

Министерство образования Нижегородской области
Государственное бюджетное образовательное учреждение дополнительного
профессионального образования
«Нижегородский институт развития образования»
(ГБОУ ДПО НИРО)

УТВЕРЖДАЮ

Ректор ГБОУ ДПО НИРО



Н.Ю. Бармин

2017 г.

**Подключение систем персональных данных образовательных
организаций и учреждений органов исполнительной власти к
информационной системе персональных данных
«Региональный сегмент Нижегородской области»**

Инд. № подл.	Подп. и дата	Взам. инв. №	Инд. № дубл.	Подп. и дата

Нижний Новгород

2017 год

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ.....	3
ВВЕДЕНИЕ.....	5
1. ОСНОВНЫЕ ПОЛОЖЕНИЯ.....	7
1.1.ОБЩЕЕ ОПИСАНИЕ ИНФОРМАЦИОННОГО ОБМЕНА.....	7
1.2.ОБЩИЕ ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ.....	7
2. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ.....	9
2.1.ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ПОДКЛЮЧЕНИЯ.....	9
2.2.ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ ЗАЩИЩЕННОГО ВЗАИМОДЕЙСТВИЯ.....	9
2.2.1. ОБЩИЕ ТРЕБОВАНИЯ.....	9
2.2.2. ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ СХЕМЫ ЗАЩИЩЕННОГО ВЗАИМОДЕЙСТВИЯ №1.....	10
2.2.3. ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ СХЕМЫ ЗАЩИЩЕННОГО ВЗАИМОДЕЙСТВИЯ №2.....	11
2.2.4. СПЕЦИАЛЬНЫЕ ТРЕБОВАНИЯ.....	12
3. КОНТРОЛЬ РЕАЛИЗАЦИИ ПОДКЛЮЧЕНИЯ К ИСПДн.....	13
4. ПЕРЕЧЕНЬ НОРМАТИВНО-ПРАВОВЫХ АКТОВ.....	13
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ.....	16

Инд. № подл.	Подп. и дата
Взам. инв. №	Инд. № дубл.
Подп. и дата	Подп. и дата
Инд. № подл.	Инд. № дубл.

4	Все				
Изм.	Лист	№ докум.	Подп.	Дата	

Технические условия

Лист

2

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

АРМ	-	Автоматизированное рабочее место
ИСПДн	-	Информационная система персональных данных
ИС	-	Информационная система
МЭ	-	Межсетевой экран
РД	-	Руководящий документ
АИС	-	Автоматизированная информационная система
СЗИ	-	Средства защиты информации
СКЗИ	-	Средства криптографической защиты информации
СЭП	-	Средство электронной подписи
ТУ	-	Технические условия
ОО	-	Образовательная организация
ОИВ	-	Орган исполнительной власти
ФСБ России	-	Федеральная служба безопасности России
ФСТЭК России	-	Федеральная служба по техническому и экспортному контролю России
ЭД	-	Эксплуатационная документация
ЭП	-	Электронная подпись
АИС Контингент	-	Региональный сегмент единой федеральной межведомственной системы учета контингента
ЦОД		Центр обработки данных

Инов. № подл.	Подп. и дата	Взам. инв. №	Инов. № дубл.	Подп. и дата

Изм.	Лист	№ докум.	Подп.	Дата

Технические условия

АННОТАЦИЯ

Настоящие технические условия определяют требования и условия, а также устанавливают порядок подключения образовательных организаций и учреждений ОИВ к региональному сегменту единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам Нижегородской области (далее – Региональный сегмент Нижегородской области).

Требования настоящих технических условий распространяются на информационные системы персональных данных ОО и учреждений ОИВ, имеющие подключение к Региональному сегменту Нижегородской области.

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата	Технические условия	Лист
						4
Изм.	Лист	№ докум.	Подп.	Дата		

ВВЕДЕНИЕ

АИС «Контингент» - региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам.

Основопологающим документом для внедрения системы в регионах Российской Федерации является Распоряжение Правительства Российской Федерации от 25 октября 2014 г. № 2125-р.

Обязательные данные, которые должен содержать региональный сегмент единой федеральной межведомственной системы «Контингент», приводятся в документе Министерства информационных технологий и связи «Унифицированные функционально-технические требования к региональному сегменту единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам».

Назначение системы:

- получение информации о количестве обучающихся, проживающих на территории субъекта РФ;
- получение оперативной информации об очередях на зачисление в организации дошкольного, начального общего, среднего общего, основного общего, профессионального и дополнительного образования субъекта РФ и о степени их наполнения;
- прогнозирование необходимого количества мест в организациях субъекта РФ, осуществляющих образовательную деятельность;
- формирование полного набора данных об этапах обучения и достижениях, обучающихся субъекта РФ при их обучении в организациях, осуществляющих образовательную деятельность, включая результаты дополнительного образования;
- получение информации о влиянии образовательного процесса на состояние здоровья обучающихся субъекта РФ;
- ведение статистической отчетности, формирование и предоставление сводной аналитической информации об образовательных организациях и контингенте обучающихся субъекта РФ.

В соответствии с Распоряжением Правительства Нижегородской области №534-р от 25.04.2016 ГБОУ ДПО НИРО является уполномоченным администратором АИС «Контингент» в регионе.

ЦОД ГБОУ ДПО НИРО аттестован на соответствие требованиям по безопасности информации и является информационной системой персональных данных «Региональный сегмент Нижегородской области» Государственного бюджетного образовательного учреждения дополнительного профессионального образования «Нижегородский институт развития образования».

Изм.	Лист	№ докум.	Подп.	Дата
Изн. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Технические условия

Лист

5

Требования настоящих технических условий устанавливают состав, содержание, а также порядок выполнения работ по подключению ИСПДн образовательных организаций, учреждений ОИВ (АРМ поставщиков данных), а также состав программно-технических средств, в том числе средств защиты информации, необходимых для организации защищенного взаимодействия ИСПДн ОО и ОИВ с ИСПДн «Региональный сегмент Нижегородской области».

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата	
Изм.	Лист	№ докум.	Подп.	Дата	<p style="text-align: center;"><i>Технические условия</i></p>

1. ОСНОВНЫЕ ПОЛОЖЕНИЯ

1.1 Общее описание информационного обмена

Обмен информацией между ИСПДн «Региональный сегмент Нижегородской области» и ИСПДн ОО и ОИВ осуществляется в электронном виде с использованием сетей связи общего пользования (сети Интернет).

В ИСПДн «Региональный сегмент Нижегородской области» для защиты информации конфиденциального характера используются сертифицированные шифровальные (криптографические) средства на базе продуктов семейства ViPNet. Для организации защищенного взаимодействия между ИСПДн «Региональный сегмент Нижегородской области» (сетью № 6526) и ИСПДн ОО и ОИВ по сети Интернет должна применяться технология виртуальных частных сетей - VPN, реализованная с использованием сертифицированных шифровальных (криптографических) средств, совместимых с решениями семейства ViPNet.

При осуществлении информационного обмена основными сетевыми телекоммуникационными протоколами являются протоколы семейства TCP/IP.

1.2 Общие требования по защите информации.

В соответствии с нормативно-правовыми актами в сфере защиты информации в ИСПДн «Региональный сегмент Нижегородской области» и ИСПДн ОО и ОИВ, должны быть приняты меры по защите содержащейся в них информации.

Доступ уполномоченным должностным лицам внешних поставщиков данных (ОО и ОИВ) к информации, содержащейся в ИСПДн «Региональный сегмент Нижегородской области», предоставляется администратором АИС - ГБОУ ДПО НИРО с учетом установленных законодательством Российской Федерации требований к обеспечению безопасности персональных данных при их обработке в информационных системах, ограничений по использованию информации и при условии применения программно-технических средств, позволяющих идентифицировать лицо, получающее доступ к информации.

Для обеспечения выполнения функций хранения и обработки данных рекомендуется использовать программное обеспечение, удовлетворяющее следующим требованиям: СУБД должна поддерживать дискреционные и мандатный механизмы контроля доступа к данным. Программное обеспечение должно иметь действующий сертификат соответствия требованиям информационной безопасности.

Хранение и обработка информации, содержащейся в региональной информационной системе и ИСПДн ОО и ОИВ, а также обмен информацией осуществляются после принятия необходимых мер по защите указанной информации от повреждения или утраты, предусмотренных нормативными правовыми актами Российской Федерации в области защиты информации.

Руководители организаций поставщиков данных назначают лиц, ответственных

Изм.	Лист	№ докум.	Подп.	Дата

Технические условия

Лист

7

за внесение сведений в региональную информационную систему, а также лиц, ответственных за обеспечение мер по защите информации, содержащейся в ИСПДн ОО и ОИВ.

Поставщики данных ОО и ОИВ несут предусмотренную законодательством Российской Федерации ответственность за полноту, достоверность и актуальность сведений, внесенных ими в Региональную информационную систему.

Инов. № подл.	Подп. и дата	Взам. инв. №	Инов. № дубл.	Подп. и дата
Изм.	Лист	№ докум.	Подп.	Дата
<i>Технические условия</i>				Лист
				8

2. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

2.1. Требования к организации подключения

Организация подключения ИСПДн образовательной организации к ИСПДн «Региональный сегмент Нижегородской области» 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 (ФСТЭК России, ФСБ России);
- требованиями настоящих Технических условий.

До начала выполнения работ по подключению ИСПДн ОО и ОИВ к ИСПДн «Региональный сегмент Нижегородской области» схема защищенного взаимодействия должна быть согласована с региональным администратором ГБОУ ДПО НИРО путем заключения Соглашения.

2.2. Требования к реализации защищенного взаимодействия

2.2.1. Общие требования

Для организации защищенного взаимодействия ИСПДн ОО и ОИВ с ИСПДн «Региональный сегмент Нижегородской области», в ИСПДн ОО и ОИВ должны быть выполнены организационные и технические мероприятия, подтверждающие соответствие системы защиты информации ИСПДн ОО и ОИВ.

Для обеспечения защиты информации, содержащейся в ИСПДн образовательной организации, должны применяться средства защиты информации, прошедшие процедуру оценки соответствия в форме сертификации на соответствие требованиям по безопасности информации.

Для организации защищенного электронного взаимодействия и информационного обмена между ИСПДн «Региональный сегмент Нижегородской области» и ИСПДн ОО и ОИВ по сети Интернет в состав системы защиты информации ИСПДн ОО и ОИВ должны входить шифровальные (криптографические) средства, совместимые с решениями семейства ViPNet.

Для проведения работ по защите информации в ходе создания и эксплуатации ИСПДн ОО и ОИВ (оператором) в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие:

- лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации, позволяющую выполнять работы по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах

Исп. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата
--------------	--------------	--------------	--------------	--------------

Изм.	Лист	№ докум.	Подп.	Дата
------	------	----------	-------	------

Технические условия

Лист

9

- информатизации, проведения аттестационных испытаний и аттестации на соответствие требованиям по защите информации;
- проектирования в защищенном исполнении средств и систем информатизации, установки, монтажа, средств защиты информации;
- лицензию ФСБ России на деятельность по распространению шифровальных/криптографических средств, техническому обслуживанию шифровальных/криптографических средств, а также оказанию услуг в области шифрования информации.

2.2.2. Требования к реализации схемы защищенного взаимодействия № 1

Взаимодействие ИСПДн ОО и ОИВ с ИСПДн «Региональный сегмент Нижегородской области» должно осуществляться с использованием средства криптографической защиты информации семейства ViPNet входящего в состав ViPNet сети № 6526, владельцем которой является ГБОУ ДПО НИРО.

Возможны два варианта реализации схемы защищенного взаимодействия №1.

Схема защищенного взаимодействия № 1 (Вариант 1).

Для организации взаимодействия ИСПДн ОО и ОИВ с ИСПДн «Региональный сегмент Нижегородской области» по схеме № 1 (вариант 1), подключаемая ИСПДн ОО или ОИВ должна иметь комплект документов, подтверждающих соответствие системы защиты информации ИСПДн организации требованиям безопасности информации.

Для обработки персональных данных в ИСПДн организации должен использоваться сертифицированный программно-аппаратный комплекс (далее - ПАК) с предустановленной специализированной операционной системой, программным межсетевым экраном (сертифицированным ФСТЭК России) и ViPNet совместимым средством криптографической защиты (сертифицированным ФСБ России).

Схема защищенного взаимодействия № 1 (Вариант 2).

Для организации взаимодействия ИСПДн ОО или ОИВ с ИСПДн «Региональный сегмент Нижегородской области» по схеме № 1 (вариант 2), подключаемая ИСПДн образовательной организации должна иметь действующий аттестат, подтверждающий её соответствие требованиям безопасности информации, предъявляемым к информационным системам персональных данных.

Для обработки персональных данных в ИСПДн организации должен использоваться АРМ, оснащенный сертифицированным ФСТЭК России по требованиям безопасности информации средством защиты от несанкционированного доступа, сертифицированным ФСТЭК/ФСБ России межсетевым экраном, сертифицированным средством антивирусной защиты, клиентской частью ViPNet - совместимого решения, выполняющего функции средства криптографической защиты информации (сертифицированного ФСБ России) и(или) другие сертифицированные средства защиты информации, необходимые для нейтрализации актуальных угроз безопасности персональных данных при их обработке в ИСПДн организации.

Исп.	Лист	№ докум.	Подп.	Дата
Изм.	Лист	№ докум.	Подп.	Дата

Изм.	Лист	№ докум.	Подп.	Дата
------	------	----------	-------	------

2.2.3. Требования к реализации схемы защищенного взаимодействия №2

Для организации взаимодействия ИСПДн организации (ОО или ОИВ) с ИСПДн «Региональный сегмент Нижегородской области» по схеме № 2, подключаемая ИСПДн организации должна иметь действующий аттестат, подтверждающий её соответствие требованиям безопасности информации, предъявляемым к информационным системам персональных данных.

Схема защищенного взаимодействия № 2

Защищенное взаимодействие осуществляется между ViPNet-сетью организации и ViPNet-сетью ИСПДн «Региональный сегмент Нижегородской области» (сеть № 6526).

Для защиты персональных данных в ИСПДн образовательной организации должны использоваться: сертифицированное ФСТЭК России по требованиям безопасности информации средство защиты от несанкционированного доступа, сертифицированное ФСТЭК/ФСБ России средство межсетевое экранирование, сертифицированное средство антивирусной защиты, ViPNet-совместимое решение, выполняющие функции средства криптографической защиты информации (сертифицированного ФСБ России) и(или) другие сертифицированные средства защиты информации, необходимые для нейтрализации актуальных угроз безопасности персональных данных при их обработке в ИСПДн организации.

Данные для передачи в ИСПДн «Региональный сегмент Нижегородской области» формируются в аттестованной ИСПДн организации и передаются в ИСПДн «Региональный сегмент Нижегородской области» через защищенный сертифицированным средством криптографической защиты канал, образуемый между ViPNet-совместимым решением организации и ViPNet-совместимым решением ИСПДн «Региональный сегмент Нижегородской области».

Требования к реализации схемы защищенного взаимодействия № 3.

Для организации взаимодействия ИСПДн организации с ИСПДн «Региональный сегмент Нижегородской области» по схеме № 3, подключаемая ИСПДн должна иметь действующий аттестат, подтверждающий её соответствие требованиям безопасности информации, предъявляемым к информационным системам персональных данных.

Схема защищенного взаимодействия № 3

Для организации взаимодействия ИСПДн организации с ИСПДн «Региональный сегмент Нижегородской области» по схеме № 3 должны использоваться каналы связи, защищенные с использованием средства криптографической защиты информации семейства ViPNet сертифицированного ФСБ России), обеспечивающего туннелирование трафика по технологии ViPNet между сегментами локальной вычислительной сети ИСПДн организации, а также туннелирование трафика по технологии ViPNet между сегментом локальной вычислительной сети ИСПДн организации и сегментом локальной вычислительной

Изм.	Лист	№ докум.	Подп.	Дата
Изм.	Лист	№ докум.	Подп.	Дата

сети ИСПДн «Региональный сегмент Нижегородской области». Для защиты персональных данных в ИСПДн организации должны использоваться: сертифицированное ФСТЭК России по требованиям безопасности информации средство защиты от несанкционированного доступа, сертифицированное ФСТЭК/ФСБ России средство межсетевое экранирования, сертифицированное средство антивирусной защиты, ViPNet-совместимое решение, выполняющие функции средства криптографической защиты информации (сертифицированного ФСБ России) и(или) другие сертифицированные средства защиты информации, необходимые для нейтрализации актуальных угроз безопасности персональных данных при их обработке в ИСПДн образовательной организации.

2.2.4. Специальные требования

Помещения для размещения технических средств ИСПДн организации должны удовлетворять требованиям ТУ и ЭД на данные средства.

Схема подключения ИСПДн организации (ОО или ОИВ) к ИСПДн «Региональный сегмент Нижегородской области», а также необходимые для их корректного функционирования настройки должны быть предварительно согласованы с ГБОУ ДПО НИРО.

Работы по установке, монтажу, запуску и первоначальной настройке средств защиты информации и СКЗИ должны выполняться в соответствии с требованиями настоящих ТУ и ЭД на данные средства.

Эксплуатация средств защиты информации и СКЗИ должна осуществляться в соответствии с организационно-технической, организационно-распорядительной и ЭД на систему защиты информации ИСПДн организации.

Обеспечение защиты информации в ходе эксплуатации ИСПДн организации (ОО или ОИВ) осуществляется её владельцем в соответствии с организационно-технической, организационно-распорядительной, ЭД на систему защиты информации ИСПДн организации и нормативно-техническими документами РФ в сфере защиты информации.

В ГБОУ ДПО НИРО предоставляется скан-копия приказа о вводе ИСПДн организации в действие, а также скан-копия действующего аттестата соответствия ИСПДн организации требованиям по безопасности информации, осуществляющей взаимодействие с ИСПДн «Региональный сегмент Нижегородской области» (сетью № 6526).

В случае проведения повторной аттестации ИСПДн организации, подключенной к ИСПДн «Региональный сегмент Нижегородской области» (после окончания срока действия аттестата соответствия), владелец ИСПДн организации обязан предоставить в ГБОУ ДПО НИРО скан-копию действующего аттестата соответствия.

Исп. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Изм.	Лист	№ докум.	Подп.	Дата	<i>Технические условия</i>	Лист 12

3. КОНТРОЛЬ РЕАЛИЗАЦИИ ПОДКЛЮЧЕНИЯ К ИСПДн

Ответственность за соблюдение требований настоящих ТУ, обеспечение защиты информации в ходе эксплуатации ИСПДн организации, а также ответственность за соблюдение требований к эксплуатации средств защиты информации и СКЗИ в составе системы защиты информации ИСПДн организации, используемых в выбранной схеме подключения, лежит на владельцах, подключаемых ИСПДн.

Уполномоченный администратор АИС «Контингент» ГБОУ ДПО НИРО имеет право проводить проверки реализации схем подключения.

В случае выявления нарушений требований настоящих ТУ, ГБОУ ДПО НИРО немедленно производит отключение соответствующей ИСПДн организации от ИСПДн «Региональный сегмент Нижегородской области» (сети № 6526).

4. ПЕРЕЧЕНЬ НОРМАТИВНО-ПРАВОВЫХ АКТОВ

Настоящие технические условия разработаны на основании требований следующих законодательных, нормативно-правовых и нормативных документов:

- Федеральный закон Российской Федерации «Об образовании в Российской Федерации» (от 29.12.2012 г. № 273-ФЗ);
- Федеральный закон Российской Федерации «О персональных данных» (от 27.07.2006 № 152-ФЗ);
- Постановление Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (от 01.11.2012г. №1119);
- Распоряжение Правительства Российской Федерации от 25 октября 2014 г. № 2125-р «Об утверждении Концепции создания единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам»;
- Распоряжение Правительства Российской Федерации от 14 февраля 2015 г. № 236-р «Об утверждении плана мероприятий ("дорожной карты") по созданию единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам»;
- Унифицированные функционально-технические требования к региональному сегменту единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам;
- Распоряжение Правительства Нижегородской области от 25 апреля 2016 года №534-р «О создании регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным

Ив. № подл.	Подп. и дата	Взам. инв. №	Ив. № дубл.	Подп. и дата

Изм.	Лист	№ докум.	Подп.	Дата

Технические условия

Лист

13

образовательным программам и дополнительным общеобразовательным программам» (в ред.23.12.2016);

- Приказ министерства информационных технологий, связи и средств массовой информации Нижегородской области и министерства образования Нижегородской области «Об утверждении регламента технического взаимодействия регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам с внешними информационными системам (за исключением федерального сегмента)» от 03.10.2016 № 113-од/3473;
- Постановление Правительства Российской Федерации «Об утверждении Положения 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)» (от 16 апреля 2012 г. №313);
- Постановление Правительства Российской Федерации «О лицензировании деятельности по технической защите конфиденциальной информации» (от 3 февраля 2012 г. №79);
- Приказ Федеральной службы по техническому и экспортному контролю «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (от 18.02.2013г. № 21);
- Приказ Федеральной службы по техническому и экспортному контролю (далее - ФСТЭК России) «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (от 11.02.2013 г. № 17);
- «Типовые требования 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»,

Изн. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата
Изм.	Лист	№ докум.	Подп.	Дата

Технические условия

Лист

14

утвержденные руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/6/6-622;

- Других технических и методических документов ФСТЭК России и ФСБ России в области обеспечения информационной безопасности и защиты персональных данных.

Инов. № подл.	Подп. и дата	Взам. инв. №	Инов. № дубл.	Подп. и дата
Изм.	Лист	№ докум.	Подп.	Дата

Технические условия

Лист

15

Лист регистрации изменений

Изм.	Номера листов				Всего листов (страниц) в докум.	№ докум.	Входящий № сопроводительного докум. и дата	Подп.	Дата
	изменённых	заменённых	новых	аннулированных					

	Инд. № подл.	Подп. и дата	Взам. инв. №	Инд. № дубл.	Подп. и дата

Изм.	Лист	№ докум.	Подп.	Дата