ЕДИНАЯ ИНФОРМАЦИОННАЯ СИСТЕМА УЧЕТА И МОНИТОРИНГА ОБРАЗОВАТЕЛЬНЫХ ДОСТИЖЕНИЙ ОБУЧАЮЩИХСЯ ОБЩЕОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ МОСКОВСКОЙ ОБЛАСТИ

Шаблоны организационно-распорядительных документов для типовых сегментов

Содержание

ПРОЕКТ ПРИКАЗА ОБ ОРГАНИЗАЦИИ РАБОТ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ОБРАБОТКЕ В ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ

ПРИКАЗ
_____ года№ _____
Об организации работ по защите персональных данных при обработке в государственной информационной системе

В целях организации работы по защите персональных данных в государственной информационной системе «XXXXXXXXXX» Организации XXXXXXX, с учетом требований Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных», методических документов Федеральной службы по техническому и экспортному контролю Российской Федерации и в соответствии Руководящим документом Государственной технической комиссии при Президенте Российской Федерации от 30.08.2002 года № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденным Приказом Государственной технической комиссии при Президенте Российской Федерации от 30.08.2002 года № 282.

ПРИКАЗЫВАЮ:

1. Разработать (указывается комплект ОРД для разработки):

2. Назначить ответственным за обеспечение информационной безопасности (администратор информационной безопасности) _____.

3. Возложить ответственность за выполнение требований по защите персональных данных, в соответствии с документом «Положением об обработке ПДн» и законодательством Российской Федерации, методическое руководство, реализацию и контроль за эффективностью мер по защите персональных данных на администратора информационной безопасности.

4. Администратору информационной безопасности:

Организовать работу в соответствии с документом «Инструкция администратора информационной безопасности».

5. Требования документа «Положения об обработке ПДн» в части работы с персональными данными в электронном виде вступают в силу с момента ввода в эксплуатацию системы защиты персональных данных Системы и утверждения документа «Инструкция пользователя информационной системы персональных данных».

6. Контроль за исполнением настоящего приказа оставляю за собой.

ПРОЕКТ ПРИКАЗА О НАЗНАЧЕНИИ АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПРИКАЗ

№ от «____»_____ 2015 года

о назначении администратора информационной безопасности

В целях проведения мероприятий по обеспечению безопасности персональных данных, обрабатываемых в государственной информационной системе, «XXXXXXXXXX» и для осуществления контроля их выполнения сотрудниками XXXXXXXXX.

П Р И К А З Ы В А Ю:

1. Назначить администратором информационной безопасности на площадках по адресам:
2. Администратору в работе руководствоваться «Инструкцией администратора информационной безопасности».
3. Контроль за выполнением настоящего приказа оставляю за собой.

Должность Подпись ФИО

ПОЛИТИКА В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1 Общие положения

Указывается для чего разработана данная политика. Для какой системы. Дается общая информация.

2 Правовые основания и цели обработки персональных данных

Описывается нормативная база на основании которой разрабатывается политика Оператора в области обработки персональных данных. Указывается перечень локальных документов, разработанных во исполнении настоящей политики.

Указываются цели обработки персональных данных.

3 Обрабатываемые категории персональных данных и источники их поступления

В информационных системах персональных данных Оператора обрабатываются следующие категории персональных данных: (Перечисляются все ПДн обрабатываемые в системе).

4 Основные принципы обработки, передачи и хранения персональных данных

Указывается информация об обеспечении принципов обработки ПДн, указывается информация о трансграничной передаче данных. Другая информация на усмотрение оператора.

5 Меры по обеспечению безопасности персональных данных при их обработке

Указываются меры для защиты ПДн, принимаемые оператором.

6 Права субъектов персональных данных

Описываются права субъектов ПДн.

7 Сроки обработки (хранения) персональных данных

Указываются сроки обработки и хранения ПДн..

8 Уточнение, блокирование и уничтожение персональных данных

Указываются цели блокировки и уничтожения ПДн, а также способы и порядок процедур.

9 Заключительные положения

Описываются случаи при которых данная политика подлежит изменению, а также на кого возлагается контроль за исполнением требований данной политики

ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1 Общие положения

Настоящее положение о порядке организации и проведения работ по технической защите персональных данных (далее – Положение) является основным документом по защите персональных данных, содержащихся в базах данных, и определяет цели, порядок организации, планирования и выполнения мероприятий по технической защите персональных данных.

Состав персональных данных представлен в документе…….

Положение разработано в соответствии с требованиями ……

Требования Положения направлены на …...

Основные направления работ по защите персональных данных (далее – ЗПДн):

1…

2…

3…

2 Порядок определения защищаемой информации

Описывается порядок определения защищаемой информации.

3 Порядок привлечения специализированных сторонних организаций при разработке и эксплуатации объектов информатизации и средств защиты

Организация работ по ЗПДн, методическое руководство, реализация и контроль за эффективностью мер по ЗПДн возлагается на ответственного за обеспечение информационной безопасности (администратора информационной безопасности).

Для выполнения мероприятий по ЗПДн могут привлекаться специализированные организации, имеющие соответствующие лицензии ФСТЭК и/или ФСБ России.

При выполнении отдельных видов работ по ЗПДн с привлечением специализированных организаций определяются отдельные специалисты, ответственные за организацию и проведение этих работ.

Планируемые мероприятия по ЗПДн разрабатываются ответственным за обеспечение информационной безопасности и включаются отдельным разделом в годовой план мероприятий по ЗПДн.

Раздел плана по ЗПДн должен включать следующие подразделы:

- мероприятия по выполнению решений ФСТЭК России, приказов и распоряжений вышестоящей организации по ЗПДн;
- организационно-методическое обеспечение работ по ЗПДн (разработка, корректировка и согласование организационно-методических документов, планов, отчетов; составление заявок на технические устройства ЗПДн; обучение сотрудников);
- контрольные мероприятия (оценка достаточности применяемых мер и средств ЗПДн; эффективность принимаемых мер ЗПДн; участие в работе контролирующих органов).

4 Порядок разработки, ввода в действие и эксплуатации объектов информатизации

Порядок, методы и способы ЗПДн определяются руководящими и нормативно-методическими документами ФСБ и ФСТЭК России.

Достаточность принятых мер по обеспечению безопасности ПДн при её обработке в системах оценивается при проведении государственного контроля и надзора.

Безопасность ПДн при их обработке в ГИС обеспечивается с помощью СЗПДн, включающей организационные меры и средства защиты информации, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки, а также используемые в ГИС информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

Эксплуатация СЗПДн и средств защиты в её составе осуществляется в соответствии с технологическим процессом и инструкциями по эксплуатации средств защиты.

Для обеспечения защиты ПДн при эксплуатации СЗПДн и средств защиты необходимо соблюдать следующие требования:

–
–
–
–
–

Все носители ПДн на бумажной, магнитной, оптической (магнито-оптической) основе, используемые в процессе обработки ПДн в ГИС, подлежат учету в соответствии с….

Временно не используемые учтенные носители информации должны храниться в специально оборудованных для этого местах, недоступных для посторонних лиц в соответствии с ….

Периодический контроль включает в себя:

1

2

3

5 Ответственность должностных лиц

Должностными лицами, ответственными за организацию и осуществление мероприятий по ЗПДн являются:

–

Функциональные обязанности и права:

6 Основные нормативные правовые акты и методические документы по защите информации

1) Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;

2) Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ;

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

4) приказа ФСТЭК России «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах персональных данных» от 11.02.2013 № 17;

5) приказа ФСБ России «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» от 10.07.2014 № 378;

6) Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";

7) «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной ФСТЭК России 15.02.2008;

8) «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной ФСТЭК России 14.02.2008;

9) ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;

10) ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования».

7 Список сокращений

Сокращение	Обозначение

ПОЛОЖЕНИЕ О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ЕЁ ОБРАБОТКЕ В СИСТЕМЕ

1 Общие положения

1.1 Данное «Положение об организации и проведению работ по обеспечению безопасности персональных данных при их автоматизированной обработке в «XXXXXXXX» (далее – Положение) разработано в соответствии с Законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», методическими рекомендациями ФСТЭК России и ФСБ России в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн).

1.2 Положение определяет порядок работы персонала государственной информационной системы «Единая информационная система учета и мониторинга образовательных достижений обучающихся общеобразовательных организаций Московской области» (далее – ГИС) в части обеспечения безопасности ПДн при их обработке, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в ГИС, порядок проверки электронного журнала обращений к ГИС, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ГИС, порядок охраны и допуска посторонних лиц в защищаемые помещения.

2 Порядок работы пользователей ГИС в части обеспечения безопасности ПДн при их обработке в ГИС

2.1 Настоящий порядок определяет действия пользователей ГИС в части обеспечения безопасности ПДн при их обработке в ГИС. Далее подробно описание прав и обязанностей пользователей и ответственных за обеспечение ИБ.

3 Порядок контроля защиты информации в ГИС и приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления. Порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации и принятие мер по предотвращению возможных опасных последствий

Подробное описание задач и видов контроля защиты информации. Порядок ведения контроля и исполнителей.

4 Заключительные положения

4.1 Требования настоящего Положения обязательны для всех сотрудников обрабатывающих конфиденциальную информацию (персональные данные).

4.2 Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

ПЕРЕЧЕНЬ ЗАЩИЩАЕМЫХ РЕСУРСОВ ГИС ИСУОД

Перечень защищаемых ресурсов

№ п/п	Наименование защищаемого информационного ресурса	Описание
1.	Средства настройки и управления СЗИ Системы от НСД.	–
2.	Основные конфигурационные файлы ПО и СЗИ Системы, участвующего в обработке ПДн.	–
3.	Отчуждаемые накопители (магнитные и оптические диски, флэш-носители и др.), содержащие ПДн из Системы.	
4.	Основные конфигурационные файлы ОС Системы.	
5.	Файлы баз данных и средств управления базами данных Системы.	

Список терминов и сокращений

Сокращение	Расшифровка
Система	Аппаратно-программный единой информационной системы учета и мониторинга образовательных достижений обучающихся общеобразовательных организаций Московской области.
БД	База данных.
НСД	Несанкционированный доступ.
ОС	Операционная система.
ПДн	Персональные данные.
ПО	Программное обеспечение.
СЗИ	Система защиты информации.
СУБД	Система управления базами данных.

ПЕРЕЧЕНЬ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА ОРГАНИЗАЦИИ

УТВЕРЖДАЮ

_____

_____

_____

(ФИО)

«___»_____ 20__ г.

Перечень сведений конфиденциального характера организации XXXXXXXXXX

№ п/п	Наименование Системы	Перечень сведений, обрабатываемых в системе

ПЕРЕЧЕНЬ СОТРУДНИКОВ, ДОПУЩЕННЫХ К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ

УТВЕРЖДАЮ

_____
_____

_____
(ФИО)

«___»_____ 20__ г.

Перечень сотрудников, допущенных к обработке персональных данных в государственной информационной системе XXXXXXXXXX

№ п/п	Фамилия, имя, отчество	Должность

ПОРЯДОК ВЗАИМОДЕЙСТВИЯ С УПОЛНОМОЧЕННЫМ ОРГАНОМ ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

1 Общие положения

1.1 Настоящий документ определяет порядок взаимодействия с уполномоченным органом по защите прав субъектов персональных данных (далее – ПДн) в целях организации соблюдения требований Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных» (далее – Закон).

1.2 Перед началом обработки ПДн Оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных (далее – Роскомнадзор) о своем намерении осуществлять обработку ПДн, за исключением случаев, предусмотренных частью 2 статьи 22 Закона.

1.3 Требования Положения обязательны для исполнения всеми сотрудниками Оператора, на кого оно распространяется.

1.4 В процессе взаимодействия с уполномоченным органом по защите прав субъектов ПДн принимает участие Ответственный за организацию обработки ПДн.

2 Обязанности оператора персональных данных, права Роскомнадзора

Описываются обязанности оператора ПДн в соответствии с действующим законодательством.

3 Порядок взаимодействия с уполномоченным органом по защите прав субъектов персональных данных

Подробно описывается порядок взаимодействия с уполномоченным органом. Порядок внесения изменений в реестр операторов ПДн. Порядок и сроки ответов на запросы уполномоченных органов. Порядок взаимодействия при проведении проверок.

Приложение А

Шаблоны документов для взаимодействия с уполномоченным органом по защите прав субъектов ПДн

1.1 Уведомление о внесении изменений в ПДн

Руководителю территориального Управления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций

УВЕДОМЛЕНИЕ
о внесении изменений в персональные данные

Тип оператора: юридическое лицо

Наименование:

Адрес: _____

действующее в соответствии с: _____
(правовое основание обработки персональных данных)

в отношении персональных данных: _____
(имя субъекта персональных данных)

на основании: _____
(основание внесения изменений в персональные данные)

внесло следующие изменения:

наименование	***исходное значение***	***изменено***
(наименование категории персональных данных: ФИО, адрес, телефон и т.п.)	(исходное значение)	(новое значение)

Указанные персональные данные вводятся в обработку с учетом внесенных изменений с _____
(дата возобновления обработки)

Срок или условие прекращения обработки персональных данных _____

_____

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

«__» _____ 201_ г.

1.2 Уведомление об уничтожении ПДн

Руководителю территориального Управления
Федеральной службы по надзору в сфере связи,
информационных технологий и массовых
коммуникаций

УВЕДОМЛЕНИЕ
об уничтожении персональных данных

Тип оператора: юридическое лицо

Наименование:

Адрес: _____

Руководствуясь: _____
(правовое основание обработки персональных данных)

в целях: _____
(цель обработки персональных данных)

осуществлял обработку следующих категорий персональных данных:

_____

_____
(перечень ПДн)

принадлежащих _____
(имя субъекта персональных данных)

_____
(если имеются, дополнительные сведения для идентификации: дата рождения / адрес…)

с _____ по _____
(дата начала обработки персональных данных) (дата прекращения обработки)

Обработка вышеуказанных персональных данных оператором была прекращена, а сами данные уничтожены в связи с:

_____
(причина прекращения обработки персональных данных: окончание срока обработки или событие, с которым связано достижение цели или утрата необходимости обработки)

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

«__» _____ 201_ г.

1.3 Уведомление об устранении нарушений в порядке обработке ПДн

Руководителю территориального Управления
Федеральной службы по надзору в сфере связи,
информационных технологий и массовых
коммуникаций

УВЕДОМЛЕНИЕ

об устранении нарушений в порядке обработки персональных данных

Тип оператора: юридическое лицо

Наименование:

Адрес: _____

В отношении порядка обработки персональных данных, принадлежащих:

_____

_____

(имя субъекта персональных данных и дополнительные сведения для идентификации, если имеются: дата рождения / адрес…)

Были допущены следующие нарушения:

_____

(указать выявленные нарушения)

Указанные нарушения были устранены _____

(дата устранения нарушений)

на основании: _____

(правовое основание устранения выявленных нарушений)

Персональные данные вновь вводятся в обработку с _____

(дата ввода в обработку)

Срок или условие прекращения обработки персональных данных:

_____

_____ _____ _____

(должность) (подпись) (Ф.И.О.)

«__» _____ 201_ г.

ЛИСТ ОЗНАКОМЛЕНИЯ СОТРУДНИКОВ

с Порядком взаимодействия с уполномоченным органом по защите прав субъектов персональных данных

С Порядком ознакомлен(ы):

№ п/п	Ф.И.О. сотрудника	Дата ознакомления	Подпись в ознакомлении
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			
26.			
27.			
28.			
29.			
30.			
31.			
32.			

ПОРЯДОК ОБРАБОТКИ ОБРАЩЕНИЙ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

1 Термины и определения

Субъект персональных данных – физическое лицо, чьи данные обрабатываются либо могут обрабатываться у Оператора.

Оператор – обработчик персональных данных.

2 Общие положения

Регламент реагирования на обращения субъектов (далее − Регламент), разработан в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных», действующим законодательством.

Регламент устанавливает правила оформления ответа субъектам персональных данных.

3 Права субъекта персональных данных

Субъект имеет право:

4 Правила оформления запроса субъекта

Описание правил оформления запроса

5 Правила составления ответа субъекту

Ответ должен быть отправлен в течение 10 дней с даты получения запроса от субъекта персональных данных. Ответ должны составить совместно сотрудники информационной безопасности и сотрудники юридического управления, четко определить цели и сроки к конкретному субъекту персональных данных и дать грамотный ответ, в письменном виде используя бланк ответа (Приложение А).

6 Правила регистрации обращений субъектов

При поступлении запроса обращения субъектов (Приложение В), сотрудник обязан зарегистрировать такой запрос в журнале регистрации обращений субъектов (Приложение Б). Сотруднику необходимо указать свое ФИО и должность, отметить в журнале дату поступления запроса, а также указать ФИО субъекта персональных данных.

Приложение А

/Бланк организации/

Гражданину/Гражданке ФИО

Ответ на запрос субъекта персональных данных

На Ваш запрос, полученный от _____. относительно обработки Ваших персональных данных сообщаем следующее.

1. ООО «XXXXXXXXX» обрабатывает Ваши персональные данные, на основании подписанного с Вами договора №____ от _____ или на ином основании _____
   со следующими целями и сроками:
   –
   –
2. Обрабатываются следующие персональные данные:
   –
3. Способ обработки персональных данных:

С использованием средств автоматизации ____, без использования средств автоматизации ____

4. Обработка персональных данных включает следующие действия: сбор, систематизацию, накопление, хранение, уточнение, использование, блокирование, уничтожение, а также право на передачу такой информации третьим лицам и получение информации и документов от третьих лиц для осуществления проверки достоверности и полноты информации о Субъекте и в случаях, установленных законодательством.

5. Обработкой Ваших персональных данных занимаются сотрудники_____, никто другой к обработке Ваших персональных данных не допускается. Ваши персональные данные будут обрабатываться вплоть до достижения указанных целей обработки. Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением,
Должность ФИО отправителя

(дата, подпись, печать)

Приложение Б

Журнал регистрации обращений субъектов персональных данных

От кого: ФИО субъекта	Дата получения запроса	ФИО получателя/роспись	Дата отправки ответа субъекту

Приложение В

В ООО «XXXXXXXX»
Адрес:

**Запрос на предоставление информации
об обработке персональных данных**

От_____
(фамилия, имя, отчество)

Паспорт:
_____выданный_____
(серия, номер) (дата выдачи)

_____
(место выдачи паспорта)

Адрес:
_____
(адрес места жительства)

Основания, по которым лицо выступает в качестве законного представителя субъекта персональных данных:_____

Сведения, подтверждающие факт обработки персональных данных в ООО «XXXXXX»:_____
_____

В соответствии со ст.14 федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных» прошу предоставить следующую информацию, касающуюся обработки моих персональных данных:

- Подтвердить факт обработки моих персональных данных;
- Правовые основания и цели обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- относящиеся ко мне обрабатываемые персональные данные;
- сроки обработки персональных данных, в том числе сроки их хранения;
- информацию об осуществленной или о предполагаемой трансграничной передаче моих персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку моих персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения_____

Данный запрос является первичным/повторным, на основании того, что:_____
_____
Указанные сведения прошу предоставить по адресу:_____
_____

_____ _____ _____
(дата) (подпись) (расшифровка подписи)

ИНСТРУКЦИЯ АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1 Общие положения

Настоящая инструкция определяет функции администратора информационной безопасности.

Администратор информационной безопасности назначается на должность и освобождается от должности в установленном действующим трудовым законодательством порядке приказом.

2 Основные функции администратора информационной безопасности

Основные функции администратора информационной безопасности:

3 Порядок парольной защиты в ГИС

Описываются действия администратора о контролю исполнения требований парольной политики в организации.

4 Порядок программно-технического обслуживания ГИС

Описываются действия администратора по обеспечению программно-технического обслуживания системы.

5 Перечень нормативных документов, использованных при разработке данной инструкции

Перечень нормативных документов, использованных при разработке данной инструкции:

6 Список терминов и сокращений

Сокращение	Расшифровка
Система, ИСУОД	Аппаратно-программный единой информационной системы учета и мониторинга образовательных достижений обучающихся общеобразовательных организаций Московской области.
ГИС	Государственная информационная система.
ПДн	Персональные данные.

Сокращение	Расшифровка
Система, ИСУОД	Аппаратно-программный единой информационной системы учета и мониторинга образовательных достижений обучающихся общеобразовательных организаций Московской области.
ПО	Программное обеспечение.
ТС	Технические средства.
ФСБ	Федеральная служба безопасности.
ФСТЭК	Федеральная служба по техническому и экспортному контролю.

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ

1 Общие положения

Настоящая инструкция определяет функции пользователя системы «XXXXXXXXX» по вопросам обеспечения конфиденциальности при проведении в системе работ с использованием персональных данных.

К пользователям системы относятся:

2 Основные функции пользователя

2.1 Обязанности пользователя

2.2 Права пользователя

2.3 Ответственность пользователя

3 Порядок парольной защиты в системе

Описывается подробно порядок парольной защиты в системе.

4 Перечень нормативных документов, использованных при разработке данного порядка

Перечень нормативных документов, использованных при разработке данного порядка:

5 Список терминов и сокращений

Сокращение	Расшифровка

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ БЕЗОПАСНОСТИ

1 Общие положения

Данный документ определяет правила и основные требования по обеспечению антивирусной защиты

2 Инструкция по применению средств антивирусной защиты

Подробная инструкция. Какие средства применяются, настройка средств, частота и порядок обновления, действия пользователей и администратора.

3 Список терминов и сокращений

Сокращение	Расшифровка

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ В СЕГМЕНТЕ ГИС ИСОУД

1 Правила формирования пароля

Описываются правила формирования пароля к системе.

2 Правила ввода пароля

Описываются правила ввода пароля

3 Правила хранение пароля

К хранению пароля применяются следующие правила:

ПОЛОЖЕНИЕ О РАЗРЕШИТЕЛЬНОЙ СИСТЕМЕ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ, СОДЕРЖАЩИМСЯ В ГИС ИСУОД

1. Общие положения

Настоящее Положение устанавливает правила доступа сотрудников XXXXX (далее Предприятие) и сторонних организаций к персональным данным, содержащимся в базах данных (далее – персональные данные).

В настоящем Положении используются следующие основные понятия:

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»).

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»).

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания (в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»).

Информационные ресурсы Предприятия, содержащие персональные данные – отдельные документы и массивы документов, а также документы и массивы документов в информационных системах (банках данных, архивах), доступ к которым ограничен в соответствии с действующим законодательством и локальными нормативными документами Предприятия, и которые содержат персональные данные.

Доступ пользователя к информационным ресурсам – ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

2. Порядок предоставления доступа

Описывается порядок предоставления доступа, основания его предоставления.

3. Порядок получения разрешения на предоставление доступа

Описывается порядок получения разрешения на предоставление доступа, указываются лица, уполномоченные разрешать доступ.

4. Порядок прекращения доступа

Описывается порядок прекращения доступа, основания для прекращения доступа

5. Контроль доступа к информационным ресурсам

Описывается каким образом и кем осуществляется контроль предоставления доступа.

6. Ответственность

Описание ответственности всех задействованных лиц.

7. Перечень нормативных документов, использованных при разработке данного порядка

Приводится перечень нормативных документов, использованных при разработке Порядка.

Приложение А

Заявка на доступ к информационным ресурсам

Наименование информационного ресурса	
ФИО сотрудника, получающего доступ	
Права	
Основание получения доступа	

Подпись руководителя структурного подразделения, запрашивающего доступ:

Должность подпись ФИО

Согласовано:

Администратор

информационной безопасности ФИО

Доступ предоставлен:

Администратор АС ФИО

Отметка об ознакомлении пользователя с нормативными документами по информационной безопасности :

Дата	Подпись

ИНСТРУКЦИЯ ПО АРХИВАЦИИ ИНФОРМАЦИОННЫХ РЕСУРСОВ СИСТЕМЫ

1 Назначение и область действия

Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ определяет действия (далее – Инструкция), связанные с функционированием системы «XXXXXXXXX» (далее – Система), меры и средства поддержания непрерывности работы и восстановления работоспособности Системы.

Целью настоящего документа является превентивная защита элементов системы от предотвращения потери защищаемой информации.

Задачей данной Инструкции является:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

Действие настоящей Инструкции распространяется на всех пользователей Системы, имеющих доступ к ресурсам, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается Администратор системы.

Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается Администратор информационной безопасности.

2 Порядок реагирования на инцидент

В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов системы, предоставляемых пользователям системы, а также потерей защищаемой информации.

Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;

- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств системы;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

Все действия в процессе реагирования на Инцидент должны документироваться ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю».

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники (Администратор информационной безопасности, Администратор и Оператор системы), предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

3 Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1 Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения системы включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Все критичные помещения (помещения, в которых размещаются элементы системы и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств системы в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы системы, сетевое и коммуникационное

оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

Системы обеспечения отказоустойчивости:

- кластеризация;
- технология RAID.

Для обеспечения отказоустойчивости критичных компонентов системы при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов системы должны использоваться территориально удаленные системы кластеров.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т. п.).

3.2 Организационные меры

Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных – не реже раза в неделю;
- для технологической информации – не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы системы – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

Носители должны храниться в несгораемом шкафу в помещении, оборудованном системой пожаротушения.

Носители должны храниться не менее года, для возможности восстановления данных.

4 Список терминов и сокращений

Сокращение	Расшифровка

ИНСТРУКЦИЯ ПО ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

1. Общие положения

Настоящая Инструкция разработана в соответствии с «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным постановлением Правительства РФ от 15.09.2008 № 687, является дополнением к «Положению об обработке персональных данных в _____»

(наименование образовательного учреждения)

и определяет правила работы с персональными данными и их материальными носителями без использования средств автоматизации.

Обработка персональных данных, полученных от работника, содержащихся в государственной информационной системе «ИСУОД» (далее - ГИС) либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Документ, содержащий персональные данные - материальный носитель с зафиксированной на нем в любой форме информацией, содержащей персональные данные работников (или граждан в договорах с физическими лицами) в виде текста, фотографии и (или) их сочетания.

С учетом большого объема (массовости) документов, содержащих персональные данные, и строго регламентированного порядка их хранения пометка конфиденциальности на них не ставится.

С настоящей инструкцией должны быть ознакомлены под подпись работники, допускаемые к обработке персональных данных без использования средств автоматизации. Листы ознакомления хранятся у ответственного за систему защиты информации в информационной системе персональных данных.

2. Порядок обработки персональных данных

Персональные данные должны обособляться от иной информации путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков).

При фиксации персональных данных на материальных носителях не допускается фиксации на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных - использовать отдельный материальный носитель для каждой из категорий.

Работники, осуществляющие обработку персональных данных, информируются непосредственным начальником (руководителем) о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

Типовые формы документов должны быть составлены таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

Хранение документов, содержащих персональные данные, осуществляется в металлических шкафах или сейфах.

Уничтожение документов, содержащих персональные данные, осуществляется способом, не позволяющим в дальнейшем ознакомиться с персональными данными.

3. Обязанности сотрудника, допущенного к обработке персональных данных

При работе с документами, содержащими персональные данные, сотрудник обязан исключить возможность ознакомления, просмотра этих документов лицами, не допущенными к работе с ними (в том числе другими работниками своего структурного подразделения).

При выносе документов, содержащих персональные данные, за пределы территории

_____

(наименование образовательного учреждения)

(далее - ОУ) по служебной необходимости сотрудник должен принять все возможные меры, исключающие утрату (утерю, хищение) таких документов.

При утрате (утере, хищении) документов, содержащих персональные данные, работник обязан немедленно доложить о таком факте своему непосредственному начальнику (руководителю). Непосредственный начальник (руководитель) должен сообщить заместителю директора, курирующему вопросы защиты информации о факте утраты (утере, хищении) документов, содержащих персональные данные. По каждому такому факту назначается служебное расследование.

4. Сотрудникам, допущенным к обработке персональных данных, запрещается:

1. Сообщать сведения, являющиеся персональными данными, лицам, не имеющим права доступа к этим сведениям.

2. Делать неучтенные копии документов, содержащих персональные данные.

3. Оставлять документы, содержащие персональные данные, на рабочих столах без присмотра.

4. Покидать помещение, не поместив документы с персональными данными в закрываемые сейфы, шкафы.

5. Выносить документы, содержащие персональные данные, из помещений ОУ без служебной необходимости.

5. Ответственность

1. Ответственность за неисполнение или ненадлежащее выполнение требований настоящей Инструкции возлагается на работников и руководителей подразделений.

2. Контроль за выполнением положений настоящей Инструкции возлагается на ответственного за систему защиты информации (СЗИ) ГИС в ОУ.

3. За нарушение правил обработки персональных данных, их неправомерное разглашение или распространение, виновные лица несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

4. В случае если в результате действий работника был причинен подлежащий возмещению работодателем ущерб третьим лицам, работник несет перед работодателем материальную ответственность в соответствии с главой 39 Трудового кодекса РФ.

5. В случае разглашения персональных данных, ставших известными работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника, трудовой договор с работником может быть расторгнут работодателем (подпункт «в» пункта 6 статьи 81 Трудового кодекса РФ).

Лист ознакомления

с Инструкцией
по обработке персональных данных в

_____,

(наименование образовательного учреждения)

осуществляемой без использования средств автоматизации

№ п/п	Фамилия, имя, отчество работника	Дата ознакомления с Инструкцией	Подпись работника

ЖУРНАЛ УЧЕТА СЪЕМНЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Форма Журнала учета машинных носителей данных

№ п/п	Регистрацион-ный номер/дата	Тип/ёмкость машинного носителя персональных данных	Номер экземпляра/ количество экземпляров	Место установки (использова-ния)/дата установки	Ответственное должностное лицо (ФИО)	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения машинного носителя персональных данных	Сведения об уничтожении машинных носителей персональных данных, стирании информации (подпись, дата)

ЖУРНАЛ УЧЕТА МЕРОПРИЯТИЙ ПО КОНТРОЛЮ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Форма Журнала учета мероприятий по контролю обеспечения защиты персональных данных

№	Дата проведения проверки	№, дата справки по результатам проверки или краткое содержание проверки	ФИО проверяющего	Подпись проверяющего

ЖУРНАЛ УЧЕТА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Форма Журнала учета инцидентов информационной безопасности

№	Дата инцидента	№, дата справки или акта по результатам расследования или краткое содержание инцидента	ФИО проверяющего	Подпись проверяющего

ЖУРНАЛ УЧЕТА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ЖУРНАЛ

учета применяемых средств защиты информации

в системе защиты информации информационной системы персональных данных, обрабатываемых в

_____,

(наименование образовательного учреждения)

расположенном по адресу

_____

(адрес образовательного учреждения)

Дата начала: «___» _____ 20__ г.

Дата окончания: «___» _____ 20__ г.

Хранить: ___ лет

Ответственный за заполнение: _____

_____ 20__ год

(город)

АННОТАЦИЯ

Журнал учета применяемых средств защиты информации содержит перечень средств защиты информации, представленный с регистрационными номерами, отметками о выдаче/получении, а так же об установке и изъятии (уничтожении) средств защиты информации.

Журнал учета применяемых средств защиты информации разработан в соответствии с постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

ПОРЯДОК ЗАПОЛНЕНИЯ ЖУРНАЛА УЧЕТА

1. Журнал учета заполняется шариковой ручкой синего цвета.
2. Не допускается написания более одной строчки текста в строке журнала, т.е. текст переносится на следующую строку журнала.
3. № пункта, номера - необходимо проставлять арабскими цифрами без точки на конце.
4. Наименование средств защиты писать полностью без сокращений.
5. Формат даты: ЧЧ. ММ. ГГ.
6. Для исправления ошибок необходимо перечеркнуть (одной чертой) неправильное написание, вписать правильное и поставить подпись должностного лица организации, заверив ее печатью организации, с указанием даты исправления. Не допускается исправления ошибок с помощью корректирующего средства.

ЖУРНАЛ
учета применяемых средств защиты информации

№ п/п	Регистрационный номер	Наименование	Сведения об установке средства защиты информации			Сведения об изъятии/удалении средства защиты информации			Примечание
			Дата установки	Место установки (использования)	ФИО производившего установку, подпись	Дата изъятия/ удаления	ФИО производившего изъятие/удаление, подпись	Причина изъятия/удаления	

Пронумеровано и прошнуровано
___ (_____) лист__

Директор _____
_____
(наименование
образовательного учреждения)

_____
(ФИО)

М.П.