случае выявления нарушений требований настоящих технических условий, ГКУ СО «ЦРЦТ» немедленно производит отключение соответствующей ИС сторонней организации от ГИС.

Начальник отдела информационной
безопасности



А.В. Виноградов

Приложение 1

**Форма акта настройки
средств защиты информации в составе ИС, подключаемой к государственной
информационной системе «Автоматизированная информационная система
«Предоставление государственных и муниципальных услуг в электронной форме»**

УТВЕРЖДАЮ

Руководитель подключаемого учреждения

ФИО

«_____» _____ 2021 г.

АКТ

настройки средств защиты в составе ИС «Наименование»

1. Наименование подключаемой ИС:
Информационная система «Наименование».

2. Состав основных технических средств и систем в составе ИС:

Наименование	Учетный (инвентарный) номер	ФИО ответственного работника	Должность работника
Сервер №1	4102501556512	Егоров Виталий Андреевич	Отдел технического обеспечения
АРМ №1	4102501445652	Сидоров Евгений Андреевич	Ведущий специалист отдела сопровождения

3. Состав средств защиты информации:

Тип СЗИ	Наименование	Версия	Дата настройки	Серийный номер (СЗЗ)	Сертификат соответствия ФСТЭК России (ФСБ России)
Сервер № 1					
Средство защиты информации от НСД	Dallas-Lock 8.0-K	8.0.565.2	20.02.2020	13306-2075-448 (3 989991)	Сертификат соответствия ФСТЭК России от 25.11.2016 № 2720

Средство антивирусной защиты	«Kaspersky Security для Windows Server»	10.1.2	20.02.2021	СМП8067- 23434 (Н 451194)	Сертификат соответствия ФСТЭК России от 25.12.2017 № 3840
АРМ № 1, 2					
Средство защиты информации от НСД	Dallas Lock 8.0-K	8.0.565.2	04.03.2021	13306-2075-448 (З 989991)	Сертификат соответствия ФСТЭК России от 25.11.2016 № 2720
Средство антивирусной защиты	Kaspersky Endpoint Security 11	11.3	05.03.2021	СМП8067- 29444 (Н 450182)	Сертификат соответствия ФСТЭК России от 22.01.2019 № 4068
Средство межсетевого экранирования	ViPNet Client 4	4.5	04.03.2021	КлКС2-4- 105558 (Н 022551)	Сертификат соответствия ФСТЭК России от 30.11.2016 № 3727
Отдельно установленные средства защиты информации					
Средство межсетевого экранирования	ViPNet Coordinator	HW1000 Q5	20.02.2021	030-35711 (Л 995878)	Сертификат соответствия ФСТЭК России от 26.01.2017 № 3692

Ответственный за обеспечение защиты подключаемой ИС _____ ФИО