

## Договор поручения № 110105

защиты информации государственной информационной системы персональных данных  
Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО»  
в соответствии с предъявляемыми требованиями

г. Екатеринбург

«01» октября 2018 г.

Государственное автономное образовательное учреждение дополнительного профессионального образования Свердловской области «Институт развития образования», именуемое в дальнейшем «Доверитель», в лице ректора Грединой Оксаны Владимировны, действующего на основании Устава, с одной стороны, и Муниципальное казенное общеобразовательное учреждение Харловская средняя общеобразовательная школа, именуемое в дальнейшем «Поверенный», в лице директора Галишевой Татьяны Александровны, действующего на основании Устава, с другой стороны, заключили настоящий Договор о нижеследующем:

### 1. ПРЕДМЕТ ДОГОВОРА

1.1. Доверитель поручает, а Поверенный принимает на себя обязательство обеспечивать защиту информации государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО» в соответствии с установленными требованиями по информационной безопасности. Целью передачи средств защиты информации в эксплуатацию Поверенному является исполнение обязательств по выполнению Приказа Министерства общего и профессионального образования Свердловской области от 02.10.2013 №627-и «О формировании и ведении региональной информационной системы обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования на территории Свердловской области» в действующей редакции.

1.2. Состав средств защиты вычислительной техники государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО», переданных Поверенному в эксплуатацию Доверителем, приведены в Приложении №1 к настоящему Договору.

1.3. Доверитель гарантирует:

1.3.1. Информация и средства вычислительной техники, используемые в государственной информационной системе персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО» получены законными способами, цели сбора и обработки информации совместимы с целями, указанными в п. 1.1 настоящего Договора.

1.3.2. В государственной информационной системе персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО» реализованы меры защиты информации в соответствии с требованиями, предъявляемыми к защите по классу защищенности К3, установленному Приказом ФСТЭК России №17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», информационная система имеет действующий аттестат соответствия по требованиям безопасности информации.

1.3.3. Осуществляется своевременное доведение до Поверенной информации в случае изменения требований по информационной безопасности, предъявляемых к средствам вычислительной техники, входящими в состав государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО» и находящихся в эксплуатации Поверенного.

1.4. Поверенный гарантирует:

1.4.1. Эксплуатация средств вычислительной техники, входящей в состав государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО» осуществляется в полном соответствии с требованиями к защите информации, предъявляемыми Доверителем.

1.4.2. При эксплуатации средств вычислительной техники государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО» обеспечивается выполнение действующих условий и требований законодательства Российской Федерации к обработке и защите персональных данных.

1.4.3. Осуществляется незамедлительное уведомление Доверителя об изменениях следующих характеристик эксплуатируемых средств вычислительной техники, подключенной к государственной информационной системе персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО»: состав и условия размещения технических и программных средств и систем; состав (комплектность) продукции, используемой в целях защиты информации, схема ее монтажа (параметры установки и настройки), способствующие снижению класса защищенности системы.

1.5. Поверенный выполняет Поручение лично.

1.6. В случае изменений характеристик эксплуатируемых средств вычислительной техники государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО», оговоренных в п. 1.3 настоящего Договора, Поверенный информирует об этом Доверителя и действует в соответствии с его инструкциями.

## 2. КОНФИДЕНЦИАЛЬНОСТЬ

2.1. Стороны обязуются соблюдать режим конфиденциальности в отношении данных, ставших им известными при исполнении настоящего Договора.

2.2. При обработке информации на средствах вычислительной техники государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО» Поверенный обеспечивает их безопасность комплексом организационных и технических мер в необходимых для достижения указанной цели объемах. В частности, безопасность достигается применением по мере необходимости следующих мер:

2.2.1. Применением организационных и технических мер по обеспечению безопасности информации при ее обработке в государственной информационной системе персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО», необходимых для выполнения предъявляемых Доверителем требований к защите информации (локальные нормативные акты Доверителя, устанавливающие обязательные для выполнения требования к защите информации, приведены в Приложении №2 к настоящему Договору).

2.2.2. Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

2.2.3. Оценкой эффективности принимаемых мер по обеспечению безопасности информации до ввода в эксплуатацию средств вычислительной техники государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО».

2.2.4. Учетом машинных носителей информации государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО».

2.2.5. Обнаружением фактов несанкционированного доступа к компонентам государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО» и своевременным принятием мер по реагированию.

2.2.6. Восстановлением информации, обрабатываемой на эксплуатируемых средствах вычислительной техники государственной информационной системе персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО», модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.2.7. Установлением правил доступа к эксплуатируемым средствам вычислительной техники государственной информационной системе персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО» и регистрации действий пользователей.

2.2.8. Контролем за принимаемыми мерами по обеспечению безопасности информации и уровнем защищенности эксплуатируемых средств вычислительной техники государственной информационной системе персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО».

2.3. Режим конфиденциальности в отношении настоящего Договора действует в течение 3 лет до момента его прекращения.

### 3. ОБЯЗАННОСТИ И ПРАВА СТОРОН

3.1. Поверенный обязуется:

3.1.1. Своевременно и качественно выполнить Договор с соблюдением требований ст. ст. 18, 18.1, 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», ст. 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Приказа ФСТЭК России №17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

3.1.2. Принимать исчерпывающие меры по обеспечению безопасности информации и средств вычислительной техники государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО» при выполнении Договора.

3.1.3. Не использовать средства вычислительной техники, входящие в состав государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО», для целей, не связанных с исполнением Договора.

3.2. Доверитель обязуется:

3.2.1. Предоставить Поверенному средства защиты вычислительной техники, необходимые для исполнения Договора.

3.2.2. Не препятствовать Поверенному в доступе к государственной информационной системе персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО», необходимого для исполнения Договора.

### 4. ВОЗНАГРАЖДЕНИЕ ПОВЕРЕННОГО

4.1. Настоящий договор является безвозмездным.

### 5. ОТВЕТСТВЕННОСТЬ СТОРОН

5.1. Ответственность за действия Поверенного с персональными данными, связанные с исполнением настоящего Договора, несет Поверенный перед субъектом персональных данных.

5.2. Ответственность за обеспечение безопасности информации и требуемого уровня защищенности эксплуатируемых средств вычислительной техники государственной информационной системе персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО» несет Поверенный перед Доверителем.

5.3. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение своих обязательств по Договору, если оно произошло вследствие непреодолимой силы, то есть чрезвычайных и непредотвратимых обстоятельств, включая, но не ограничиваясь, наводнение, землетрясение, ураган, смерч, пожар и другие стихийные бедствия, военные

действия и гражданские волнения, изменения законодательства Российской Федерации, препятствующие сторонам в исполнении своих обязательств по договору.

## 6. СРОК ДЕЙСТВИЯ, ИЗМЕНЕНИЕ И ДОСРОЧНОЕ РАСТОРЖЕНИЕ ДОГОВОРА

6.1. Договор заключен на срок до «25» декабря 2020 года.

6.2. Все изменения и дополнения к Договору действительны, если совершены в письменной форме и подписаны обеими Сторонами. Соответствующие дополнительные соглашения Сторон являются неотъемлемой частью Договора.

## 7. РАЗРЕШЕНИЕ СПОРОВ

7.1. Стороны будут стремиться к разрешению всех возможных споров и разногласий, которые могут возникнуть по Договору или в связи с ним, путем переговоров.

7.2. Споры, не урегулированные путем переговоров, передаются на рассмотрение суда в порядке, предусмотренном действующим законодательством Российской Федерации.

## 8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1. Договор вступает в силу со дня его подписания Сторонами.

8.2. Договор составлен в двух экземплярах, по одному для каждой из Сторон.

## 9. РЕКВИЗИТЫ И ПОДПИСИ СТОРОН:

Доверитель:

Государственное автономное  
образовательное учреждение  
дополнительного  
профессионального образования  
Свердловской области «Институт  
развития образования»  
Юридический адрес:  
620137, Свердловская обл.,  
г. Екатеринбург, ул. Академическая,  
д.16

Почтовый адрес:  
620137, Свердловская обл.,  
г. Екатеринбург, ул. Академическая,  
д.16

ИНН/КПП 6662056567/667001001  
р/с 40601810165773000001  
л/с 30012906200, 33012906200  
Уральское ГУ Банка России  
БИК 046577001

Поверенный:

Муниципальное казенное общеобразовательное  
учреждение Харловская средняя  
общеобразовательная школа

Юридический адрес:

Индекс: 623804, Свердловская область,  
р-н ИРБИТСКИЙ,  
с. ХАРЛОВСКОЕ,

(населенный пункт)

ул. СОВЕТСКАЯ, д. 4А.

Почтовый адрес:

Индекс: 623804, Свердловская область,  
р-н ИРБИТСКИЙ,  
с. ХАРЛОВСКОЕ,

(населенный пункт)

ул. СОВЕТСКАЯ, д. 4А.

ИНН/КПП: 6611005821 1667601001

р/с 40204810700000226242

л/с 03906070910

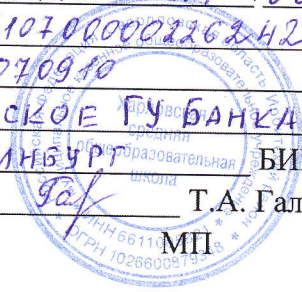
Банк УРАЛЬСКОЕ ГУ БАНКА РОССИИ

Г. ЕКАТЕРИНБУРГ БИК 046577001

Директор Т.А. Галишева

Ректор О.В. Гредина

МП



Состав средств защиты вычислительной техники государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО», переданных в эксплуатацию

На персональные компьютеры, используемые в государственной информационной системе персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО» могут быть установлены следующие программные средства:

- 1) АИС ГИА-9
- 2) ABBY TestReader Network
- 3) Станция печати TestReader
- 4) Модуль сканирования (драйвер сканера)
- 5) Acrobat Reader
- 6) Станция авторизации
- 7) Станция удаленного сканирования
- 8) Microsoft Office или OpenOffice.org
- 9) Microsoft Windows 7

В состав средств защиты информации, устанавливаемых на автоматизированных рабочих местах, используемых для обработки экзаменационных материалов в государственной информационной системе персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО», входят:

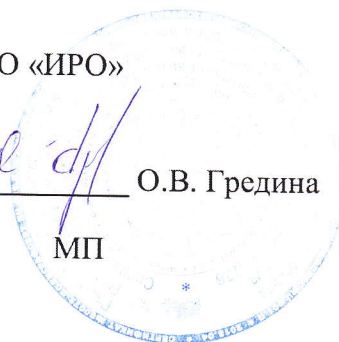
- 1) Средство защиты от вредоносного кода Kaspersky Endpoint Security 10 для Windows (сертификат соответствия ФСТЭК России №3025, выдан 25.11.2013, действителен до 25.11.2019).
- 2) Средство защиты информации от несанкционированного доступа Dallas Lock 8-0.K (сертификат соответствия ФСТЭК России №2720, выдан 25.09.2012, действителен до 25.09.2018).
- 3) Программный комплекс VipNet Client 4 (Сертификат соответствия ФСТЭК России №3727, выдан 30.11.2016, действителен до 30.11.2019; Сертификат соответствия ФСБ РФ СФ515-2907, выдан 17.06.2016, действителен до 29.04.2019; Сертификат соответствия ФСБ РФ СФ/124-2876, выдан 30.03.2016, действителен до 31.12.2018).

Установка иного программного обеспечения на автоматизированные рабочие места не допускается.

Настройка средств защиты информации должна обеспечивать третий класс защищенности (КЗ) в соответствии с Приказом ФСТЭК России №17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», и осуществляется в соответствии с требованиями по информационной безопасности, предъявляемыми Доверителем (Приложение №2 к настоящему Договору).

Доверитель:  
ГАОУ ДПО СО «ИРО»

Ректор \_\_\_\_\_ О.В. Гредина



Поверенный:

МКОУ Харловская СОШ

Директор \_\_\_\_\_ Т.А. Галишева



Состав требований по защите информации, предъявляемых к средствам вычислительной техники государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО»

1. Общие сведения

Центр обработки информации и организации ЕГЭ (структурное подразделение ГАОУ ДПО СО «ИРО») представляет собой подразделение, деятельность которого направлена на организационно-технологические и информационные сопровождения государственной итоговой аттестации выпускников образовательных организаций, завершающих освоение основных образовательных программ основного общего образования и среднего общего образования, на территории Свердловской области, в форме ЕГЭ и ОГЭ.

Аттестованный сегмент государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО» расположен по адресу г. Екатеринбург, ул. Академическая, 16.

Удаленное автоматизированное рабочее место государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО», находящееся в эксплуатации у Поверенного, расположено по адресу: индекс 623804, Свердловская область, р-н ИРБИТСКИЙ, с. ХАРЛОВСКОЕ, ул. СОВЕТСКАЯ д. 4А  
(населенный пункт)

2. Перечень подсистем обеспечения информационной безопасности, их назначение и основные характеристики

Перечень подсистем информационной безопасности, выполняемые ими функции и средства реализации функций представлены в таблице 2.1.

Таблица 2.1 – Перечень подсистем обеспечения информационной безопасности, выполняемые ими функции и средства реализации функций

Подсистемы обеспечения информационной безопасности	Функции подсистемы	Средства реализации функций
Управления доступом	Управление доступом к информационным ресурсам	ПК VipNet Client 4, СрЗИ от НСД Dallas Lock 8-0.К
Контроля целостности	Контроль состава и обеспечение неизменности программной среды рабочих станций. Контроль состава технических средств обработки информации	СрЗИ от НСД Dallas Lock 8-0.К
Регистрации и учета	Регистрация и сбор событий безопасности. Реагирование на события безопасности.	ПК VipNet Client 4, СрЗИ от НСД Dallas Lock 8-0.К, Kaspersky Endpoint Security 10 для Windows
Антивирусная защита	Защита от вредоносного кода. Регистрация событий обнаружения объектов, зараженных компьютерными вирусами в журнале регистрации событий.	Kaspersky Endpoint Security 10 для Windows

Подсистемы обеспечения информационной безопасности	Функции подсистемы	Средства реализации функций
	Формирование статистических отчетов о попытках и фактах заражения.	
Защиты межсетевого взаимодействия	Межсетевое экранирование. Криптографическая защита. Централизованное управление.	ПК VipNet Client 4

### 3. Требования, предъявляемые к функциям, выполняемым системой

#### 3.1 Требования к функциям подсистемы управления доступом

Подсистема управления доступом должна реализовывать следующие функции:

- управление доступом к информационным ресурсам.  
Функция управления доступом к информационным ресурсам должна обеспечивать:
  - использование для входа в ОС РС уникальных идентификаторов, позволяющих однозначно идентифицировать пользователей и процессы, запущенные от имени их учетной записи;
  - идентификацию и проверку подлинности пользователей при входе в ОС РС по идентификатору (коду) и паролю условно-постоянного действия длиной не менее восьми буквенно-цифровых символов;
  - идентификацию и проверку подлинности пользователей при входе в ОС РС с применением средств двухфакторной аутентификации;
  - максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток;
  - блокировку программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут;
  - смену паролей не более чем через 120 дней.

#### 3.2 Требования к функциям подсистемы регистрации событий безопасности

Подсистема регистрации событий безопасности должна реализовывать следующие функции:

- регистрация и сбор событий безопасности.
- реагирование на события безопасности.  
Функция регистрации и сбора событий безопасности должна обеспечивать:
  - регистрацию следующих событий:
    - вход (выход), а также попытки входа субъектов доступа в ГИСПДн и загрузки (останова) ОС;
    - подключение машинных носителей информации и вывод информации на носители информации;
    - запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;
    - попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;

- попытки удаленного доступа.
- хранение информации о событиях безопасности в течении срока, достаточного для расследования инцидентов безопасности.

Функция реагирования на события безопасности должна обеспечивать:

- возможность просмотра и анализа результатов регистрации событий, относящихся к безопасности информации, и реагирования на них;
- возможность своевременного реагирования на сбои, возникающие в процессе регистрации событий безопасности.

### 3.3 Требования к функциям подсистемы обеспечения целостности

Подсистема обеспечения целостности должна реализовывать следующие функции:

- контроль состава и обеспечение неизменности программной среды рабочих станций.
- контроль состава технических средств обработки информации.  
Функция обеспечения неизменности программной среды РС обеспечивает запрет установки (инсталляции) запрещенного к использованию ПО и (или) его компонентов, в том числе средств разработки и отладки.  
Функция контроля состава технических средств обработки информации обеспечивает запрет применения запрещенных технических средств обработки информации.

### 3.4 Требования к функциям подсистемы антивирусной защиты

Подсистема антивирусной защиты должна реализовывать следующие функции:

- Защита от вредоносного кода.
- Регистрация событий обнаружения объектов, зараженных компьютерными вирусами в журнале регистрации событий.
- Формирование статистических отчетов о попытках и фактах заражения.

### 3.5 Требования к функциям подсистемы защиты межсетевого взаимодействия

Подсистема защиты межсетевого взаимодействия должна реализовывать следующие функции:

- Межсетевое экранирование.
- Криптографическая защита.  
Функция межсетевого экранирования обеспечивает:
  - фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
  - фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств. Перечень служебных протоколов определяется Организацией, осуществляющей ввод в действие МСВ ИРО, на стадии Ввода в действие;
  - фильтрацию на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя (сетевой адрес, порт);
  - регистрацию и учет фильтруемых пакетов;
  - регистрацию и учет запросов на установление виртуальных соединений;
  - локальную сигнализацию попыток нарушения правил фильтрации;
  - идентификацию и аутентификацию администратора межсетевого экрана (МЭ) при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;



- предотвращение доступа к МЭ неидентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась;
- идентификацию и аутентификацию администратора МЭ при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации;
- регистрацию входа (выхода) администратора МЭ в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения МЭ);
- регистрацию действий администратора МЭ по изменению правил фильтрации.

### 3.6 Требования к видам обеспечения

#### 3.6.1 Требования к техническому обеспечению

Состав применяемых средств защиты информации приведен в разделе 2 настоящего Приложения.

Конфигурация применяемых средств защиты информации предоставляется Доверителем при передаче средств защиты вычислительной техники в эксплуатацию Поверенному.

#### 3.6.2 Требования к программному обеспечению

Состав ПО, устанавливаемого на средства вычислительной техники, должен соответствовать составу, зафиксированному в Приложении 1 к настоящему Договору.

ПО должно обладать соответствующими лицензиями на его использование.

Применяемые средства защиты информации должны иметь свидетельства прохождения в установленном порядке процедуры оценки соответствия средств защиты информации (должны быть сертифицированными ФСТЭК России).

#### 3.6.3 Требования к организационному и другим видам обеспечения

Поверенному необходимо обеспечить выполнение организационных мер защиты, закрепленных в следующих организационно-распорядительных документах Доверителя (комплект документации передается Доверителем при подписании настоящего Договора):

- 1) Положение по организации и проведению работ по обеспечению безопасности информации при ее обработке в государственных информационных системах персональных данных государственного автономного образовательного учреждения дополнительного профессионального образования Свердловской области «Институт развития образования», утвержденное приказом ректора Института Грединой О.В. от 16.03.2017 №103, с приложениями:
  - Приложение №1 «Регламент разграничения прав доступа»;
  - Приложение №2 «Регламент по работе с защищаемыми носителями информации»;
  - Приложение №3 «Регламент по организации парольной защиты в государственной информационной системе персональных данных»;
  - Приложение №4 «Регламент по организации антивирусного контроля в государственной информационной системе персональных данных»;
  - Приложение №5 «Регламент внесения изменений в государственные информационные системы»;

- 2) Положение по обработке и защите персональных данных государственного автономного образовательного учреждения дополнительного профессионального образования Свердловской области «Институт развития образования», утвержденное приказом ректора Института Грединой О.В. от 12.12.2014 №353, с приложениями:
    - Приложение №1 «Согласие на обработку персональных данных (в редакции приказа ГАОУ ДПО СО «ИРО» от 12.07.2017 №252»;
  - 3) Положение об организации режима безопасности помещений информационных систем, в которых осуществляется обработка конфиденциальной информации государственного автономного образовательного учреждения дополнительного профессионального образования Свердловской области «Институт развития образования», утвержденное приказом ректора Института Грединой О.В. от 16.03.2017 №101, с приложениями:
    - Приложение №1 «Журнал вскрытия помещения»;
    - Приложение №1 «Журнал учета ключей от помещений»;
  - 4) Положение о проведении контроля эффективности защиты информации, утвержденное приказом ректора Института Грединой О.В. от 16.03.2017 №99, с приложениями:
    - Приложение №1 «Форма отчета о проведении проверки контроля эффективности защиты информации»;
  - 5) Положение о порядке организации и контроля использования средств криптографической защиты информации государственного автономного образовательного учреждения дополнительного профессионального образования Свердловской области «Институт развития образования», утвержденное приказом ректора Института Грединой О.В. от 16.03.2017 №105;
  - 6) Регламент резервного копирования, применяемого при использовании системы резервного копирования и восстановления данных государственного автономного образовательного учреждения дополнительного профессионального образования Свердловской области «Институт развития образования», утвержденное приказом ректора Института Грединой О.В. от 16.03.2017 №102, с приложениями:
    - Приложение А «Перечень данных, подлежащих резервному копированию»;
    - Приложение Б «Политики создания и хранения данных резервных копий»;
    - Приложение В «Перечень лиц, ответственных за систему резервного копирования и восстановления данных»;
    - Приложение Г «Журнал настроек»;
    - Приложение Д «Методика резервного копирования»;
    - Приложение Е «Методика проведения периодических проверок резервных копий»;
    - Приложение И «Методика восстановления данных»;
    - Приложение К «Основные критерии результативности системы резервного копирования и восстановления данных»;
  - 7) Положение о порядке выявления и реагирования на инциденты информационной безопасности государственного автономного образовательного учреждения дополнительного профессионального образования Свердловской области «Институт развития образования», утвержденное приказом ректора Института Грединой О.В. от 16.03.2017 №104, с приложениями:
    - Приложение №1 «Перечень инцидентов информационной безопасности».
- Поверенному необходимо принять и поддерживать в актуальном состоянии соответствующие организационно-распорядительные документы в составе:
- 1) Журнал учета защищаемых носителей информации.

- 2) Журнал учета средств защиты информации, эксплуатационной и технической информации к ним.
- 3) Журнал проведения проверок состояния защиты эксплуатируемых средств вычислительной техники государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО».
- 4) Матрица доступа пользователей к эксплуатируемым средствам вычислительной техники государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО».
- 5) Перечень помещений, в которых размещены эксплуатируемые средства вычислительной техники государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО».
- 6) Приказ о назначении администратора безопасности при работе с эксплуатируемыми средствами вычислительной техники государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО».
- 7) Инструкция администратора безопасности при работе с эксплуатируемыми средствами вычислительной техники государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО».
- 8) Приказ о назначении должностного лица, отвечающего за организацию обработки персональных данных в организации Поверенного.
- 9) Инструкция должностного лица, отвечающего за организацию обработки персональных данных в организации Поверенного.
- 10) Приказ о назначении лица, ответственного за обеспечение безопасности информации в организации Поверенного.
- 11) Инструкция лица, ответственного за обеспечение безопасности информации в организации Поверенного.
- 12) Приказ об определении границ контролируемой зоны организации Поверенного.
- 13) Приказ об утверждении плана внутренних проверок состояния защиты эксплуатируемых средств вычислительной техники государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО».
- 14) Список лиц, допущенных в помещения, в которых размещены эксплуатируемые средства вычислительной техники государственной информационной системы персональных данных Центра обработки информации и организации ЕГЭ ГАОУ ДПО СО «ИРО».

Доверитель:

ГАОУ ДПО СО «ИРО»

Ректор \_\_\_\_\_

О.В. Гредина

МП

Поверенный:

МКОУ Харловская СОШ

Директор \_\_\_\_\_

Т.А. Галишева

