

ДЕПАРТАМЕНТ ФИНАНСОВ ИВАНОВСКОЙ ОБЛАСТИ

УТВЕРЖДЕН
«16» января 2026 г.

**РЕГЛАМЕНТ ПОДКЛЮЧЕНИЯ ВНЕШНИХ
ПОЛЬЗОВАТЕЛЕЙ
К ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ
«СИСТЕМА УПРАВЛЕНИЯ РЕГИОНАЛЬНЫМИ
ФИНАНСАМИ ИВАНОВСКОЙ ОБЛАСТИ»
ДЕПАРТАМЕНТА ФИНАНСОВ ИВАНОВСКОЙ ОБЛАСТИ**

г. Иваново
2026

Оглавление

Сокращения и определения.....	3
1. Введение.....	4
2. Требования к организации подключения	5
3. Требования к реализации системы защиты информации и защищенного взаимодействия.....	8
4. Порядок подключения АРМ внешних пользователей ГИС для возможности включения их в защищенную ГИС СУРФ Ивановской области	10

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

АРМ	- автоматизированное рабочее место;
Внешние пользователи	- участники информационного взаимодействия, осуществляющие подключение к государственной информационной системе «Система управления региональными финансами Ивановской области» с использованием внешних информационно-телекоммуникационных сетей, не входящих в контролируемую зону, в которой функционируют программные и технические средства государственной информационной системы «Система управления региональными финансами Ивановской области»;
Оператор ГИС	- Департамент финансов Ивановской области; - государственная информационная система «Система управления региональными финансами Ивановской области» Департамента финансов Ивановской области;
Регламент	- регламент подключения внешних пользователей к государственной информационной системе «Система управления региональными финансами Ивановской области» Департамента финансов Ивановской области;
СЗИ	- средство защиты информации;
СКЗИ	- средство криптографической защиты информации;
СЗИ от НСД	- средства защиты информации от несанкционированного доступа.

1. ВВЕДЕНИЕ

Данный документ регламентирует процесс подключения внешних пользователей к государственной информационной системе «Система управления региональными финансами Ивановской области» (далее – ГИС СУРФ Ивановской области, ГИС) Департамента финансов Ивановской области (далее – Департамент, Оператор).

Внешними пользователями ГИС СУРФ Ивановской области Департамента являются субъекты (пользователи ГИС СУРФ Ивановской области), не являющиеся сотрудниками Департамента.

Основной целью Регламента является определение обязательного плана работ при подключении внешних пользователей ГИС СУРФ Ивановской области в защищенную сеть Департамента, необходимых для выполнения требований по обеспечению информационной безопасности в ГИС СУРФ Ивановской области.

Регламент разработан в соответствии с Приказом ФСТЭК России от 11.03.2013 № 17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и Приказом ФСТЭК России от 18.02.2013 № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ПОДКЛЮЧЕНИЯ

2.1. Организация и принятие мер по защите информации при подключении внешних пользователей к ГИС СУРФ Ивановской области осуществляются в соответствии со следующими требованиями:

- Федерального закона «Об информации, информационных технологиях и о защите информации», Федерального закона «О защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Федерального закона «О персональных данных»;

- нормативных правовых актов, методических и руководящих документов Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России) и Федеральной службы безопасности Российской Федерации (далее – ФСБ России) в области защиты информации;

- настоящего Регламента.

2.2. Требования к организации защищенного взаимодействия.

Для организации защищенного взаимодействия АРМ внешних пользователей с ГИС СУРФ Ивановской области должен использоваться АРМ, на котором установлены сертифицированные по требованиям безопасности информации средства криптографической, антивирусной защиты информации и средства защиты информации от несанкционированного доступа.

2.2.1. Для реализации комплекса организационных и технических мероприятий по защите информации, в соответствии с требованиями приказа ФСБ России № 378 от 10.07.2014, методическими рекомендациями ФСБ России № 149/7/2/6-432 от 31.03.2015, приказом ФСБ России № 117 от 18.03.2025, согласно масштабу ГИС СУРФ Ивановской области и уровню значимости обрабатываемой информации минимально допустимый класс СКЗИ, подлежащих использованию для защиты информации, обрабатываемой в ГИС СУРФ Ивановской области, определен как КС1.

2.2.2. Реализация антивирусной защиты должна предусматривать:

- применение средств антивирусной защиты на АРМ;
- установку, конфигурирование и управление средствами антивирусной защиты;

- проведение периодических проверок компонентов АРМ на наличие вредоносных компьютерных программ;

- проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей

информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов;

- оповещение об обнаружении вредоносных компьютерных программ;
- определение и выполнение действий по реагированию на обнаружение объектов, подвергшихся заражению вредоносными компьютерными программами;
- регулярное, не реже 1 раза в день, обновление антивирусных баз;
- обновление версий программного обеспечения средств антивирусной защиты по мере их выпуска производителем;
- периодическую проверку работоспособности средств антивирусной защиты.

2.2.3. Средство защиты информации от несанкционированного доступа должно реализовывать следующие функции:

- аутентификация пользователей с использованием паролей, электронных ключей, смарт-карт или других доверенных средств, включая двухфакторную аутентификацию;
- разграничение доступа на основе ролей или мандатных меток с контролем прав на файлы, папки, процессы и сетевые ресурсы;
- учет и аудит событий безопасности, регистрация входа/выхода пользователей, попыток несанкционированного доступа, изменений политик и критических операций;
- защита от запуска несанкционированных программ с помощью белых/чёрных списков исполняемых файлов;
- целостность программного обеспечения, защита системных файлов и компонентов средств защиты информации от модификации.

2.3. Обобщенная схема информационного взаимодействия ГИС СУРФ Ивановской области с АРМ внешних пользователей ГИС.

Обобщенная схема информационного взаимодействия ГИС СУРФ Ивановской области с АРМ внешних пользователей ГИС представлена на рисунке 1.

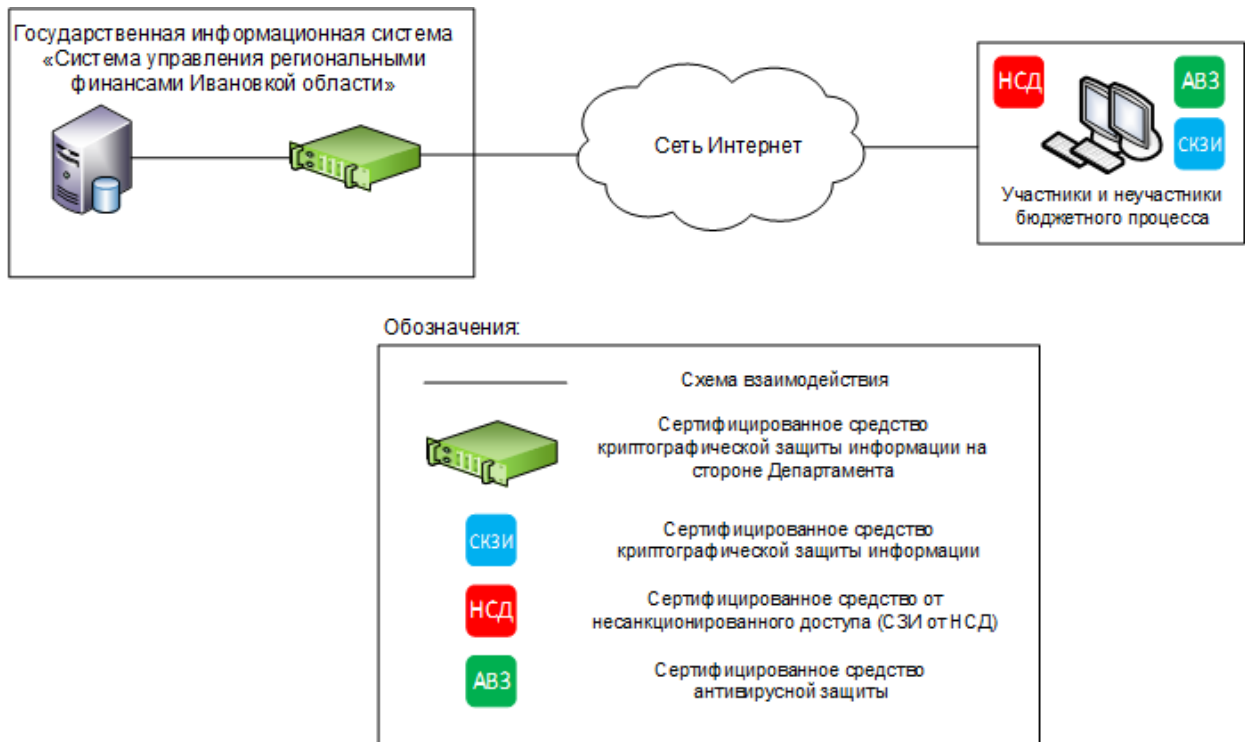


Рисунок 1. Обобщенная схема информационного взаимодействия ГИС СУРФ Ивановской области с АРМ внешних пользователей ГИС

3. ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ И ЗАЩИЩЕННОГО ВЗАИМОДЕЙСТВИЯ

Для возможности организации защищенного информационного взаимодействия АРМ внешних пользователей с ГИС СУРФ Ивановской области и обеспечения требований по защите информации участники информационного взаимодействия должны обеспечить реализацию следующих организационных и технических мероприятий.

3.1 Технические мероприятия, включают:

3.1.1. Приобретение, установку и настройку сертифицированных по требованиям безопасности информации:

- средства криптографической защиты информации;
- средства антивирусной защиты информации;
- средства защиты информации от несанкционированного доступа.

3.1.2. Получение сертификатов ключей электронной подписи;

3.1.3. Проверка связи с ГИС СУРФ Ивановской области.

Перечень рекомендуемых СЗИ и СКЗИ представлен в приложении 2.

3.2 Организационные мероприятия, включают:

– назначение ответственного за организацию обработки защищаемой информации, согласно соответствующему разработанному и утвержденному документу.

– назначение ответственного за обеспечение безопасности защищаемой информации, согласно соответствующему и утвержденному документу;

– определение перечней сотрудников, осуществляющих обработку защищаемой информации и имеющих доступ к обрабатываемой защищаемой информации, согласно соответствующему разработанному и утвержденному документу.

– определение перечня мер по обеспечению безопасности помещений, в которых размещены государственные информационные системы защищаемой информации и сохранности носителей защищаемой информации, согласно соответствующему разработанному и утвержденному документу.

– определение перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты, согласно соответствующему разработанному и утвержденному документу;

– определение политики в отношении обработки защищаемой информации, согласно соответствующему разработанному и утвержденному документу.

Все сетевые запросы к ресурсам ГИС Департамента должны проходить исключительно через установленное VPN-соединение. Прямой доступ в обход СКЗИ запрещен. Не допускается взаимодействие АРМ внешних пользователей при неполной или некорректной реализации защищенного подключения, невыполнении всех необходимых требований по обеспечению информационной безопасности, отсутствию или некорректной настройке технических средств защиты информации.

Необходимо использование сетей связи, расположенных на территории Российской Федерации.

4. ПОРЯДОК ПОДКЛЮЧЕНИЯ АРМ ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ ГИС ДЛЯ ВОЗМОЖНОСТИ ВКЛЮЧЕНИЯ ИХ В ЗАЩИЩЕННУЮ ГИС СУРФ ИВАНОВСКОЙ ОБЛАСТИ

Для АРМ внешних пользователей ГИС реализация обязательных требований достигается путем применения порядка следующих технических и организационных мер:

4.1 Получение средств криптографической защиты информации.

Для подключения к ГИС СУРФ Ивановской области необходимо отправить запрос Оператору ГИС на получение сертифицированного ФСБ России СКЗИ. Список, рекомендуемых для подключения, средств криптографической защиты информации предоставлен в приложении 2.

4.2 Приобретение средства антивирусной защиты информации и СЗИ от НСД.

Для выполнения требований по обеспечению информационной безопасности при подключении к ГИС СУРФ Ивановской области, необходимо приобрести средство антивирусной защиты информации, СЗИ от НСД и права на их использование. Список, рекомендуемых, средств антивирусной защиты информации и СЗИ от НСД предоставлен в приложении 2.

4.3 Установка и настройка средства криптографической защиты информации.

Произвести установку СКЗИ на АРМ, удовлетворяющее требованиям, предъявляемых средством к операционной системе и обновлениям к ней. По итогу установки составляется акт установки и ввода в эксплуатацию.

4.4 Получение сертификатов ключей электронной подписи.

Отправить запрос Оператору ГИС на получение сертификатов ключей электронной подписи, в соответствии с выбранным для подключения СКЗИ. После получения сертификатов ключей электронной подписи, произвести их установку.

4.5 Установка и настройка средства антивирусной защиты информации и СЗИ от НСД.

Произвести установку средства антивирусной защиты и СЗИ от НСД на АРМ, удовлетворяющее требованиям предъявляемых средством к операционной системе, программным и аппаратным компонентам. По итогу установки составляется акт установки и ввода в эксплуатацию.

4.6 Проверка связи с подключаемым узлом.

Произвести подключение к ГИС СУРФ Ивановской области. Результатом проверки должно служить установленное соединение.

4.7 Организационные мероприятия.

Выполнить организационные мероприятия, согласно п.3.2.

4.8 Оформление акта.

Заполнить акт, указанный в приложении 1, и отправить Оператору ГИС.

Приложение 1
к Регламенту подключения внешних
пользователей к государственной
информационной системе «Система
управления региональными финансами
Ивановской области» Департамента
финансов Ивановской области

Акт
о готовности к подключению к ГИС СУРФ Ивановской области

г. Иваново

«___» _____ 2025 г.

Основание:

Составлен комиссией:

председатель – _____

члены комиссии: _____

Комиссия провела проверку выполнения технических и организационных мер по созданию
защищенного _____ канала _____ связи

« _____
(наименование организации) _____ »

(далее – организация) с ГИС СУРФ Ивановской области.

Комиссия выявила в организации следующие средства защиты информации:

1. Средство криптографической защиты информации:

1.1. _____;*

2. Средство антивирусной защиты информации:

2.1. _____;*

3. Средство защиты информации от несанкционированного доступа:

3.1. _____;*

Акт установки и готовности к вводу в эксплуатацию средств защиты информации (в том
числе криптографических) № _____;

Комиссия сообщает:

о готовности « _____
(наименование организации) _____ »

к подключению к ГИС СУРФ Ивановской области.

Составлен в 2-х экземплярах.

Председатель комиссии: _____

Члены комиссии: _____

* Рекомендуемые средства защиты информации предоставлены в приложении 2

Приложение 2
к Регламенту подключения внешних
пользователей к государственной
информационной системе «Система
управления региональными финансами
Ивановской области» Департамента
финансов Ивановской области»

**Рекомендуемые средства защиты информации,
сертифицированных по требованиям безопасности информации, для
установки на АРМ для подключения к ГИС СУРФ Ивановской области**

1. Средства криптографической защиты информации:
 - 1.1. СКЗИ «Континент TLS – клиент» Версия 2.
 - 1.2. СКЗИ «Континент ZTN Клиент для Linux»¹.
 - 1.3. СКЗИ «КриптоПро CSP» версия 5.0.
2. Средства антивирусной защиты информации:
 - 2.1. Программное изделие Kaspersky Endpoint Security.
 - 2.2. Dr.Web Enterprise Security Suite.
3. Средства защиты информации от несанкционированного доступа:
 - 3.1. Система защиты информации от несанкционированного доступа Dallas Lock.
 - 3.2. Средство защиты информации Secret Net Studio.

¹ На данный момент отсутствует действующий сертификат ФСБ России, сертификация продукта ожидается во 2 квартале 2026 года.