УТВЕРЖДАЮ
Заместитель министра транспорта и связи
Свердловской области

_____С.Н. Фролов

«20» 06 2014 г.

Требования
по защите информации в
единой информационно-коммуникационной инфраструктуре Свердловской области
при подключении пользователей
к Государственным информационным системам Свердловской области и
Информационным системам персональных данных

1.Общие положения

Технические и организационные меры по защите информации в единой информационно-коммуникационной инфраструктуре Свердловской области (далее - ИК-инфраструктура) разработаны на основании следующих Руководящих документов:

Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федерального закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

приказов Федеральной службы по техническому и экспортному контролю Российской Федерации от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

постановления Правительства Свердловской области от 06.05.2013 № 578-ПП «Об утверждении Концепции развития единой информационно-коммуникационной инфраструктуры Свердловской области»;

Методического документа «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014 года;

«Методических рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденные руководством 8 центра ФСБ России 21.02.2008 № 149/5-144;

«Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные руководством 8 центра ФСБ России 21.02.2008 № 149/6/6-622.

2.Назначение и состав Единой информационно-коммуникационной структуры Свердловской области.

Единая информационно-коммуникационная инфраструктура Свердловской области представляет собой совокупность информационных и коммуникационных инфраструктур, в том числе единая сеть передачи данных Правительства Свердловской области (далее – ЕСПД) и центры обработки данных Правительства Свердловской области (основной и резервный) (далее – ЦОД), предназначенные для предоставления базовых инструментов информатизации и единых информационных сервисов всем пользователям ИК-инфраструктуры.

Под средством ИК-инфраструктуры предоставляется (может - предоставляться) доступ к Государственным информационным системам Свердловской области.

Элементы единой информационно-коммуникационной инфраструктуры Свердловской области (ЦОД ГБУ Свердловской области «Оператор электронного правительства, коммутационные узлы для подключения исполнительных органов государственной власти Свердловской области к ЦОДу) аттестованы по 2 классу защищенности информационных систем и 2 уровню защищенности персональных данных.

Для информационных систем 2 класса защищённости меры защиты информации обеспечивают 2, 3 и 4 уровни защищённости персональных данных.

Класс защищенности Государственных информационных систем Свердловской области, оператором которых является Министерство транспорта и связи Свердловской области, представлен в таблице № 1.

Таблица № 1

№ п/п	Наименование государственной информационной системы	Номер ГИС в реестре государственных систем Свердловской области	Требования по защите информации в ГИС	
			Класс защищенности ГИС	Уровень защищенности персональных данных
1	Государственная автоматизированная информационная система "Автоматизированная система управления деятельностью исполнительных органов государственной власти Свердловской области"	ИС-13/0003 от 5.07.2013	2	2
2	Государственная информационная система "Автоматизированная информационная система "Е-услуги. Образование"	ИС-13/0004 от 5.07.2013	2	2
3	Региональная государственная информационная система «Реестр государственных и муниципальных услуг (функций) Свердловской области»	ИС-14/0010 от 04.02.2014	3	3
4	Государственная информационная система Свердловской области "Региональная навигационно-информационная система транспортного комплекса Свердловской области на базе технологий ГЛОНАСС и ГЛОНАСС/GPS"	ИС-13/0002 от 5.07.2013	3	3

3. Мероприятия по защите информации в ИК-инфраструктуре при подключении к Государственным информационным системам и системам персональных данных.

3.1 Общие требования.

При подключении к Государственным информационным системам и Информационным системам персональных данных участниками ИК-инфраструктуры должны быть реализованы следующие меры защиты информации:

идентификация и аутентификация субъектов доступа и объектов доступа;
управление доступом субъектов доступа к объектам доступа;
ограничение программной среды;
защита машинных носителей информации;
регистрация событий безопасности;
антивирусная защита;
обнаружение (предотвращение) вторжений;
контроль (анализ) защищенности информации;
обеспечение целостности информационной системы и информации;
обеспечение доступности информации;
защита среды виртуализации;
защита технических средств;
защита информационной системы, ее средств и систем связи и передачи данных.

Применение беспроводных технологий связи для доступа к Государственным информационным системам и Информационным системам персональных данных возможно только при использовании средств криптографической защиты информации совместимых со средствами, использующимися в центральном сегменте ИК-инфраструктуры.

3.2 Организационные мероприятия по обеспечению безопасности информации.

Комплекс организационных мероприятий по защите информации, при подключении к Государственным информационным системам и информационным системам персональных данных в ИК-инфраструктуре Свердловской области, должен включать в себя следующие меры:

все технические средства обработки информации и носители информации должны быть размещены в пределах контролируемой зоны;

все помещения, в которых происходит обработка и хранение защищаемой информации, а так же помещение с оборудованием, обеспечивающим технологический процесс обработки информации, должны быть оснащены средствами охранно-пожарной сигнализации;

входные двери в помещения должны быть оснащены надежными замками;

допуск в помещения вспомогательного и обслуживающего персонала (уборщиц, электромонтеров, сантехников и т.д.) должен производиться только в случае служебной необходимости в присутствии лиц, ответственных за эксплуатацию помещений;

физическая охрана технических средств информационной системы должна предусматривать контроль доступа в помещения;

должно проводиться резервирование технических средств, дублирование массивов и носителей информации;

должен быть определен перечень лиц допущенных к обработке информации в ИС;

должен быть назначен ответственный за обеспечение безопасности информации;

все машинные носители информации, средства защиты информации должны быть учтены в специальных журналах.

3.3 Технические мероприятия

3.3.1 Общие требования к реализации технических мероприятий по обеспечению безопасности информации.

Применяемые технические средства защиты информации должны соответствовать требованиям к средствам защиты информации определенным в п.26 Приказа ФСТЭК России от 11 февраля 2013 г. № 17 для информационных систем 2 класса защищенности.

Выбранные для использования сертифицированные по требованиям безопасности информации средства защиты должны соответствовать:

средства вычислительной техники - не ниже 5 класса в соответствии с РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;

системы обнаружения вторжений и средства антивирусной защиты - не ниже 4 класса защиты;

межсетевые экраны - не ниже 3 класса в соответствии с РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации»;

программное обеспечение СЗИ не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей в соответствии с РД «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей».

3.3.2 Обеспечение безопасности информации при передаче по телекоммуникационным каналам связи.

При передаче информации по телекоммуникационным каналам связи необходимо обеспечить защиту передаваемой информации от несанкционированного доступа к ней криптографическими средствами защиты информации.

Применяемые криптографические средства защиты информации должны быть полностью совместимы с уже существующими средствами защиты каналов связи Правительства Свердловской области (ViPNet сеть № 2057, в составе: ПО ViPNet Administrator, ПАК ViPNet Coordinator HW1000, ПАК ViPNet Coordinator HW100C).

Класс применяемых криптографических средств зависит от мер, реализованных в учреждении по обеспечению безопасности информации и определяется в соответствии со следующими рекомендациями:

в случае реализации комплекса мероприятий организационного и технического характера обеспечивающего отсутствие несанкционированного доступа к автоматизированным рабочим местам (далее – АРМ) пользователей ИК-Инфраструктуры со стороны потенциально возможных внутренних нарушителей безопасности информации (сотрудников и внешних посетителей, не являющихся зарегистрированными пользователями, имеющими право постоянного или разового доступа в контролируемую зону в которой расположен АРМ Пользователя) достаточными средствами криптографической защиты информации являются средства класса КС1;

в случае отсутствия комплекса мероприятий организационного и технического характера обеспечивающего отсутствие несанкционированного доступа к АРМ Пользователей ИК-Инфраструктуры со стороны потенциально возможных внутренних нарушителей безопасности информации необходимо применять средства криптографической защиты информации класса не ниже КС2.

4. Порядок проведения мероприятий по защите информации в информационных системах при подключении к Государственным информационным системам и информационным системам персональных данных в ИК –инфраструктуре Свердловской области.

Для проведения работ по защите информации при подключении к Государственным информационным системам и Информационным системам персональных данных в ИК-инфраструктуре Свердловской области необходимо руководствоваться нормативными документами перечисленными в разделе № 1 текущего документа, для проведения указанных мероприятий допускается привлечение организаций, имеющих лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 04 мая 2011 года № 99-ФЗ «О лицензировании отдельных видов деятельности».

5. Рекомендации к средствам защиты информации.

Применяемые технические средства защиты информации должны быть сертифицированы ФСТЭК России (ФСБ России в части средств криптографической защиты информации) и соответствовать требованиям к средствам защиты информации определенным:

-Приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» для информационных систем 2 класса защищенности;

-Приказом ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений»;

-Приказом ФСТЭК России от 20 марта 2012 г. № 28 «Требования к средствам антивирусной защиты».

Меры по защите АРМ пользователей ИК-инфраструктуры определяются пользователями ИК – инфраструктуры самостоятельно (или с привлечением организаций – лицензиатов ФСТЭК России и ФСБ России по направлениям технической и криптографической защиты информации) в зависимости от уже реализованных в учреждении мер организационного и технического характера по обеспечению безопасности информации в соответствии с требованиями Федеральных законов и нормативных документов ФСТЭК России и ФСБ России, а также в соответствии с требованиями настоящего документа.

При выборе средств защиты необходимо руководствоваться следующими рекомендациями:

№ п/п	Средства защиты информации	
1	Средства антивирусной защиты	Средства антивирусной защиты должны быть лицензионными и сертифицированными ФСТЭК России с ежедневно обновляемыми базами сигнатур. (Kaspersky Endpoint Security - медиапак)
2	Средства защиты информации при передаче по каналам связи	Применяемые средства должны быть полностью совместимы с уже существующими средствами защиты каналов связи Правительства Свердловской области (ViPNet сеть № 2057) (ViPNet Coordinator HW, ViPNet Client, или аналоги)
3	Средства межсетевого экранирования	Средства межсетевого экранирования должны корректно функционировать в рамках существующей ИК-Инфраструктуры Правительства Свердловской области (ViPNet Coordinator HW, ViPNet Client, или аналоги)

4	Системы обнаружения вторжений	Системы обнаружения вторжений должны корректно функционировать в рамках существующей ИК-Инфраструктуры Правительства Свердловской области В качестве средства обнаружения вторжений допустимо использование программно – аппаратного комплекса ViPNet IDS 1000, который корректно функционирует в действующей развернутой сети ViPNet Правительства СО
5	Средства защиты от несанкционированного доступа с программным модулем доверенной загрузки	Средства защиты должны быть способны корректно функционировать на рабочих стациях входящих в домен Правительства Свердловской области. **Вариант № 1** Dallas Lock 8.0-С или аналоги с программным модулем доверенной загрузки **Вариант № 2** Средство от НСД SecretNet или аналоги Средства ДЗ ПАК Соболь или аналоги
6	Средства доверенной загрузки	

Примечание:

1. На сегодняшний день всем требованиям Приказа ФСТЭК России № 28 «Требования к средствам антивирусной защиты» соответствует только сертифицированный продукт Kaspersky Endpoint Security 10. Остальные (Dr.Web, NOD32 и т.д) такой сертификат не получили. Закупленные ранее антивирусы годятся, но только до конца действия сертификатов соответствия ФСТЭК России.

2. Для ГИС класса К2 обязательно наличие средств обнаружения вторжений, таких как ViPNet IDS 1000 или 2000.

6. Подключение к Государственным информационным системам и Информационным системам персональных данных.

Подключение к Государственным информационным системам и Информационным системам персональных данных производится по соглашению между оператором Государственной информационной системы и руководителями учреждений и организаций, планирующих осуществить подключение к информационной системе.

Подключение АРМ пользователей к Государственным информационным системам в ИК-инфраструктуре производиться только после выполнения учреждением всех требований по обеспечению безопасности информации (в том числе и персональных данных) предусмотренных федеральными законами, нормативными документами и определенными настоящим документом.

Предоставление доступа пользователей к Государственным информационным системам должно осуществляется на основании заявок, оформленных установленным порядком, проект заявки прилагается (Приложение № 1).

Ответственными за допуск учреждений и организаций к Государственным информационным системам являются операторы данных систем.

Ответственными за допуск сотрудников к Государственным информационным системам являются руководители учреждений и организаций, подключенных к ИК-инфраструктуре.

Начальник отдела О. Цегельный

Приложение № 1

Заявка на подключение к
Государственной информационной системе Свердловской области

Прошу предоставить доступ к Государственной информационной системе Свердловской области

_____

Данные об органе/организации			
Полное наименование органа/организации			
Краткое наименование органа/организации			
Данные об уполномоченном должностном лице органа/организации			
№ п/п	Фамилия, Имя отчество	должность	Рабочий телефон Адрес электронной почты
1			
2			
3			
4			
5			
6			
Данные о проведении мероприятий по защите информации			
Дата и номер аттестата соответствия	Если имеется		
Используемые средства защиты информации			
ФИО, контактная информация администратора безопасности			
Данные о согласовании доступа с оператором Государственной информационной системы			
Номер и дата письма о согласовании доступа			
Кем согласовано (Должность, ФИО)			

Руководитель _____ Фамилия, Инициалы

(дата)