Управление образования Администрации города Нижний Тагил
Муниципальное бюджетное общеобразовательное учреждение
Средняя общеобразовательная школа № 144

ПРИКАЗ

от 02.09.2019г. № 281

«О внесении изменений в приказы от 24.12.2017г. № 357 «О защите персональных данных»

ПРИКАЗЫВАЮ:

1. Внести изменения в следующие приложения к приказу от 24.12.2017г. № 357 «О защите персональных данных» в связи с исполнением должностных обязанностей другими сотрудниками с 01.09.2019г.:

1.1. Пункт 1.4. приказа от 24.12.2017г. № 357 «О защите персональных данных»: Утвердить перечень должностей, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей согласно **приложению № 1** к настоящему приказу.

1.2. Пункт 2.1. приказа от 24.12.2017г. № 357 «О защите персональных данных»: утвердить состав комиссии по защите информации согласно **приложению № 4** к настоящему приказу.

2. Назначить ответственным за эксплуатацию ИС инженера –программиста - Соколову К.Ю.

Директор МБОУ СОШ № 144 Л.Г. Ловчикова

С приказом ознакомлена: К.Ю. Соколова

Приложение №1 к Приказу № 357 от 24 декабря 2017

ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ, ДОСТУП КОТОРЫХ К ПЕРСОНАЛЬНЫМ ДАННЫМ, В ТОМ ЧИСЛЕ ОБРАБАТЫВАЕМЫМ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. В МБОУ СОШ № 144 к сотрудникам, имеющим доступ к персональным данным для исполнения должностных обязанностей, относятся:

- директор ОУ, Ловчикова Л.Г.
- заместитель директора по УР, Елисеева Л.П.
- заместитель директора по ВР, Фомина О.Л.
- заместитель директора по ПВ, Вилохин Б.А.
- заместитель директора по АХЧ, Гордеева Е.Л.
- секретарь, Иванову С.С.
- специалист по кадрам, Иванову С.С.
- учитель информатики, ответственный за информатизацию, Соколову К.Ю.
- педагог- библиотекарь, Буркова С.В.
- педагог-психолог, Дядюшкина Е.И.
- специалист по охране труда, Дормедонтова Н.А.
- председатель профсоюза, Перевощикова Е.А.
- классные руководители (доступ к персональным данным своего класса)

2. Государственные органы, получающие персональные в виде отчетности

Согласно законодательству Российской Федерации и иным нормативно-правовым актам, МБОУ СОШ № 144 передает персональные данные в виде отчетности в следующие государственные органы:

- Пенсионный Фонд России;
- Федеральная налоговая служба;
- Фонд социального страхования;
- МУ МВД России «Нижнетагильское»
- Управление социальной политики по городу Нижний Тагил и Пригородному району
- ТО ПМПК города Нижний Тагил

Приложение № 4 к Приказу № 357 от 24 декабря 2017

СОСТАВ КОМИССИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Председатель комиссии	Елисеева Л.П., зам.директора по УР
Члены комиссии	Гордеева Е.Л., зам.директора по АХЧ
	Соколова К.Ю., учитель информатики
	Соколова К.Ю., инженер-программист

Приложение №11 к Приказу № 357 от 24 декабря 2017

ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ И ЛИЦ, ОТВЕТСТВЕННЫХ ЗА ВЕДЕНИЕ ЖУРНАЛОВ

№ п/п	НАЗВАНИЕ ЖУРНАЛОВ	ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ	ПЕРЕЧЕНЬ ЛИЦ	РОСПИСЬ
1.	ЖУРНАЛ учета машинных носителей персональных данных (стационарные носители)	Заместитель директора по АХЧ	Гордеева Е.Л.	
2.	ЖУРНАЛ учета машинных носителей персональных данных (съемные носители)	Заместитель директора по АХЧ	Гордеева Е.Л.	
3.	ЖУРНАЛ учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных	Заместитель директора по УР	Елисеева Л.П.	
4.	ЖУРНАЛ учета средств защиты информации	Заместитель директора по АХЧ	Гордеева Е.Л.	
5.	ЖУРНАЛ учета согласий субъектов персональных данных	Секретарь	Иванова С.С.	
6.	ЖУРНАЛ учета хранилищ	Заместитель директора по АХЧ	Гордеева Е.Л.	
7.	ЖУРНАЛ учета ЭП	Заместитель директора по АХЧ	Гордеева Е.Л.	
8.	ЖУРНАЛ учета выдачи паролей	Учитель информатики	Соколова К.Ю.	
9.	ЖУРНАЛ учета обращений субъектов персональных данных по вопросам обработки персональных данных	Секретарь	Иванова С.С.	
10.	ЖУРНАЛ антивирусных проверок информационных систем	Инженер-программист/учитель информатики	Соколова К.Ю.	
11.	ЖУРНАЛ учета выявленных инцидентов информационной безопасности	Инженер-программист/учитель информатики	Соколова К.Ю.	
12.	ЖУРНАЛ учета передачи персональных данных	Секретарь	Иванова С.С.	

13.	ЖУРНАЛ периодического тестирования средств защиты информации	Инженер-программист/учитель информатики	Соколова К.Ю.	
14.	ЖУРНАЛ учета проверок электронных журналов обращений к информационным системам персональных данных	Инженер-программист/учитель информатики	Соколова К.Ю.	
15.	ЖУРНАЛ уничтожения носителей персональных данных	Заместитель директора по УР	Елисеева Л.П.	

Управление образования Администрации города Нижний Тагил
Муниципальное бюджетное общеобразовательное учреждение
Средняя общеобразовательная школа № 144

ПРИКАЗ

от 24.12.2017г. № 357

«О защите персональных данных»

В соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных, Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

ПРИКАЗЫВАЮ:

3. Возложить обязанности по защите информации:

3.1. Назначить ответственным за организацию обработки персональных данных: заместителя директора по УР Елисееву Л.П., заместителя директора во ВР Фомину О.Л., заместителя директора по ПВ Вилохин Б.А.

3.2. Назначить ответственными за обеспечение безопасности персональных данных в информационных системах персональных данных заместителя директора по УР Елисееву Л.П., специалиста по кадрам Иванову С.С., заместителя директора по АХЧ Гордееву Е.Л.

3.3. Назначить ответственным за эксплуатацию ИС инженера –программиста Хабибуллина Р.

3.4. Утвердить перечень должностей, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей согласно приложению 1 к настоящему приказу.

3.5. Утвердить перечень должностей, ведущих обработку персональных данных без использования средств автоматизации согласно приложению 2 к настоящему приказу.

3.6. Утвердить перечень лиц, ответственных за обезличивание персональных данных согласно приложению 3 к настоящему приказу.

4. Создать комиссию по защите информации:

4.1. Утвердить состав комиссии по защите информации согласно приложению 4 к настоящему приказу.

4.2. Утвердить положение о комиссии по защите информации согласно приложению 5 к настоящему приказу.

5. Утвердить типовые формы документов по защите информации:

5.1. Согласие на обработку персональных данных согласно приложениям 6,7 к настоящему приказу.

5.2. Разъяснение субъекту персональных данных согласно приложению 8 к настоящему приказу.

5.3. Обязательство о неразглашении информации, содержащей персональные данные, согласно приложению 9 к настоящему приказу.

5.4. Журналы по защите информации согласно приложению 10 к настоящему приказу.

5.5. Перечень должностей и лиц, ответственных за ведение журналов согласно приложению 11 к настоящему приказу.

5.6. Протокол заседания комиссии по защите информации согласно приложению 12 к настоящему приказу.

5.7. Акт определения уровня защищенности ПДн при их обработке в ИСПДн и класса защищенности ИС согласно приложению 13 к настоящему приказу.

5.8. Акт об уничтожении персональных данных субъектов персональных данных согласно приложению 14 к настоящему приказу.

6. Утвердить перечень информационных систем персональных данных согласно приложению 15 к настоящему приказу.

7. Утвердить перечень обрабатываемых персональных данных согласно приложению 16 к настоящему приказу.

8. Утвердить перечень помещений для обработки персональных данных в МБОУ СОШ №144 согласно приложению 17 к настоящему приказу.

9. Утвердить политику в отношении обработки персональных данных согласно приложению 18.

10. Утвердить инструкции и правила по защите информации:

– Инструкцию ответственного за организацию обработки персональных данных согласно приложению 19 к настоящему приказу.

– Правила рассмотрения запросов субъектов персональных данных согласно приложению 20 к настоящему приказу.

– Правила работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей, согласно приложению 21 к настоящему приказу;

– Инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных согласно приложению 22 к настоящему приказу;

– Инструкцию по организации резервного копирования, согласно приложению 23 к настоящему приказу;

– Инструкцию по организации парольной защиты, согласно приложению 24 к настоящему приказу;

– Инструкцию по организации антивирусной защиты, согласно приложению 25 к настоящему приказу;

– Инструкцию по проверке электронного журнала обращений к информационной системе персональных данных, согласно приложению 26 к настоящему приказу;

– Порядок уничтожения персональных данных при достижении целей обработки и (или) при наступлении законных оснований, согласно приложению 27 к настоящему приказу;

– Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, согласно приложению 28 к настоящему приказу;

– Инструкцию по обращению с криптосредствами согласно приложению 29 к настоящему приказу;

– Инструкцию по обработке персональных данных без использования средств автоматизации согласно приложению 30 к настоящему приказу;

– Правила работы с обезличенными данными согласно приложению 31 к настоящему приказу;

– Инструкцию по работе с инцидентами информационной безопасности согласно приложению 32 к настоящему приказу;

– Инструкцию ответственного за эксплуатацию информационных систем персональных данных согласно приложению 33 к настоящему приказу.

11. Утвердить план мероприятий по защите информации согласно приложению 34 к настоящему приказу.

Директор МБОУ СОШ № 144 Л.Г. Ловчикова

С приказом ознакомлены:

Л.П. Елисеева
О.Л. Фомина
Б.А. Вилохин
Е.Л. Гордеева
С.С. Полянская
С.В. Бобкин
С.В. Буркова
Е.И. Дядюшкина
И.Ю. Петрухина
Е.А. Перевощикова

классные руководители:

1а -Линник Ирина Николаевна
1б-Филиппова Ксения Леонидовна
2а-Козина Любовь Леонидовна
2б-Перевощикова Елена Александровна
3а-Петрухина Ирина Юрьевна
3б-Кротова Наталья Викторовна
3в-Иванова Марина Сергеевна
4а-Тютина Татьяна Владимировна
5а-Головина Ирина Владимировна
5б-Демченко Екатерина Александровна
6а-Гибадулина Лариса Викторовна
6б-Трушкова Светлана Николаевна
7а- Сидельникова Оксана Владимировна
7б-Головина Ирина Владимировна
8а-Дядюшкина Елена Ивановна
8б-Волкова Ольга Михайловна
8в-Казанцева Ольга Владимировна
9а-Пестрецова Светлана Владимировна
9б-Хащенко Галина Анатольевна
10а-Ларионова Светлана Владимировна
11а-Святченко Елена Александровна

Приложение №1 к Приказу № 357 от 24 декабря 2017

ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ, ДОСТУП КОТОРЫХ К ПЕРСОНАЛЬНЫМ ДАННЫМ, В ТОМ ЧИСЛЕ ОБРАБАТЫВАЕМЫМ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

3. **В МБОУ СОШ № 144 к сотрудникам, имеющим доступ к персональным данным для исполнения должностных обязанностей, относятся:**

- директор ОУ, Ловчикова Л.Г.
- заместитель директора по УР, Елисеева Л.П.
- заместитель директора по ВР, Фомина О.Л.
- заместитель директора по ПВ, Вилохин Б.А.
- заместитель директора по АХЧ, Гордеева Е.Л.
- секретарь, Полянская С.С.
- специалист по кадрам, Полянская С.С.
- учитель информатики, ответственный за информатизацию, Бобкин С.В.
- педагог- библиотекарь, Буркова С.В.
- педагог-психолог, Дядюшкина Е.И.
- инженер по ОТ, Петрухина И.Ю.
- председатель профсоюза, Перевощикова Е.А.
- классные руководители (доступ к персональным данным своего класса)

4. **Государственные органы, получающие персональные в виде отчетности**

Согласно законодательству Российской Федерации и иным нормативно-правовым актам, МБОУ СОШ № 144 передает персональные данные в виде отчетности в следующие государственные органы:

- Пенсионный Фонд России;
- Федеральная налоговая служба;
- Фонд социального страхования;
- МУ МВД России «Нижнетагильское»
- Управление социальной политики по городу Нижний Тагил и Пригородному району
- ТО ПМПК города Нижний Тагил

Приложение №2 к Приказу № 357 от 24 декабря 2017

ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ, ВЕДУЩИХ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

- директор ОУ, Ловчикова Л.Г.
- заместитель директора по УР, Елисеева Л.П.
- заместитель директора по ВР, Фомина О.Л.
- заместитель директора по ПВ, Вилохин Б.А.
- заместитель директора по АХЧ, Гордеева Е.Л.
- секретарь, Полянская С.С.
- специалист по кадрам, Полянская С.С.
- инженер по ОТ, Петрухина И.Ю.

Приложение №3 к Приказу № 357 от 24 декабря 2017

ПЕРЕЧЕНЬ ЛИЦ, ОТВЕТСТВЕННЫХ ЗА

ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

ДОЛЖНОСТЬ	Ф.И.О.
Директор	Ловчикова Л.Г.
Секретарь	Полянская С.С.
Специалист по кадрам	Полянская С.С.
Заместитель директора по УР	Елисеева Л.П.
Заместитель директора по АХЧ	Гордеева Е.Л.

Приложение №4 к Приказу № 357 от 24 декабря 2017

СОСТАВ КОМИССИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Председатель комиссии	Елисеева Л.П., зам.директора по УР
Члены комиссии	Гордеева Е.Л., зам.директора по АХЧ
	Бобкин С.В., учитель информатики
	Хабибуллин Р.Б., инженер-программист

Приложение №5 к Приказу № 357 от 24 декабря 2017

ПОЛОЖЕНИЕ
О КОМИССИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

1. Общие положения

1.1. Настоящее Положение определяет основные задачи, порядок формирования, полномочия и ответственность комиссии.

2. Основные задачи комиссии

2.1. Основными задачами комиссии являются:

2.1.1. Сбор и анализ исходных данных по информационным системам персональных данных МБОУ СОШ № 144.

2.1.2. Определение значений параметров для проведения классификации информационных систем в соответствии с Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2.1.3. Определение значений параметров для установления уровня защищенности персональных данных 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».

2.1.4. Определение класса защищенности информационных систем персональных данных МБОУ СОШ № 144 на основании собранных данных.

2.1.5. Определение уровня защищенности персональных данных при их обработке в информационных системах персональных данных.

3. Порядок формирования комиссии

3.1. Комиссия формируется из числа штатных сотрудников МБОУ СОШ № 144, участвующих в процессе обработки персональных данных.

3.2. В состав Комиссии входит не менее четырех человек – членов Комиссии, в их числе – председатель Комиссии.

3.3. Члены комиссии назначаются приказом директора МБОУ СОШ № 144

3.4. В случае изменения состава Комиссии, в приказ вносятся соответствующие изменения.

4. Полномочия комиссии

4.1. Для осуществления задач, указанных в разделе 2 настоящего Положения, Комиссия имеет право:

4.1.1. Получать необходимые сведения у всех работников МБОУ СОШ № 144, участвующих в обработке персональных данных.

4.1.2. Просматривать электронные базы данных и бумажные носители, содержащие персональные данные, с целью выявления состава обрабатываемых персональных данных.

4.1.3. Отслеживать технологический процесс обработки персональных данных.

4.1.4. Выявлять или получать готовые сведения о структуре локальной вычислительной сети МБОУ СОШ № 144.

4.1.5. Определять или получать готовые сведения о наличии и способах доступа к сетям общего пользования.

4.1.6. Определять или получать готовые сведения о технических и программных средствах обработки персональных данных.

4.1.7. Определять или получать готовые сведения об условиях, местах и способах передачи персональных данных в сторонние организации.

5. Отчетность комиссии

5.1. Комиссия при выполнении своих задач должна составить протокол заседания комиссии.

5.2. В результате своей деятельности Комиссия должна составить Акт(ы) определения уровня защищенности персональных данных и класса защищенности информационных систем персональных данных.

Приложение №6 к Приказу от 24 декабря 2017

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА

Я,

_____

(Ф.И.О. полностью)

зарегистрированный(-ая) по адресу: _____

_____,

(индекс и адрес регистрации согласно паспорту)

паспорт серии _____№_____ выдан_____

_____,

являясь работником МБОУ СОШ № 144 (далее – Оператор), находящегося по адресу: город Нижний Тагил ул. Гвардейская,72, своей волей и в своем интересе выражаю согласие на обработку моих персональных данных Оператором в целях информационного обеспечения для формирования общедоступных источников персональных данных (справочников, адресных книг, информации в СМИ и на сайте организации т.д.), включая выполнение действия по сбору, систематизации, накоплению, хранению, уточнению (обновлению, изменению), распространению (в том числе передаче) и уничтожению моих персональных данных, входящих в следующий перечень общедоступных сведений:

1. Фамилия, имя, отчество.
2. Рабочий номер телефона и адрес электронной почты.
3. Сведения о профессии, должности, образовании.
4. Иные сведения, специально предоставленные мной для размещения в общедоступных источниках персональных данных.

Для целей обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, оформления доверенностей, прохождении конкурсного отбора, безналичных платежей на мой счет, выражаю согласие на получение и передачу моих персональных данных путем подачи и получения запросов в отношении органов местного самоуправления, государственных органов и организаций (для этих целей дополнительно к общедоступным сведениям могут быть получены или переданы сведения о дате рождения, гражданстве, доходах, паспортных данных, предыдущих местах работы, идентификационном номере налогоплательщика, свидетельстве государственного пенсионного страхования, допуске к сведениям, составляющим государственную тайну, социальных льготах и выплатах, на которые я имею право в соответствии с действующим законодательством).

Вышеприведенное согласие на обработку моих персональных данных представлено с учетом п. 2 ст. 6 и п. 2 ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в соответствии с которыми обработка персональных данных, осуществляемая на основе федерального закона либо для исполнения договора, стороной в котором я являюсь, может осуществляться Оператором без моего дополнительного согласия.

Настоящее согласие вступает в силу с момента его подписания на срок действия трудового договора с Оператором и может быть отозвано путем подачи Оператору письменного заявления.

«____»_____20__г. _____

(подпись и фамилия, имя, отчество прописью полностью)

Приложение №7 к Приказу № 357 от 24 декабря 2017

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ РОДИТЕЛЕЙ И ИХ ДЕТЕЙ
(при подачи заявления о приеме в школу)

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» даю своё согласие на обработку моих и моего ребёнка персональных данных, указанных в заявлении, а также их передачу в электронной форме по открытым каналам связи сети Интернет в государственные и муниципальные органы и долгосрочное использование в целях предоставления образовательной услуги согласно действующего законодательства. Настоящее согласие может быть отозвано мной в письменной форме и действует до даты подачи мной заявления об отзыве. С порядком подачи заявления в электронном виде ознакомлен(а).

_____ _____
(ФИО заявителя) (подпись заявителя)

Приложение №8 к Приказу № 357 от 24 декабря 2017

РАЗЪЯСНЕНИЕ
СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Мне, _____
разъяснены юридические последствия отказа предоставить свои персональные данные в МБОУ СОШ № 144.

В соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152 ФЗ «О персональных данных», определен перечень персональных данных, которые субъект персональных данных обязан предоставить в МБОУ СОШ № 144 в связи с поступлением на работу/ поступлением моего ребёнка в школу.

Без представления субъектом персональных данных обязательных /для заключения трудового договора сведений, трудовой договор не может быть заключен/ для подачи заявления в школу, ребёнок не может быть зачислен в школу .

_____ _____ _____
дата подпись расшифровка

Приложение №9 к Приказу № 357 от 24 декабря 2017

ОБЯЗАТЕЛЬСТВО

О НЕРАЗГЛАШЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____ , паспорт
серии _____ номер _____, выдан _____
"___" _____ 20_____ года

понимаю, что получаю доступ к персональным данным работников/учащихся МБОУ СОШ № 144. Я также понимаю, что во время исполнения своих обязанностей я занимаюсь сбором, обработкой и хранением персональных данных.

Я понимаю, что разглашение такого рода информации может нанести ущерб работникам и учащимся организации, как прямой, так и косвенный.В связи с этим даю обязательство при работе (сборе, обработке и хранении) с персональными данными с соблюдать все описанные в Положении об обработке персональных данных в МБОУ СОШ № 144 требования.
Я подтверждаю, что не имею права разглашать сведения о (об):
- анкетных и биографических данных;
- образовании;
- трудовом и общем стаже;
- составе семьи;
- паспортных данных;
- воинском учете;
- заработной плате работника;
- социальных льготах;
- специальности;
- занимаемой должности;
- наличии судимостей;
- адресе места жительства, домашнем телефоне;
- месте работы или учебы членов семьи и родственников;
- содержании трудового договора;
- составе декларируемых сведений о наличии материальных ценностей;
- содержании декларации, подаваемой в налоговую инспекцию;
- подлинниках и копиях приказов по личному составу;
-личных делах учащихся;
- личных делах сотрудников и трудовых книжках сотрудников;
- делах, содержащих материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копиях отчетов, направляемых в органы статистики.
Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных работника, учащегося, или их утраты я несу ответственность в соответствии с ст. 90 ТК РФ.С Положении об обработке персональных данных в МБОУ СОШ № 144 ознакомлен(а).

Ф.И.О._____ Должность _____
Подпись: _____ Дата: _____

Приложение №10 к Приказу № 357 от 24 декабря 2017

ЖУРНАЛ
учета машинных носителей персональных данных (стационарные носители)

№ п/п	Регистрационный номер	Тип и ёмкость	Дата и место установки (использования)	Ответственное должностное лицо (Ф.И.О)

ЖУРНАЛ
учета машинных носителей персональных данных (съемные носители)

№ п/п	Регистрационный номер	Тип и ёмкость	Получил (Ф.И.О, дата, подпись)	Сдал (Ф.И.О, дата, подпись)	Место хранения	Ответственное должностное лицо (Ф.И.О)

ЖУРНАЛ
учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных

№ п/п	Сведения о допуске к персональным данным				Сведения о прекращении допуска к персональным данным	
	Наименование информационной системы персональных данных/способ обработки ПДн	ФИО, должность получившего допуск	Дата и номер приказа о допуске	Дата и подпись допускаемого лица	Дата и номер приказа о прекращении допуска	Номер приказа об увольнении или дата и подпись лица об ознакомлении с документом, прекращающим допуск к ПДн

ЖУРНАЛ
учета средств защиты информации

№ п/п	Индекс и наименование средства защиты информации	Серийный (заводской) номер	Номер специального защитного знака	Наименование организации, установившей СЗИ	Место установки	Примечание

ЖУРНАЛ
учета согласий субъектов персональных данных

№ п/п	Дата и номер согласия	Ф.И.О. субъекта персональных данных

ЖУРНАЛ
учета хранилищ

№ п/п	Регистрационный (учетный) номер хранилища	Вид хранилища	Дата постановки на учет	Фамилия и подпись принявшего (ответственного), дата	Место расположения (номер помещения)	Дата и номер акта о выводе из эксплуатаци	Примечание

ЖУРНАЛ
учета ЭП

№ п/п	Номера экземпляров ключевых документов	Номера криптографических ключей	Наименование СКЗИ	Отметка о получении		Отметка о выдаче		
				От кого получены (УУЦ)	Дата	ФИО пользователя	Дата	Подпись

ЖУРНАЛ
учета выдачи паролей

№ п/п	Дата получения пароля	Ф.И.О. получателя	Подпись получателя

ЖУРНАЛ
учета обращений субъектов персональных данных по вопросам обработки персональных данных

№ п/п	Дата обращения	ФИО обратившегося	Цель обращения	Отметка о предоставлении информации или отказе в ее предоставлении / дата предоставления или отказа в предоставлении информации	Подпись ответственного	Примечание

ЖУРНАЛ
антивирусных проверок информационных систем

№ п/п	Дата и время проверки	Наименование ИСПДн (составной части ИСПДн)	Какими средствами проводилась проверка	Результаты проверки		Наименование инфицированных файлов, источника поступления (носитель, организация)	Примечание (принятые меры)	Фамилия и подпись лица, проводившего проверку
				кол-во проверенных файлов	кол-во инфицированных файлов			

ЖУРНАЛ
учета выявленных инцидентов информационной безопасности

№ п/п	Дата и время	Описание инцидента	Ответственный за реагирование на инцидент	Отметка об устранении инцидента	Дата устранения инцидента	Подпись ответственного лица	Примечание

ЖУРНАЛ
учета передачи персональных данных

№ п/п	Сведения о запрашивающем лице	Состав запрашиваемых персональных данных	Цель получения персональных данных	Отметка о передаче или отказе в передаче персональных данных	Дата передачи/отказа в передаче персональных данных	Подпись запрашивающего лица

ЖУРНАЛ
периодического тестирования средств защиты информации

№ п/п	Наименование средства защиты информации от НСД или криптосредства	Регистрационные номера СЗИ от НСД или криптосредства	Дата тестирования	Фамилия и подпись ответсвенного пользователя, проводившего тестирование	Наименование теста, используемые средства для проведения теста	Результат тестирования (успешный/неуспешный), комментарий	Дата очередного тестирования

ЖУРНАЛ
учета проверок электронных журналов обращений к информационным системам персональных данных

№ п/п	Дата проверки	Наименование ИСПДн, компьютера, технического средства	Наименование проверяемого журнала	Выявленные нарушения требований безопасности, нештатные ситуации	Подпись администратора безопасности	Примечание

ЖУРНАЛ
уничтожения носителей персональных данных

№ п/п	Наименование ИСПДн, в которой уничтожаются персональные данные	Ф.И.О. субъекта, персональные данные которого подлежат уничтожению	Обоснование уничтожения	Наименование файла, и его месторасположение	Дата уничтожения	Ф.И.О. и подпись Исполнителя	Ф.И.О. и подпись ответственного за обработку персональных данных

Приложение №11 к Приказу № 357 от 24 декабря 2017

ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ И ЛИЦ, ОТВЕТСТВЕННЫХ ЗА ВЕДЕНИЕ ЖУРНАЛОВ

№п/п	НАЗВАНИЕ ЖУРНАЛОВ	ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ	ПЕРЕЧЕНЬ ЛИЦ	РОСПИСЬ
	ЖУРНАЛ учета машинных носителей персональных данных (стационарные носители)	Заместитель директора по АХЧ	Гордеева Е.Л.	
	ЖУРНАЛ учета машинных носителей персональных данных (съемные носители)	Заместитель директора по АХЧ	Гордеева Е.Л.	
	ЖУРНАЛ учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных	Заместитель директора по УР	Елисеева Л.П.	
	ЖУРНАЛ учета средств защиты информации	Заместитель директора по АХЧ	Гордеева Е.Л.	
	ЖУРНАЛ учета согласий субъектов персональных данных	Секретарь	Полянская С.С.	
	ЖУРНАЛ учета хранилищ	Заместитель директора по АХЧ	Гордеева Е.Л.	
	ЖУРНАЛ учета ЭП	Заместитель директора по АХЧ	Гордеева Е.Л.	
	ЖУРНАЛ учета выдачи паролей	Учитель информатики	Бобкин С.В.	
	ЖУРНАЛ учета обращений субъектов персональных данных по вопросам обработки персональных данных	Секретарь	Полянская С.С.	
	ЖУРНАЛ антивирусных проверок информационных систем	Инженер-программист/учитель информатики	Хабибулин Р.Б.	
	ЖУРНАЛ учета выявленных инцидентов информационной безопасности	Инженер-программист/учитель информатики	Хабибулин Р.Б.	
	ЖУРНАЛ учета передачи персональных данных	Секретарь	Полянская С.С.	
	ЖУРНАЛ периодического тестирования средств защиты информации	Инженер-программист/учитель информатики	Хабибулин Р.Б.	
	ЖУРНАЛ учета проверок электронных журналов обращений к информационным системам персональных данных	Инженер-программист/учитель информатики	Хабибулин Р.Б.	

	ЖУРНАЛ уничтожения носителей персональных данных	Заместитель директора по УР	Елисеева Л.П.	

Приложение №12 к Приказу № 357 от 24 декабря 2017

ПРОТОКОЛ № 1
ЗАСЕДАНИЯ КОМИССИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Дата и время проведения _____

Место проведения _____

Председатель комиссии _____ ФИО

Члены комиссии _____ ФИО

_____ ФИО

_____ ФИО

Повестка дня

Определение информационных систем персональных данных (далее - ИСПДн), принадлежащих МБОУ СОШ № 144.

1. Слушали: _____ доложил(а) исходные данные об ИСПДн МБОУ СОШ № 144.

Выступил(а): _____ предложил(а) утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПДн МБОУ СОШ № 144.

Постановили:

Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС МБОУ СОШ № 144.

2. Слушали: _____ доложил(а) исходные данные об ИСПДн МБОУ СОШ № 144

Выступил(а): _____ предложил(а) утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПДн МБОУ СОШ № 144.

Постановили:

Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС МБОУ СОШ № 144.

Председатель комиссии _____ ФИО

Члены комиссии _____ ФИО

_____ ФИО

_____ ФИО

Приложение №13 к Приказу № 357 от 24 декабря 2017

АКТ
ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ ПДН ПРИ ИХ ОБРАБОТКЕ В ИСПДН МБОУ СОШ № 144 И КЛАССА ЗАЩИЩЕННОСТИ ИС МБОУ СОШ № 144

Председатель комиссии _____ ФИО
Члены комиссии _____ ФИО
_____ ФИО
_____ ФИО

Рассмотрев исходные данные об информационной системе персональных данных (далее - ИСПДн), комиссия определила:

– Категории персональных данных обрабатываемых в ИСПДн: в информационной системе обрабатываются специальные категории персональных данных;

– Категории субъектов: персональные данные субъектов персональных данных, не являющихся сотрудниками оператора;

– Объем обрабатываемых персональных данных: менее 100 000;

– Тип актуальных угроз: для информационной системы актуальны угрозы 3-го типа;

– Уровень значимости информации: информация имеет низкий уровень значимости УЗ 3;

– Масштаб информационной системы: информационная система имеет объектовый масштаб.

Комиссия решила, в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а так же в соответствии с приказом ФСТЭК Российской Федерации от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и на основании анализа исходных данных, необходимо обеспечить третий уровень защищенности (УЗ 3) персональных данных и установить третий класс защищенности информационной системы (К3).

Результат оценки вреда:

Для информационной системы актуальны угрозы 3-го типа.

Уровень значимости информации определен степенью возможного ущерба для обладателя информации от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации, руководствуясь следующей формулой:

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)], где степень возможного ущерба определяется обладателем информации.

Комиссия утвердила следующее:

УЗ = [(конфиденциальность, низкая степень ущерба) (целостность, низкая степень ущерба) (доступность, низкая степень ущерба)] – таким образом, комиссия установила низкий уровень значимости (УЗ 3) (возможны незначительные негативные последствия).

Председатель комиссии	_____	ФИО
Члены комиссии	_____	ФИО
	_____	ФИО
	_____	ФИО

«__»_____20__ г.

Приложение №14 к Приказу № 357 от 24 декабря 2017

АКТ
ОБ УНИЧТОЖЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Комиссия в составе:

Роль	ФИО	Должность
Председатель		
Члены комиссии		

Установила, что на основании достижения цели обработки персональных данных, в соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных» гл. 2, ст. 5, пункт 7, подлежат уничтожению сведения, составляющие персональные данные:

№ п/п	Сведения, содержащие персональные данные	Место хранения	Кол-во ед. хранения	Примечание

Указанные персональные данные уничтожены путем_____
_____
(удаления с помощью средств гарантированного удаления информации, уничтожения носителя и т.п.)

Председатель комиссии:

_____ _____
подпись расшифровка

Члены комиссии:

_____ _____
подпись расшифровка

_____ _____
подпись расшифровка

Приложение №15 к Приказу № 357 от 24 декабря 2017

ПЕРЕЧЕНЬ
ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ,
ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ МБОУ СОШ № 144

№ п/п	Содержание сведений	Подразделения, использующие в работе персональные данные
1	Информация, необходимая для внесения в региональную информационную систему данных участников государственной итоговой аттестации	МБОУ СОШ № 144
2	Информация, необходимая для внесения в региональную информационную систему данных педагогических работников образовательной организации для прохождения ими курсовой подготовки	МБОУ СОШ № 144
3	Информация, необходимая для внесения в информационные системы «Е-Услуги. Образование», «Сетевой город. Образование», на сайт ОУ данных обучающихся, их родителей (законных представителей) и педагогических работников	МБОУ СОШ № 144

Приложение №16 к Приказу № 357 от 24 декабря 2017

ПЕРЕЧЕНЬ
ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В МБОУ СОШ № 144
В СВЯЗИ С ОСУЩЕСТВЛЕНИЕМ СВОЕЙ ДЕЯТЕЛЬНОСТИ В СООТВЕТСТВИИ
С ПРЕДМЕТОМ И ЦЕЛЯМИ ДЕЯТЕЛЬНОСТИ
ПУТЕМ ВЫПОЛНЕНИЯ РАБОТ, ОКАЗАНИЯ УСЛУГ В СФЕРЕ ОБРАЗОВАНИЯ

Раздел I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящий Перечень персональных данных и иных объектов, подлежащих защите (далее по тексту - Перечень) МБОУ СОШ № 144 (далее - ОО) разработан в соответствии с результатами анализа. Перечень содержит полный список категорий персональных.

2. Сведениями, составляющими персональные данные, в ОО является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных):

- персональные данные работников;
- персональные данные родителей (законных представителей);
- персональные данные учащихся.

Раздел II. ОБРАБАТЫВАЕМАЯ ИНФОРМАЦИЯ

Статья 1. Персональные данные работников

1. Состав персональных данных

1.1. Персональные данные работников ОО включают:

- фамилия, имя, отчество ;
- фамилия при рождении (либо другие фамилии, если они были);
- день, месяц, год и место рождения;
- паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ);
- гражданство;
- адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания;
- номера телефонов (мобильного и домашнего), в случае их регистрации на субъекта персональных данных или по адресу его места жительства;
- сведения об образовании, квалификации и о наличии специальных знаний или

специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, ученая степень, ученое звание, владение иностранными языками и другие сведения);

- сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, квалификация и специальность по окончании образовательного учреждения и другие сведения;
- сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, наименования, адреса и телефона работодателя, а также реквизитов других организаций с полным наименование занимаемых ранее в них должностей и времени работы в этих организациях, а также другие сведения;
- данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);
- ведения о знании иностранного языка (наименование и степень знания);
- ведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней;
- содержание гражданско-правового договора с гражданином;
- сведения о заработной плате (номера счетов для расчета с работниками, в том числе номера их банковских карточек);
- сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, данные о принятии\снятии на(с) учет(а) и другие сведения);
- сведения о семейном положении (состояние в браке, данные свидетельства о заключении брака, фамилия, имя, отчество супруга(и));
- сведения о номере и серии страхового свидетельства государственного пенсионного

страхования ;
- сведения об идентификационном номере налогоплательщика;
- сведения из страховых полисов обязательного (добровольного) медицинского страхования (в том числе данные соответствующих карточек медицинского страхования)
- Сведения, указанные в оригиналах и копиях приказов по персоналу ОО и материалах к ним, в том числе информация об отпусках, о командировках и т.п.;
- копии приказов, изданных в ОО, и относящиеся к субъекту персональных данных;
- сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях (в том числе наименование или название награды, звания или поощрения, дата и вид нормативного акта о награждении или дата поощрения) работников ОО;
- материалы по аттестации и оценке работников ОО;
- материалы по внутренним служебным расследованиям в отношении работников ОО; - сведения о временной нетрудоспособности работников ОО;
- табельный номер работника ОО;
- сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и другие сведения);
- состояние здоровья работников ОО;
- сведения из ОМВД о наличии/отсутствии судимости;
- фотографическое изображение;
- адрес электронной почты;
- иная необходимая информация, которую граждане добровольно сообщают о себе для получения услуг предоставляемых ОО, если ее обработка не запрещена законом.
1.2. Персональные данные работников, отнесенные ФЗ «О персональных данных» к категории биометрических или специальных, в том числе данные, касающихся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, интимной жизни, не обрабатываются.
2. Цели обработки персональных данных работников
Целью обработки указанных выше персональных данных работников является:
- выполнение уставных задач ОО, в соответствии с Уставом, исполнение обязанностей, возложенных на ОО федеральным законодательством, регламентирующим сферу обработки персональных данных;
- организация учета работников ОО для обеспечения соблюдения их законных прав, и исполнения обязанностей, установленных Трудовым кодексом Российской Федерации,

Налоговым кодексом Российской Федерации и иными нормативно-правовыми актами, а также Уставом и внутренними локальными нормативными актами ОО.

3. Сроки обработки и уничтожения персональных данных работников

Сроки обработки указанных выше персональных данных работников определяются в соответствие со сроком действия Трудового договора с субъектом ПДн, нормативов, установленных приказами Росархива, сроками исковой давности, а также иными требованиями законодательства и нормативными документами.

Персональные данные работников ОО, содержащиеся на электронных носителях, уничтожаются в течение тридцати дней со дня окончания претензионного срока по индивидуальным трудовым спорам, установленного ст.392 Трудового кодекса РФ, по причине достижения ОО цели обработки персональных данных этого Работника и на основании п.4.ст.21. Федерального закона «О персональных данных».

Статья 2. Персональные данные родителей (законных представителей)

1. Состав персональных данных

1.1. Персональные данные родителей (законных представителей) включают:

- фамилия, имя, отчество;
- паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ);
- гражданство;
- домашний и контактный (мобильный) телефоны;
- место работы и жительства;
- данные о составе семьи;
- сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и другие сведения);
- сведения о номере и серии страхового свидетельства государственного пенсионного страхования;
- данные документа об установлении опеки, попечительства, усыновлении ребенка (при наличии);
- фотографическое изображение;
- адрес электронной почты;
- иная необходимая информация, которую граждане добровольно сообщают о себе для получения услуг предоставляемых ОО, если ее обработка не запрещена законом.

1.2. Персональные данные родителей (законных представителей), отнесенные ФЗ «О

персональных данных» к категории биометрических или специальных, в том числе данные, касающихся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни, не обрабатываются.

2.Цели обработки персональных данных родителей (законных представителей)

Целью обработки указанных выше персональных данных родителей (законных представителей) является выполнение уставных задач ОО в соответствии с Уставом, исполнение требований, возложенных на ОО федеральным законодательством, регламентирующим сферу обработки персональных данных, исполнение обязанностей, возложенных на ОО федеральным законодательством, и исполнение договорных обязательств перед субъектом персональных данных.

3. Сроки обработки персональных данных родителей (законных представителей)

3.1. Сроки обработки указанных выше персональных данных родителей (законных представителей) определяются в соответствие со сроком Договора реализации образовательных программ субъектом ПДн, нормативов, установленных приказами Росархива, сроками исковой давности, а также иными требованиями законодательства и нормативными документами.

3.2. Персональные данные родителей (законных представителей), содержащиеся на электронных носителях, уничтожаются в течение тридцати дней со дня окончания претензионного срока обращения клиента с жалобой на качество предоставленных ему образовательных услуг.

Статья 3. Персональные данные учащихся.

1. Состав персональных данных

1.1. Персональные данные учащихся ОО включают:

- фамилия, имя, отчество;
- фамилия при рождении (либо другие фамилии, если они были);
- день, месяц, год и место рождения;
- паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ);
- гражданство;
- адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания;
- данные о составе семьи;
- сведения из страховых полисов обязательного (добровольного) медицинского

страхования (в том числе данные соответствующих карточек медицинского страхования);
- состояние здоровья учащихся ОО;
- сведения о временной нетрудоспособности учащихся ОО;
- сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и другие сведения);
- сведения о номере и серии страхового свидетельства государственного пенсионного страхования;
- форму обучения;
- класс(группа);
- результаты успеваемости и тестирования;
- сведения о внеурочной занятости;
- о правонарушениях;
- сведения промежуточной и итоговой аттестации;
- другие сведения хранящиеся в личном деле;
- фотографическое изображение;
- адрес электронной почты;
- иная необходимая информация, которую обучающиеся добровольно сообщают о себе для получения услуг предоставляемых ОО, если ее обработка не запрещена законом.

2. Цели обработки персональных данных учащихся

Целью обработки указанных выше персональных данных учащихся является выполнение уставных задач ОО, в соответствии с Уставом, исполнение требований, возложенных на ОО федеральным законодательством, регламентирующим сферу обработки персональных данных, исполнение обязанностей, возложенных на ОО федеральным законодательством, и исполнение договорных обязательств перед субъектом персональных данных.

3. Сроки обработки персональных данных учащихся

3.1.Сроки обработки указанных выше персональных данных учащихся определяются в соответствие со сроком Договора реализации образовательных программ с субъектом ПДн, нормативов, установленных приказами Росархива, сроками исковой давности, а также иными требованиями законодательства и нормативными документами.

3.2. Персональные данные учащихся ОО, содержащиеся на электронных носителях, уничтожаются в течение тридцати дней со дня окончания претензионного срока обращения клиента с жалобой на качество предоставленных ему образовательных услуг.

Приложение №17 к Приказу № 357 от 24 декабря 2017

ПЕРЕЧЕНЬ
ПОМЕЩЕНИЙ ДЛЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В МБОУ СОШ № 144

№ п/п	Перечень должностей, имеющих доступ к ПД	Помещения для обработки ПД
1.	директор ОУ	кабинет директора
2.	заместитель директора по УР	кабинет зам. директора по УР
3.	заместитель директора по ВР	кабинет зам. директора по ВР
4.	заместитель директора по ПВ	кабинет зам. директора по ПВ
5.	заместитель директора по АХЧ	кабинет зам. директора по АХЧ
6.	секретарь	кабинет директора
7.	учитель информатики, ответственный за информатизацию	кабинет зам. директора по УР
8.	педагог- библиотекарь	библиотека
9.	инженер по ОТ	кабинет инженера по ОТ
10.	председатель профсоюза	кабинет № 27
11.	классные руководители (доступ к персональным данным своего класса)	кабинеты классных руководителей

Приложение №18 к Приказу № 357 от 24 декабря 2017

ПОЛИТИКА
В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Политика в отношении обработки персональных данных в МБОУ СОШ № 144 (далее – Политика) разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»), Конституцией Российской Федерации, Трудовым кодексом Российской Федерации.

1.2. Политика определяет порядок и условия обработки персональных данных в МБОУ СОШ № 144 (далее – Оператор) с использованием средств автоматизации и без использования таких средств.

1.3. Обработка персональных данных осуществляется в целях приема и регистрации обращений (или запросов) граждан, организаций и общественных объединений, поступивших в администрацию МБОУ СОШ № 144, обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

2. Основные понятия, используемые в настоящей Политике

2.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

2.2. 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.

2.3. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

2.4. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.5. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.6. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.7. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в

информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

2.8. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.9. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.10. Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3. Принципы обработки персональных данных

3.1. Обработка персональных данных осуществляется на законной основе.

3.2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.4. Обработке подлежат только те персональные данные, которые отвечают целям их обработки.

3.5. Содержание и объем персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточным по отношению к заявленным целям обработки.

3.6. При обработке персональных данных обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператором обеспечивается принятие необходимых мер по удалению или уточнению неполных или неточных данных.

3.7. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4. Условия обработки персональных данных

4.1. Обработка персональных данных осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом «О персональных данных». Обработка персональных данных допускается в следующих случаях:

4.1.1. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

4.1.2. Обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для

осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей;

4.1.3. Обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

4.1.4. Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

4.1.5. Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

4.1.6. Обработка персональных данных необходима для осуществления прав и законных интересов Оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

4.1.7. Осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

4.1.8. Осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

4.2. В случае, если Оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

5. Конфиденциальность персональных данных

5.1. Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

6. Право субъекта персональных данных на доступ к его персональным данным

6.1. Субъект персональных данных имеет право на получение сведений, указанных в п. 6.7 настоящей Политики, за исключением случаев, при которых доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц. Субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не

являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6.2. Сведения, указанные в п. 6.7 настоящей Политики, должны быть предоставлены субъекту персональных данных Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных

6.3. Сведения, указанные в п. 6.7 настоящей политики, предоставляются субъекту персональных данных или его представителю Оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись субъекта персональных данных или его представителя Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

6.4. В случае, если сведения, указанные в п. 6.7 настоящей Политики, а также обрабатываемы персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в п. 6.7 настоящего положения, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

6.5. Субъект персональных данных вправе обратиться повторно к Оператору или направить ему запрос в целях получения сведений, указанных в п. 6.7 настоящей Политики, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в п. 6.4 настоящей Политики, в случае, если такие сведения и (или) обрабатываемы персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п. 6.3 настоящей Политики, должен содержать основание направления повторного запроса.

6.6. Оператор в праве отказать субъекту персональных данных в выполнении повторного запроса, несоответствующего условиям, предусмотренным п. 6.3 и п. 6.4. настоящей Политики. Такой отказ должен быть мотивированным. Обязанность предоставления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

6.7. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

6.7.1. Подтверждение факта обработки персональных данных Оператором;

6.7.2. Правовые основания и цели обработки персональных данных;

6.7.3. Цели и применяемые Оператором способы обработки персональных данных;

6.7.4. Наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которые могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;

6.7.5. Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;

6.7.6. Сроки обработки персональных данных, в том числе сроки их хранения;

6.7.7. Порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

6.7.8. Информацию об осуществленной или о предполагаемой трансграничной передаче данных;

6.7.9. Наименование или имя, фамилию, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу.

6.7.10. Иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

7. Право на обжалование действий или бездействий Оператора

7.1. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействия Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

7.2. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

8. Обязанности Оператора при сборе персональных данных

8.1. При сборе персональных данных Оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 6.7 настоящей Политики.

8.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

8.3. Если персональные данные получены не от субъекта персональных данных, Оператор, за исключением случаев, предусмотренных п. 8.4 настоящей Политики, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

8.3.1. Наименование либо фамилия, имя, отчество и адрес Оператора или его представителя;

8.3.2. Цель обработки персональных данных и ее правовое основание;

8.3.3. Предполагаемые пользователи персональных данных;

8.3.4. Установленные настоящим Федеральным законом права субъекта персональных данных;

8.3.5. Источник получения персональных данных.

8.4. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные п. 8.3 настоящего Положения, в случаях, если:

8.4.1. Субъект персональных данных уведомлен об осуществлении обработки его персональных данных Оператором;

8.4.2. Персональные данные получены Оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

8.4.3. Персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

8.4.4. Предоставление субъекту персональных данных сведений, предусмотренных частью 8.3 настоящей Политики, нарушает права и законные интересы третьих лиц.

9. Меры направленные на обеспечение выполнения Оператором обязанностей, предусмотренных Федеральным законом «О персональных данных»

9.1. Назначен ответственный за организацию обработки персональных данных.

9.2. Изданы документы, определяющие политику Оператора в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

9.3. Утверждены правила проведения внутреннего контроля соответствия обработки персональных данных требованиям Федерального закона «О персональных данных» и принятых в соответствии с ним нормативных правовых актов, настоящей Политике, локальным актам.

9.4. Проведена оценка вреда, который может быть причинен субъектам персональных данных, соотношение указанного вреда и применяемых оператором мер.

9.5. Проведено ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

10. Меры по обеспечению безопасности персональных данных при их обработке

10.1. Определены угрозы безопасности персональных данных при их обработке в информационных системах персональных данных.

10.2. Применяются организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимые для выполнения требований к защите персональных данных.

10.3. Применяются прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации.

10.4. Проведена оценка соответствия принимаемых мер по обеспечению безопасности персональных данных, получен аттестат соответствия требованиям по безопасности информации.

10.5. Ведется учет машинных носителей персональных данных.

10.6. Выполняются меры по обнаружению фактов несанкционированного доступа к персональным данным и принятию соответствующих мер.

10.7. Определен комплекс мер по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

10.8. Установлены правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных, обеспечена регистрация и учет всех действий, совершаемых с персональными данными в информационных системах персональных данных.

Осуществляется контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

Приложение №19 к Приказу № 357 от 24 декабря 2017

ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

Настоящая инструкция определяет права, обязанности и ответственность лица, ответственного за организацию обработки персональных данных.

Ответственный за организацию обработки персональных данных в своей деятельности руководствуется:

– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;

– Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687;

– Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2. Обязанности

Ответственный за организацию обработки персональных данных обязан:

– Доводить до сведения работников положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к обеспечению безопасности персональных данных;

– Осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, а именно организовывать проведение периодических (не менее одного раза в год) проверок соответствия обработки персональных данных. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывать непосредственному руководителю в письменном виде;

– Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и/или осуществлять контроль за приемом и обработкой таких обращений и запросов.

3. Ответственность

За неисполнение (ненадлежащее исполнение) своих должностных обязанностей, предусмотренных настоящей инструкцией, ответственный за организацию обработки

персональных данных несет персональную ответственность в соответствии с законодательством Российской Федерации.

4. Права

Ответственный за организацию обработки персональных данных имеет право:

– Требовать от работников письменных объяснений по фактам нарушения ими требований законодательства Российской Федерации, локальных актов о персональных данных и защите персональных данных;

– Вносить предложения непосредственному руководителю об отстранении работников от обработки персональных данных, применению к ним дисциплинарных взысканий, при обнаружении нарушения ими требований законодательства Российской Федерации, локальных актов по вопросам обработки персональных данных или требований к защите персональных данных.

С инструкцией ознакомлен(ы): _____/_____

Приложение №20 к Приказу № 357 от 24 декабря 2017

ПРАВИЛА РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ

1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

– Подтверждение факта обработки персональных данных;

– Правовые основания и цели обработки персональных данных;

– Цели и применяемые оператором способы 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 от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон);

– Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;

– Сроки обработки персональных данных, в том числе сроки их хранения;

– Наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу.

2. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

3. Сведения должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

4. Сведения предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

5. В случае если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной по которому является субъект персональных данных.

6. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 5 настоящих правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 4 настоящих правил, должен содержать обоснование направления повторного запроса.

7. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 5 и 6 настоящих правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

8. Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных:

– Оператор обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение 30 (тридцати) дней с даты получения запроса субъекта персональных данных или его представителя.

– В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 (тридцати) дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

– Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий 7 (семи) рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными

или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий 7 (семи) рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях, предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

– Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение 30 (тридцати) дней с даты получения такого запроса.

Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

С правилами ознакомлен(ы): _____/_____

Приложение №21 к Приказу № 357 от 24 декабря 2017

ПРАВИЛА РАБОТЫ ЛИЦ, ДОСТУП КОТОРЫХ К ПЕРСОНАЛЬНЫМ ДАННЫМ, В ТОМ ЧИСЛЕ ОБРАБАТЫВАЕМЫМ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ, НЕОБХОДИМ ДЛЯ ВЫПОЛНЕНИЯ ИМИ СЛУЖЕБНЫХ (ТРУДОВЫХ) ОБЯЗАННОСТЕЙ

Допуск для работы на автоматизированных рабочих местах (далее – АРМ) состоящих в составе информационной системы персональных данных (далее – ИСПДн) осуществляется на основании утвержденного перечня лиц, доступ которых к персональным данным, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей (далее – Пользователи ИСПДн).

Пользователь ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения и записи информации, содержащей персональные данные (далее – ПДн), разрешается использовать только машинные носители информации, учтенные в журнале учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации.

Пользователь несет ответственность за правильность включения и выключения АРМ, входа и выхода в систему и за все свои действия при работе в ИСПДн.

Вход пользователя в систему осуществляется по выдаваемому ему электронному идентификатору и по персональному паролю.

При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов и иных вредоносных программ с использованием штатных антивирусных средств, установленных на АРМ. В случае обнаружения вирусов либо вредоносных программ пользователь ИСПДн обязан немедленно прекратить их использование и действовать в соответствии с требованиями инструкции по организации антивирусной защиты.

Каждый работник, участвующий в рамках своих служебных обязанностей в процессах обработки персональных данных в ИСПДн и имеющий доступ к АРМ, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

– Строго соблюдать установленные соответствующими инструкциями правила обеспечения безопасности информации в ИСПДн;

– Знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;

– Хранить в тайне свой пароль (пароли). Выполнять требования инструкции по организации парольной защиты в полном объеме;

– Хранить индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);

– Выполнять требования инструкции по организации антивирусной защиты в полном объеме;

– Немедленно известить ответственного за обеспечение безопасности персональных данных в случае утери электронного идентификатора или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

– Несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ;

– Отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения;

– Некорректного функционирования установленных на АРМ технических средств защиты;

– Непредусмотренных отводов кабелей и подключенных устройств.

Пользователю АРМ категорически запрещается:

– Использовать компоненты программного и аппаратного обеспечения АРМ в личных целях;

– Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;

– Записывать и хранить конфиденциальную информацию (содержащую персональные данные) на неучтенных машинных носителях информации (гибких магнитных дисках, флэш-накопителях и т.п.);

– Оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

– Оставлять без личного присмотра на рабочем месте или в ином месте свой электронный идентификатор, машинные носители и распечатки, содержащие персональные данные;

– Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты;

– Размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации, содержащей персональные данные.

С правилами ознакомлен(ы): _____/_____

Приложение №22 к Приказу № 357 от 24 декабря 2017

ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

Настоящая инструкция определяет права и обязанности лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – ИСПДн).

Лицо ответственное за обеспечение безопасности персональных данных в ИСПДн (далее – администратор информационной безопасности) это лицо, отвечающее за обеспечение заданных характеристик информации, содержащей персональные данные (конфиденциальности, целостности и доступности) в процессе их обработки в ИСПДн.

Администратор информационной безопасности в ИСПДн осуществляет контроль за выполнением требований нормативно-правовых и организационно-распорядительных документов по организации обработки и обеспечению безопасности персональных данных при их обработке в ИСПДн с использованием автоматизированных рабочих мест.

2. Обязанности администратора информационной безопасности

Администратор информационной безопасности обязан:

– Знать требования нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности персональных данных при их обработке в ИСПДн;

– Знать перечень обрабатываемых персональных данных, состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных.

– Уметь пользоваться средствами защиты информации и осуществлять их непосредственное администрирование;

– Еженедельно осуществлять резервное копирование информации, содержащей персональные данные (при необходимости);

– Обязан осуществлять периодический контроль за выполнением работниками эксплуатирующими ИСПДн (пользователями ИСПДн), мероприятий по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн;

– Участвовать в работе по проведению внутреннего контроля соответствия обработки персональных данных требованиям по защите информации;

– Обязан анализировать журнал системы защиты информации от несанкционированного доступа (НСД), проводить проверки электронного журнала обращений к информационным системам персональных данных;

– Обязан обеспечивать строгое выполнение требований по обеспечению защиты информации при организации технического обслуживания АРМ;

– Обязан вести журнал учета средств защиты информации, используемых в ИСПДн;

– Обязан присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию АРМ;

– Обязан проводить инструктаж пользователей ИСПДн по правилам работы с используемыми техническими средствами и средствами защиты информации в соответствии с технической документацией на используемые средства защиты;

– Обязан проводить мероприятия по организации антивирусной защиты;

– Осуществлять организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями, согласно инструкции по организации парольной защиты в информационных системах персональных данных;

– Обязан организовать ведение журнала учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации;

– Обязан немедленно сообщать ответственному за организацию обработки персональных данных, информацию об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ, а также принимать необходимые меры по устранению нарушений:

– Установить причины, по которым стал возможным НСД;

– Установить последствия, к которым привел НСД;

– Зафиксировать случай НСД в виде документа (акта, служебной записки и т.д.) с описанием причин НСД, предполагаемых или установленных нарушителей и последствий;

– Провести проверку настроек средств защиты информации и операционных систем на соответствие требованиям руководящих документов и разрешительной системы доступа пользователей к защищаемым информационным ресурсам и объектам доступа ИСПДн, при необходимости провести настройку;

– Провести инструктаж пользователей ИСПДн по выполнению требований по обеспечению защиты персональных данных.

3. Права администратора информационной безопасности.

Администратор информационной безопасности имеет право:

– Требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкции о порядке работы пользователей в ИСПДн в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;

– Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

– Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности персональных данных к ответственному за организацию обработки персональных данных в ИСПДн и/или ответственному за эксплуатацию ИСПДн;

4. Ответственность администратора информационной безопасности

На администратора информационной безопасности возлагается персональная ответственность за качество проводимых им работ по обеспечению безопасности ПДн в ИСПДн;

Администратор информационной безопасности в ИСПДн несет ответственность в соответствии с действующим законодательством Российской Федерации.

С инструкцией ознакомлен(ы): _____/_____

Приложение №23 к Приказу № 357 от 24 декабря 2017

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ РЕЗЕРВИРОВАНИЯ

1. Общие положения

Настоящая инструкция разработана с целью обеспечения возможности оперативного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационной системы персональных данных (далее – ИСПДн).

2. Резервируемое программное обеспечение и базы персональных данных

В ИСПДн резервированию подлежит:

– Общее программное обеспечение (операционная система и программные драйверы устройств (принтера, монитора, видеокарты и т.п.), поставляемые с компонентами автоматизированных рабочих мест (далее – АРМ), входящими в состав ИСПДн);

– Прикладное программное обеспечение, используемое для обработки персональных данных (средства обработки текстов и таблиц, специализированные программы и т.п.);

– Базы персональных данных (тестовые и табличные файлы, а также файлы баз данных специализированных программ);

– Программное обеспечение средств защиты информации, в том числе средств антивирусной защиты.

3. Порядок резервирования и хранения резервных копий

Резервирование общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации обеспечивается путем хранения у администратора информационной безопасности в ИСПДн машинных носителей информации, содержащих дистрибутивы данного программного обеспечения.

Машинные носители информации обновлений общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации должны также храниться у администратора информационной безопасности в ИСПДн.

Допускается хранение машинных носителей прикладного программного обеспечения и машинных носителей с обновлениями к нему в структурных подразделениях, эксплуатирующих ИСПДн.

Резервирование баз персональных данных, а также текстовых и табличных файлов, содержащих персональные данные, допускается только на учтенные установленным порядком машинные носители информации.

Резервирование осуществляется ежемесячно.

Резервные носители персональных данных хранятся в структурных подразделениях, эксплуатирующих ИСПДн, в порядке, предусмотренном для носителей информации персональных данных.

К резервному носителю персональных данных должна быть приложена учетная карточка, в которой делаются отметки о дате резервирования.

Резервные носители персональных данных не могут быть переданы за пределы структурных подразделений, эксплуатирующих ИСПДн.

Копирование информации с резервных носителей персональных данных, за исключением случая восстановления работоспособности ИСПДн, запрещается.

4. Порядок восстановления работоспособности ИСПДн

Восстановление работоспособности ИСПДн осуществляется в случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее программного обеспечения.

Данные работы осуществляются администратором информационной безопасности в ИСПДн в соответствии с эксплуатационной документацией на программное обеспечение до полного восстановления работоспособности.

В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с персональными данными. Ответственность за выполнение данного требования возлагается на администратора информационной безопасности в ИСПДн и руководителя структурного подразделения, обеспечивающего ее эксплуатацию.

Учетная карточка резервного носителя персональных данных
№ _____

Дата резервного копирования	Объект копирования	Кто производил копирование	Подпись

С инструкцией ознакомлен(ы): _____/_____

Приложение №24 к Приказу № 357 от 24 декабря 2017

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах персональных данных (далее – ИСПДн), а также контроль за действиями пользователей при работе с паролями.

Личные пароли генерируются и распределяются централизованно Администратором информационной безопасности:

– Длина пароля должна быть не менее 8 символов;

– В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);

– Символы паролей должны вводиться в режиме латинской раскладки клавиатуры;

– Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

– При смене пароля новое значение должно отличаться от предыдущих;

– Пользователь не имеет права сообщать личный пароль другим лицам;

Полная плановая смена паролей пользователей ИСПДн должна проводиться регулярно, не реже одного раза в 3 месяца.

Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение и т.п.) должна производиться администратором информационной безопасности в ИСПДн немедленно после окончания последнего сеанса работы данного пользователя ИСПДн с системой на основании письменного указания непосредственного руководителя структурного подразделения.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) администратора информационной безопасности в ИСПДн.

В случае компрометации (утеря, передача другому лицу) личного пароля, Пользователь ИСПДн обязан незамедлительно сообщить об этом администратору информационной безопасности для принятия соответствующих мер.

С инструкцией ознакомлен(ы): _____/_____

Приложение №25 к Приказу № 357 от 24 декабря 2017

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ

1. Общие требования

Настоящая инструкция определяет требования к организации антивирусной защиты информационных систем персональных данных (далее – ИСПДн) от разрушающего воздействия вирусов и вредоносных программ и устанавливает ответственность руководителя и работников структурных подразделений, эксплуатирующих и сопровождающих ИСПДн, за их выполнение. Инструкция распространяется на все существующие и вновь разрабатываемые ИСПДн. Для отдельных ИСПДн могут быть разработаны свои инструкции, учитывающие особенности работы.

К использованию в ИСПДн допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

Установка и настройка средств антивирусного контроля осуществляется администратором информационной безопасности в ИСПДн или специально назначенным лицом в соответствии с эксплуатационной документацией на антивирусных средств.

2. Применение средств антивирусного контроля

При загрузке АРМ в автоматическом режиме должен проводиться антивирусный контроль служб операционной системы, исполняемых приложений, находящихся в автозагрузке, реестра операционной системы.

Полному антивирусному контролю автоматизированные рабочие места (АРМ) должны подвергаться не реже одного раза в неделю.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, оптических и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов и других вредоносных программ. Непосредственно после установки (изменения) программного обеспечения, администратором информационной безопасности в ИСПДн должна быть выполнена антивирусная проверка на защищаемых серверах и пользовательских АРМ.

При возникновении подозрения на наличие вируса либо вредоносной программы (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.)

работник структурного подразделения самостоятельно или вместе с администратором информационной безопасности в ИСПДн должен провести внеочередной антивирусный контроль своего АРМ.

В случае обнаружения при проведении антивирусной проверки зараженных вирусами либо вредоносными программами файлов, необходимо:

– Приостановить работу в ИСПДн;

– Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя структурного подразделения и администратора информационной безопасности в ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

– Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

– Провести лечение или уничтожение зараженных файлов.

3. Ответственность

Ответственность за проведение мероприятий антивирусного контроля в подразделениях и соблюдение требований настоящей Инструкции возлагается на администратора информационной безопасности в ИСПДн и всех работников, являющихся пользователями ИСПДн.

С инструкцией ознакомлен(ы): _____/_____

Приложение №26 к Приказу № 357 от 24 декабря 2017

ИНСТРУКЦИЯ ПО ПРОВЕРКЕ ЭЛЕКТРОННОГО ЖУРНАЛА ОБРАЩЕНИЙ К ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Задачи проверки.

Под проверкой понимается отслеживание событий, происходивших на автоматизированных рабочих местах (далее – АРМ) в течение определенного времени.

Общими задачами проверки являются:

– Контролирование состояния защищенности системы;

– Выявление причин произошедших изменений;

– Определение лиц или процессов, деятельность которых привела к изменению состояния защищенности системы или к НСД;

– Установление времени изменений.

Проверку средств защиты осуществляет администратор информационной безопасности.

2. Журналы записей о событиях.

События, происходящие на АРМ, входящем в состав ИСПДн, регистрируются в журналах.

Каждому событию соответствует отдельная запись в журнале, содержащая подробную информацию для анализа события.

В состав используемых в ИСПДн средств защиты информации может входить специальное программное средство для аудита журналов событий, предназначенное для загрузки и просмотра журналов (далее — программа просмотра журналов). В программу просмотра журналов могут быть загружены записи следующих журналов:

– Штатные журналы операционной системы Windows;

– Журналы событий средств защиты информации.

3. Штатные журналы операционной систем.

В штатных журналах ОС Windows регистрируются только те события, которые имеют отношение к операционной системе. События используемых средств защиты информации в них не регистрируются.

Информация о событиях, происходящих на АРМ под управлением ОС Windows, сохраняется в следующих штатных журналах:

– Журнал приложений – содержит сведения об ошибках, предупреждениях и других событиях, возникающих при исполнении приложений;

– Системный журнал – содержит сведения об ошибках, предупреждениях и других событиях, возникающих в операционной системе;

– Журнал безопасности – хранит информацию о попытках регистрации, а также о событиях, связанных с использованием ресурсов.

Подробное описание содержимого штатных журналов ОС Windows отражено в документации к операционной системе.

Загрузка и просмотр записей штатных журналов может осуществляться как в программе просмотра журналов средств защиты, так и с помощью стандартных средств работы с журналами ОС Windows — в оснастке «Просмотр событий» («Eventviewer»).

4. Журнал событий средств защиты информации.

Журналы средств защиты информации (далее – СЗИ) хранят информацию о событиях, отслеживаемых средствами самих СЗИ, в этом журнале регистрируются события, заданные параметрами СЗИ для локальной политики безопасности.

5. Аудит.

Сведения, содержащиеся в журнале, позволяют отслеживать использование механизмов защиты, которые предоставляют средства защиты информации АРМ (шифрование файлов, полномочное управление, замкнутая программная среда и др.) подробное описание регистрируемых событий указано в соответствующих руководствах к используемым СЗИ.

6. Просмотр событий электронных журналов.

Администратор информационной безопасности в ИСПДн производит проверку электронных журналов.

В случае обнаружения нарушений администратор информационной безопасности докладывает о данном факте ответственному за организацию обработки персональных данных.

С инструкцией ознакомлен(ы): _____/_____

Приложение №27 к Приказу № 357 от 24 декабря 2017

ПОРЯДОК УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ДОСТИЖЕНИИ ЦЕЛЕЙ ОБРАБОТКИ И (ИЛИ) ПРИ НАСТУПЛЕНИИ ИНЫХ ЗАКОННЫХ ОСНОВАНИЙ

Настоящий документ устанавливает порядок уничтожения информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Документы, дела, книги и журналы учета, содержащие персональные данные, при достижении целей обработки, или при наступлении иных законных оснований, (например, утратившие практическое значение, а также с истекшим сроком хранения), подлежат уничтожению.

Уничтожение документов производится в присутствии ответственного за организацию обработки персональных данных, который несет персональную ответственность за правильность и полноту уничтожения перечисленных в акте документов (Акт составляется в свободной форме).

Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются.

После уничтожения материальных носителей ответственный за организацию подписывает акт в двух экземплярах, также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №__(дата)».

Уничтожение информации на носителях необходимо осуществлять путем стирания информации с использованием сертифицированного программного обеспечения, установленного на АРМ с гарантированным уничтожением (в соответствии с заданными характеристиками для установленного программного обеспечения с гарантированным уничтожением).

Информация, содержащая персональные данные при достижении целей обработки или при наступлении иных законных оснований (например, утратившие практическое значение, с истекшим сроком хранения) в электронном виде, подлежит уничтожению.

Приложение №28 к Приказу № 357 от 24 декабря 2017

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных в МБОУ СОШ № 144требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных» (далее – Правила), устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют порядок проведения процедур внутреннего контроля исполнения требований законодательства.

2. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных организовывается проведение периодических проверок.

3. Проверки осуществляются ответственным за организацию обработки персональных данных совместно с ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных.

4. Плановые проверки проводятся не чаще чем один раз в три месяца.

5. Внеплановые проверки проводятся по инициативе ответственного за организацию обработки персональных данных, либо ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных

6. Основанием для проведения проверки служит издание приказа «О проведении внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных»

7. При проведении проверки должны быть полностью, объективно и всесторонне установлены:

– соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Оператора персональных данных;

– соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

– достаточность (избыточность) персональных данных для целей обработки персональных данных, заявленных при сборе персональных данных;

– отсутствие (наличие) объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;

– порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

– порядок и условия применения средств защиты информации;

– соблюдение правил доступа к персональным данным;

– наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер.

8. Ответственный за организацию обработки персональных данных и ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных в ходе проверки имеют право:

– запрашивать у работников информацию, необходимую для реализации своих полномочий;

– требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

– принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

– вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

– вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

9. Ответственный за организацию обработки персональных данных в течение 3 (трех) рабочих дней направляет в адрес директора результаты проведения проверки в форме служебной записки.

С правилами ознакомлен(ы): _____/_____

Приложение №29 к Приказу № 357 от 24 декабря 2017

ИНСТРУКЦИЯ
ПО ОБРАЩЕНИЮ С КРИПТОСРЕДСТВАМИ

1. Общие положения

Настоящая инструкция регламентирует порядок обращения с шифровальными средствами (средствами криптографической защиты информации, СКЗИ), предназначенными для защиты информации, не содержащей сведений, составляющих государственную тайну, в процессе их получения, транспортировки, учета, хранения, уничтожения, встраивания в прикладные системы, тестирования, передачи клиентам, а также порядок допуска к работам с шифровальными средствами.

Все сотрудники, допущенные к работе с СКЗИ, должны ознакомиться с данной инструкцией под подпись и строго выполнять требования настоящей инструкции в части, их касающейся, а также строго выполнять требования нормативных правовых актов Российской Федерации, относящихся к деятельности с СКЗИ, нормативных и методических документов лицензирующего органа.

Разработка и проведение мероприятий по обеспечению безопасности при работе с СКЗИ осуществляется ответственным за эксплуатацию СКЗИ.

Работы с СКЗИ должны проводиться с учетом Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

2. Требования по размещению, оборудованию и охране помещений

Размещение, оборудование, охрана и режим в помещениях, в которых проводятся работы с СКЗИ (далее – помещения), должны обеспечивать безопасность СКЗИ, сведение к минимуму возможности неконтролируемого доступа посторонних лиц. Доступ сотрудников в эти помещения должен быть ограничен в соответствии со служебной необходимостью и определяться перечнем лиц, допущенных в кабинеты.

Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Для предотвращения просмотра извне окна помещений должны быть защищены (жалюзи, шторы и т.п.).

3. Порядок обращения с СКЗИ

Пользователи криптосредств обязаны:

- не разглашать информацию о ключевых документах;
- не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;
- не допускать установки ключевых документов в другие ПЭВМ.

Все поступающие СКЗИ, инсталлирующие СКЗИ носители, эксплуатационная и техническая документация (при наличии) к ним должны браться на поэкземплярный учет в журнале установленной формы (Приложение). Ведет журналы администратор информационной безопасности.

Единицей поэкземплярного учета СКЗИ является:

−для аппаратных и программно-аппаратных СКЗИ - конструктивно законченное техническое устройство;

−для программных СКЗИ – инсталлирующий СКЗИ носитель (дискета, компакт-диск (CD-ROM) и т.п.).

Должны быть приняты организационные меры с целью исключения возможности несанкционированного копирования СКЗИ.

Хранение инсталлирующих СКЗИ носителей допускается в одном хранилище с другими документами при условиях, исключающих непреднамеренное их уничтожение или иное, не предусмотренное правилами пользования СКЗИ применение.

В случае отсутствия у сотрудника индивидуального хранилища инсталлирующие СКЗИ носители по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение.

В случае утери носителя СКЗИ или вероятном копировании сотрудник обязан немедленно сообщить об этом лицу, ответственному за обеспечение безопасности при обращении с СКЗИ.

Ответственным за эксплуатацию СКЗИ периодически должен проводиться контроль сохранности и работоспособности установленного СКЗИ, а также всего используемого совместно с СКЗИ программного обеспечения для предотвращения внесения программно-аппаратных закладок и вирусов.

4.Ответственность за нарушение требований Инструкции

За нарушение требований настоящей Инструкции виновные лица несут дисциплинарную, либо материальную ответственность в зависимости от характера нарушения и тяжести наступивших отрицательных последствий.

С инструкцией ознакомлен(ы): _____/_____

Приложение №30 к Приказу № 357 от 24 декабря 2017

ИНСТРУКЦИЯ ПО ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

1. Общие положения.

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому гражданину, обратившемуся в МБОУ СОШ № 144, или сотруднику (далее – субъекту персональных данных) МБОУ СОШ № 144.

Обработка персональных данных, содержащихся в информационной системе персональных данных 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.

Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные настоящим Положением, должны применяться с учетом требований Постановления Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г. № 687, а также требований нормативных правовых актов федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации.

2. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации.

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники МБОУ СОШ № 144 или лица, осуществляющие такую обработку по договору с МБОУ СОШ № 144), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется МБОУ СОШ № 144 без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами МБОУ СОШ № 144.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес учреждения, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых учреждением способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации,– при необходимости получения письменного согласия на обработку персональных данных;
- типовая форма должна быть составлена 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.

При ведении журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещения МБОУ СОШ № 144 или в иных аналогичных целях, должны соблюдаться следующие условия:

- необходимость ведения такого журнала должна быть предусмотрена актом МБОУ СОШ № 144, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных;
- копирование содержащейся в таких журналах информации не допускается;
- персональные данные каждого субъекта персональных данных могут заноситься в такой журнал не более одного раза в каждом случае пропуска субъекта персональных данных.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, зачеркивание, стирание).

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя,– путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории

персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

С инструкцией ознакомлен(ы): _____/_____

Приложение №31 к Приказу № 357 от 24 декабря 2017

ПРАВИЛА
РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ДАННЫМИ

1.Общие положения

Настоящие Правила работы с обезличенными персональными данными МБОУ СОШ № 144 разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и определяют порядок работы с обезличенными данными МБОУ СОШ № 144.

2.Термины и определения

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» в настоящих Правилах используются следующие понятия:

- персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту 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;
- обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

3.Условия обезличивания

Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных МБОУ СОШ № 144 и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Способы обезличивания при условии дальнейшей обработки персональных данных:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- обобщение – понижение точности некоторых сведений;

- понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только населенный пункт)
- деление сведений на части и обработка в разных информационных системах;
- другие способы.

Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

4. Порядок работы с обезличенными персональными данными

Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- парольной политики;
- антивирусной политики;
- правил работы со съемными носителями (если они используется);
- правил резервного копирования;
- правил доступа в помещения, где расположены элементы информационных систем.

При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;
- правил доступа к ним и в помещения, где они хранятся.

С правилами ознакомлен(ы): _____/_____

Приложение №32 к Приказу № 357 от 24 декабря 2017

ИНСТРУКЦИЯ ПО РАБОТЕ С ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ответственность за выявление инцидентов ИБ и реагирование на них в МБОУ СОШ № 144 возлагается на администратора информационной безопасности.

Администратор информационной безопасности имеет полномочия инициировать проведение служебных проверок (ходатайствовать о наложении дисциплинарного взыскания перед руководителем МБОУ СОШ № 144) по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации.

Администратор информационной безопасности обязан вести журнал учёта инцидентов ИБ (событий, действий повлекших за собой риски безопасности защищаемой информации и создающих предпосылки к нарушению критериев безопасности информации). Сюда относятся нарушения пользователями положений организационно-распорядительных документов, установленных порядков и технологии работы в ИС, разглашение защищаемой информации и любые действия, направленные на это, не антропогенные инциденты (сбои ПО, стихийные бедствия).

В журнале в свободной форме описывается инцидент с указанием следующих данных:

- даты и времени;
- причин (умышленные и неумышленные действия, не антропогенные инциденты и т.п.) и описания инцидента и задействованных лиц;
- информации о последствиях;
- информации о возможных последствиях (экономические убытки (в связи с заменой СЗИ, повторной аттестации; временные и трудозатраты на устранение последствий, нарушение работы пользователей, ущерб субъектам ПДн и юридические последствия для МБОУ СОШ № 144 и т.п.).

Журнал с данным отчётом об инциденте предоставляется на ознакомление ответственному за организацию обработки персональных данных для принятия мер по предотвращению рецидива (возникновения повторного инцидента).

В случае возникновения рецидива со стороны пользователя или администратора информационной безопасности, по ходатайству ответственного за организацию обработки персональных данных руководителем МБОУ СОШ № 144 накладывается дисциплинарное взыскание.

Сокрытие нарушений и инцидентов ИБ, вызванных любыми должностными лицами МБОУ СОШ № 144, является грубым нарушением трудовой дисциплины. Сокрытие нарушений и инцидентов ИБ, вызванных действиями администратора информационной безопасности и ответственным за организацию обработки персональных данных, является грубейшим нарушением дисциплины, и при выяснении данного факта должно строго наказываться.

Любой сотрудник должен согласовывать следующие действия с администратором информационной безопасности:

- замена прикладного оборудования (мышь, клавиатура, принтер, монитор);
- установка дополнительного ПО;
- изменение сетевых настроек рабочего места;

– замена, изменение любой аппаратной части рабочего места.

Ответственный за организацию обработки персональных данных не может требовать от администратора информационной безопасности действий, направленных на нарушение настоящего руководства и других организационно-распорядительных документов МБОУ СОШ № 144, требовать сокрытия инцидентов ИБ, вызванных любыми должностными лицами, требовать сообщения ему паролей на средства защиты информации и нарушения установленного разграничения прав по допуску к информационным ресурсам, установленным матрицей доступа к информационными ресурсам ИС.

С инструкцией ознакомлен(ы): _____/_____

Приложение №33 к Приказу № 357 от 24 декабря 2017

ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ЭКСПЛУАТАЦИЮ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

Ответственный за эксплуатацию информационной системы персональных данных (далее – ИСПДн) в МБОУ СОШ № 144 назначается Директором.

Методическое руководство работой ответственного за эксплуатацию ИСПДн осуществляется ответственным за организацию обработки персональных данных в МБОУ СОШ № 144.

Ответственный за эксплуатацию в своей работе руководствуется положениями, руководящими и нормативными документами ФСТЭК и ФСБ России по защите информации и организационно-распорядительными документами для данной ИСПДн, а также иными нормативными документами в части защиты информации.

Ответственный за эксплуатацию ИСПДн несет ответственность за свои действия, и действия сотрудников вверенного структурного подразделения в соответствии с действующим законодательством РФ.

2. Функции ответственного за эксплуатацию ИСПДн

Осуществление контроля за целевым использованием ИСПДн, всех периферийных устройств и технических средств, входящих в состав ИСПДн.

Контроль за отсутствием в период обработки защищаемой информации в помещении, где осуществляется обработка, посторонних лиц, не допущенных к обрабатываемой информации.

Контроль использования сотрудниками структурных подразделений, эксплуатирующими ИСПДн, средств защиты информации, установленных на АРМ, входящих в состав ИСПДн.

Контроль за правильностью использования и хранения сотрудниками структурных подразделений, эксплуатирующими ИСПДн, машинных носителей информации и документов, содержащих персональные данные.

Представление заявок на пользователей, допускаемых к защищаемым ресурсам ИСПДн, с целью закрепления за ними носителей информации устройств блокировки, паролей и других средств разграничения доступа к информации, а также прав пользования средствами вычислительной техники.

Организация повышения уровня осведомленности подчиненных должностных лиц по вопросам информационной безопасности.

3. Обязанности ответственного за эксплуатацию ИСПДн

Четко знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководств по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

Обеспечивать функционирование ИСПДн в пределах возложенных на него функций.

Обеспечивать контроль выполнения установленного комплекса мероприятий по обеспечению безопасности ПДн.

Контролировать целостность печатей (пломб) на устройствах ИСПДн.

Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств ИСПДн и отправке их в ремонт.

Присутствовать при выполнении технического обслуживания ИСПДн при установке (модификации) программного обеспечения.

Информировать администратора информационной безопасности о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

Контролировать соответствие состава ИСПДн техническому паспорту на ИСПДн.

Приложение №34 к Приказу № 357 от 24 декабря 2017

ПЛАН
МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ В МБОУ СОШ № 144

1. Общие положения

План мероприятий по обеспечению защиты персональных данных (далее – План мероприятий), содержит необходимый перечень мероприятий для обеспечения защиты персональных данных в информационных системах персональных данных МБОУ СОШ № 144.

Выбор конкретных мероприятий осуществляется на основании перечня актуальных угроз безопасности, указанных в Модели угроз безопасности для соответствующей ИСПДн.

В План мероприятий включены следующие категории мероприятий:

- организационные (административные);
- физические;
- технические (аппаратные и программные);
- контролирующие.

В План мероприятий включена следующая информация:

- название мероприятия;
- периодичность мероприятия (разовое/периодическое);
- исполнитель мероприятия/ответственный за исполнение.

План внутренних проверок составляется на все информационные системы персональных данных МБОУ СОШ № 144.

План мероприятий по защите информации в МБОУ СОШ № 144

Мероприятие	Сроки	Ответственный
Организационные мероприятия		
Обследование информационных систем	январь 2018	Комиссия
Определение перечня ИСПДн	январь 2018	Комиссия
Определение обрабатываемых ПДн и объектов защиты	январь 2018	Комиссия
Определение круга лиц, участвующих в обработке ПДн	январь 2018	Директор
Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей	январь 2018	Директор
Классификация всех выявленных ИСПДн	январь 2018	Комиссия
Организация режима и контроля доступа (охраны) в помещения, в которых установлены аппаратные средства ИСПДн.	постоянно	
Организация порядка резервного копирования защищаемой информации на твердые носители	ежемесячно	Инженер-программист
Организация информирования сотрудников о порядке обработки ПДн и их обучения	по мере необходимости	Ответственный за организацию работы с ПД
Организация информирования сотрудников о введенном режиме защиты ПДн	январь 2018	Ответственный за организацию работы с ПД
Подготовка и утверждение комплекта нормативной документации, регламентирующей обработку ПДн в ИСПДн	январь-март 2018	Администрация
Технические мероприятия		
Внедрение специальной подсистемы управления доступом, регистрации и учета	по мере финансирования	Инженер-программист
Внедрение межсетевого экранирования	по мере финансирования	Инженер-программист
Внедрение криптографической защиты	по мере финансирования	Инженер-программист
Контролирующие мероприятия		
Контроль над соблюдением режима обработки ПДн	Еженедельно	Комиссия
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно	Комиссия
Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Еженедельно	Комиссия
Контроль за обеспечением резервного копирования	Ежемесячно	Комиссия
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз	Ежегодно	Комиссия
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	Ответственный за организацию работы с ПД