РОССИЙСКАЯ ФЕДЕРАЦИЯ

Муниципальное образование Ленинградской области города Кириши

МУНИЦИПАЛЬНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

«КИРИШСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 8»

187110, г.Кириши, Ленинградской области, ул. Декабристов Бестужевых, д. 15, тел\факс 587–28

П Р И К А З

от 20.07.2018 г. **№** 293-под

О работе по обработке персональных данных
в МОУ «КСОШ № 8»

На основании законодательства Российской Федерации и в исполнение действующих нормативных правовых актов в области обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных исполнения Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных»

П Р И К А З Ы В А Ю:

1. Утвердить Положение о разграничении прав доступа к обрабатываемым персональным данным (Приложение 1)
2. Назначить ответственных за обработку персональных данных в информационных системах персональных данных (Таблица 2 Приложения 1).
3. Осуществлять доступ лиц, ответственных за обработку персональных данных, на основании Таблицы 2 Приложения 1 настоящего приказа.
4. Ответственным за обработку персональных данных:
   - организовать работу по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
   - осуществлять доступ в информационные системы персональных данных на основании Положения об обработке персональных данных (приказ №489-под от 06.11.2014г.);
   - осуществлять регистрацию обращений субъектов персональных данных в Журнале учета обращений субъектов персональных данных о выполнении их законных прав (Приложение 2);
   - проводить разбирательства в случае несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищённости персональных данных;
   - принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований действующего законодательства Российской Федерации о персональных данных.
5. Ответственным за обработку персональных данных в своей работе руководствоваться законодательством Российской Федерации, действующими нормативными правовыми актами в области обеспечения безопасности персональных данных, а также организационно-правовой

документацией, утвержденной в МОУ «КСОШ № 8».

6. Утвердить Соглашение о неразглашение персональных данных субъекта (сотрудника школы). (Приложение 2).
7. Утвердить Заявление о согласии на обработку персональных данных сотрудника школы (Приложение 3).
8. Утвердить Отзыв согласия на обработку персональных данных (Приложение 4).
9. Утвердить Положение о защите, хранении, обработке и передаче персональных данных обучающихся МОУ «КСОШ № 8» (Приложение 5).
10. Утвердить Соглашение о неразглашении персональных данных субъекта (обучающегося или родителя (законного представителя)) (Приложение 6).
11. Утвердить Инструкцию по обеспечению безопасности персональных данных (Приложение 7).
12. Утвердить Инструкцию информационных систем персональных данных МОУ «КСОШ № 8» (Приложение 8).
13. Утвердить Инструкцию пользователя информационных систем персональных данных (ИСПДн) (Приложение 9).
14. Утвердить Инструкцию пользователя ИСПДн по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций (Приложение 10).
15. Утвердить Инструкцию по организации антивирусной защиты в МОУ «КСОШ № 8» (Приложение 11).
16. Создать комиссию по защите персональных данных работников школы и всех участков образовательного процесса с наделением ее полномочиями по проведению мероприятий, касающихся организации защиты персональных данных в составе:

Председатель	Королева Елена Анатольевна, директор
Члены комиссии:	Журавлева Наталья Вячеславовна, секретарь
	Третьякова Ольга Викторовна, главный бухгалтер
	Озерова Ирина Валерьевна, бухгалтер
	Куляка Ольга Владимировна, заместитель директора по учебно-воспитательной работе
	Сергеева Виктория Владимировна, заместитель директора по учебно-воспитательной работе
	Архипова Дарья Владимировна, заместитель директора по воспитательной работе
	Черных Антон Сергеевич, заместитель директора по безопасности
	Коваленко Юрий Петрович, заместитель директора по хозяйственной работе
	Агиевич Марина Михайловна, заведующий библиотекой

17. Контроль за исполнением настоящего приказа оставляю за собой.

Директор МОУ «КСОШ №8» Е.А.Королева

Приложение1
к приказу №293-под от 20.07.2018г.

ПОЛОЖЕНИЕ
о разграничении прав доступа к обрабатываемым персональным данным
в МОУ «КСОШ № 8»

1. Общие положения

1.1. Настоящее Положение о разграничении прав доступа к обрабатываемым персональным данным (далее - Положение) в МОУ «КСОШ № 8» (далее – Школа) разработано в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Правилами внутреннего трудового распорядка Школы и определяет уровень доступа должностных лиц к персональным данным работников и учащихся.

2. Основные понятия

2.1. Для целей настоящего Положения используются следующие основные понятия:

- **персональные данные работника** – любая информация, относящаяся к определенному или определяемому на основании такой информации работнику, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая работодателю в связи с трудовыми отношениями;
- **персональные данные учащихся** – информация, необходимая Школе в связи с отношениями, возникающими между обучающимся, его родителями (законными представителями) и Школой;
- **обработка персональных данных** – сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных;
- **конфиденциальность персональных данных** – обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным, требование не допускать их распространения без согласия работника (родителей (законных представителей) учащегося) или иного законного основания;
- **распространение персональных данных** – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;
- **использование персональных данных** – действия (операции) с персональными данными, совершаемые должностным лицом Школы в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников (обучающихся) либо иным образом затрагивающих их права и свободы или права и свободы других лиц;
- **блокирование персональных данных** – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;
- **уничтожение персональных данных** – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;
- **обезличивание персональных данных** – действия, в результате которых невозможно определить принадлежность персональных данных конкретному работнику (обучающемуся);
- **информация** - сведения (сообщения, данные) независимо от формы их представления.

3. Разграничение прав доступа при автоматизированной обработке информации

3.1. Разграничение прав осуществляется на основании Отчета по результатам проведения внутренней проверки, а также исходя из характера и режима обработки персональных данных в ИСПДн.

3.2. Список групп должностных лиц ответственных за обработку персональных данных в информационных системах персональных данных, а также их уровень прав доступа в ИСПДн представлен в таблице № 1.

Таблица № 1

Список групп должностных лиц ответственных за обработку персональных данных

Группа	Уровень доступа к ПДн	Разрешенные действия
Администратор безопасности	- Обладает правами Администратора ИСПДн. - Обладает полной информацией об ИСПДн. - Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн. - Имеет праав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение
Ответственный за сайт и электронный дневник	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение

4. Разграничение прав доступа при неавтоматизированной обработке персональных данных

4.1. Разграничение прав осуществляется исходя из характера и режима обработки персональных данных на материальных носителях.

4.2. Список лиц ответственных за неавтоматизированную обработку персональных, а так же их уровень прав доступа к персональным данным представлен в таблице № 2.

Таблица № 1

СПИСОК СОТРУДНИКОВ, ОТВЕТСТВЕННЫХ ЗА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ МОУ «КСОШ № 8»

Группа	*ФИО, должность*	*Персональные данные*	*Документы*	*Уровень доступа к ПДн*	*Разрешенные действия*
Администрация школы	Королева Елена Анатольевна, директор	персональные данные сотрудников, учащихся и их родителей (законных представителей)		Обладает полной информацией о персональных данных обучающихся и их родителей (законных представителей), работников школы. - Имеет доступ к личным делам обучающихся и работников, информации на материальных носителях, содержащей персональные данные обучающихся, их родителей (законных представителей) и работников школы.	- сбор и систематизация - накопление и хранение - уточнение (обновление, изменение) - использование - уничтожение - распространение - блокирование - обезличивание
Канцелярия	Журавлева Наталья Вячеславовна, секретарь	персональные данные сотрудников, учащихся и их родителей (законных представителей)	1) приказы по основной деятельности; 2) приказы по личному составу сотрудников; 3) личные дела сотрудников школы, в том числе военнообязанных, находящихся в запасе; 4) карточка унифицированной формы Т-2; 5) трудовые книжки; 6) медицинские книжки; 7) трудовые договора; 8) электронная база данных по сотрудникам 9) паспортные и анкетные данные сотрудников 10) приказы по контингенту учащихся; 11) личные дела учащихся; 12) электронная база данных по обучающимся 13) паспортные и анкетные данные учащихся и их родителей (законных представителей) 14) база данных ГИА и ЕГЭ;	- Обладает полной информацией о персональных данных обучающихся и их родителей (законных представителей), работников школы. - Имеет доступ к личным делам обучающихся и работников, информации на материальных носителях, содержащей персональные данные обучающихся, их родителей (законных представителей) и работников школы.	- сбор и систематизация - накопление и хранение - уточнение (обновление, изменение) - использование - уничтожение - распространение - блокирование - обезличивание

	Третьякова Ольга Викторовна, главный бухгалтер	персональные данные сотрудников, учащихся и их родителей (законных представителей)	1) приказы по основной деятельности; 2) приказы по личному составу сотрудников; 3) приказы по контингенту учащихся; 4) документы по тарификации сотрудников школы; 5) статистические отчеты; 6) электронная база данных по сотрудникам 7) электронная база данных по обучающимся 8) паспортные и анкетные данные сотрудников 9) паспортные и анкетные данные учащихся и их родителей (законных представителей) 10) трудовые договора; 11) трудовые книжки; 12) карточка унифицированной формы Т-2; 13) личные дела сотрудников школы;		
	Озерова Ирина Валерьевна, бухгалтер	в автоматизированной информационной системой управления сферой образования, персональные данные учащихся и их родителей (законных представителей)			
	Куляка Ольга Владимировна, заместитель директора по учебно-воспитательной работе	персональные данные сотрудников, учащихся и их родителей (законных представителей)	1) классные журналы; 2) статистические отчеты; 3) сведения о состоянии здоровья учащихся; 4) электронная база данных учащихся школы; 5) журнал учета замещенных уроков; 6) личные дела учащихся; 7) база данных ГИА и ЕГЭ; 8) организация процедурной итоговой аттестации (ЕГЭ, ГИА) 9) паспортные и анкетные данные учащихся и их родителей (законных представителей) 10) приказы по основной деятельности; 11) приказы по личному составу сотрудников; 12) личные дела сотрудников школы 13) приказы по контингенту учащихся;		

	Сергеева Виктория Владимировна, заместитель директора по учебно-воспитательной работе	персональные данные сотрудников, учащихся и их родителей (законных представителей)	1) классные журналы; 2) статистические отчеты; 3) сведения о состоянии здоровья учащихся; 4) электронная база данных учащихся школы; 5) журнал учета замещенных уроков; 6) личные дела учащихся; 7) база данных ГИА и ЕГЭ; 8) организация процедурной итоговой аттестации (ЕГЭ, ГИА) 9) паспортные и анкетные данные учащихся и их по контингенту учащихся;		
	Архипова Дарья Владимировна, заместитель директора по воспитательной работе	персональные данные учащихся и их родителей (законных представителей)	1) классные журналы; 2) электронная база данных учащихся школы; 3) личные дела учащихся; 4) социальный паспорт класса; 5) паспортные и анкетные данные учащихся и их родителей (законных представителей) 6) приказы по основной деятельности; 7) приказы по контингенту учащихся;		
	Зинькевич Светлана Юрьевна, социальный педагог			- Имеет доступ к личным делам обучающихся, информации на материальных носителях, содержащей персональные данные обучающихся, их родителей (законных представителей).	- сбор и систематизация - накопление и хранение - уточнение (обновление, изменение) - использование
	Антипова Мария Алексеевна, педагог-психолог			- Имеет доступ к личным делам обучающихся, информации на материальных носителях, содержащей персональные данные обучающихся, их родителей (законных представителей).	- сбор и систематизация - накопление и хранение - уточнение (обновление, изменение) - использование
	Бондарь Мария Михайловна, педагог-психолог				

	Черных Антон Сергеевич, заместитель директора по безопасности	персональные данные сотрудников, учащихся и их родителей (законных представителей)	1) сведения о состоянии здоровья учащихся; 2) электронная база данных учащихся школы; 3) приказы по основной деятельности; 4) приказы по контингенту учащихся; 5) медицинские книжки;		
	Коваленко Юрий Петрович, заместитель директора по хозяйственной работе	персональные данные сотрудников, учащихся и их родителей (законных представителей)	1) статистические отчеты; 2) приказы по основной деятельности; 3) приказы по личному составу сотрудников; 4) личные дела сотрудников школы		
	Агиевич Марина Михайловна, заведующий библиотекой	персональные данные сотрудников, учащихся и их родителей (законных представителей)	1) статистические отчеты; 2) электронная база данных учащихся школы; 3) приказы по основной деятельности; 4) приказы по контингенту учащихся;	- Имеет доступ к информации на материальных носителях (формуляр читателя библиотеки), содержащей персональные данные учащихся	- использование - хранение
	Аландаренко Марина Петровна, библиотекарь				
	Черных Сергей Сергеевич, преподаватель-организатор основ безопасности жизнедеятельности (ответственный за допризывную подготовку)	персональные данные учащихся допризывного возраста и их родителей (законных представителей)	1) сведения о состоянии здоровья обучающихся допризывного возраста; 2) личные дела учащихся допризывного возраста; 3) приказы по контингенту учащихся;	- Имеет доступ к личным делам обучающихся и информации на материальных носителях, содержащей персональные данные обучающихся допризывного возраста, всех сотрудников школы, в том числе военнообязанных	- сбор и систематизация - уточнение (обновление, изменение) - использование - уничтожение

	Бован Татьяна Николаевна, ответственная за пропускной режим	персональные данные сотрудников, учащихся и их родителей (законных представителей)	1) база данных учащихся школы; 2) приказы по основной деятельности; 3) приказы по контингенту учащихся		
	Королева Ольга Анатольевна, дистанционный лаборант компьютерного класса	в автоматизированной информационной системой управления сферой образования «Дневник.ru», персональные данные сотрудников, учащихся и их родителей (законных представителей)	1) электронная база данных учащихся школы; 2) электронная база данных сотрудников школы; 3) официальный сайт школы; 4) Дневник.ru 5) приказы по основной деятельности; 6) приказы по контингенту учащихся		
	Классные руководители 1 – 11 классов	персональные данные 1 -11 учащихся и их родителей (законных представителей)	1) личные дела учащихся; 2) классные журналы; 3) социальный паспорт класса; 4) паспортные и анкетные данные учащихся и их родителей (законных представителей) 5) приказы по основной деятельности; 6) приказы по контингенту учащихся	- Имеет доступ к личным делам обучающихся и информации на материальных носителях, содержащей персональные данные обучающихся только **своего класса**.	- сбор и систематизация - уточнение (обновление, изменение) - использование - уничтожение
	Педагоги дополнительного образования			- Имеет доступ к информации на материальных носителях (журнал работы объединения в системе дополнительного образования), содержащей персональные данные обучающихся и контактной информации родителей (законных представителей) обучающихся **своей группы (кружка, секции)**, детской общественной организации, органов детского самоуправления	- уточнение (обновление, изменение) - использование

	Учителя предметники			- Имеет доступ к информации на материальных носителях (классный журнал), содержащей персональные данные учащихся и контактной информации родителей учащихся классов, обучающихся предмету учителя.	- использование
	Старшие вожатые			- Имеет доступ к информации на материальных носителях (классные журналы) содержащие персональные данные обучающихся детской общественной организации, органов детского самоуправления	- использование

* Распространение (передача) информации, содержащей персональные данные, может быть осуществлена только с разрешения администрации школы в соответствии с Положением о порядке обработки и защиты персональных данных работников и учащихся МОУ «КСОШ №8» и в установленном действующим законодательством порядке.

Приложение № 2

Соглашение о неразглашении
персональных данных субъекта от сотрудника МОУ «КСОШ №8»

Я,_____ ,
(фамилия, имя, отчество)
паспорт серия_____ номер _____, выданный _____
_____ «____» _____ _____ года, понимаю, что получаю доступ к персональным данным работников МОУ «КСОШ № 8».

Я также понимаю, что во время исполнения своих обязанностей, мне приходится заниматься сбором, обработкой и хранением персональных данных.

Я понимаю, что разглашение такого рода информации может нанести ущерб субъектам персональных данных, как прямой, так и косвенный.

В связи с этим, даю обязательство, при работе (сбор, обработка и хранение) с персональными данными соблюдать все описанные в «Положении об обработке и защите персональных данных» требования.

Я подтверждаю, что не имею права разглашать сведения:

- анкетные и биографические данные;
- сведения об образовании;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- содержание трудового договора;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке, их аттестации;
- копии отчетов.

Я предупрежден (а) о том, что в случае разглашения мной сведений, касающихся персональных данных или их утраты я несу ответственность в соответствии со ст. 90 Трудового Кодекса Российской Федерации.

« ___ » _____ 20__ г. _____
(подпись)

Ссылки:
[1] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»: глава 1, ст. 3.
[2] Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», ст. 2.
[3] В законодательно определенных случаях может предусматриваться необходимость предъявления при заключении трудового договора дополнительных документов.
[4] ТК РФ, гл. 14, ст. 86, п. 3.
[5] ТК РФ, гл. 14, ст. 86, п. 4.
[6] ТК РФ, гл. 14, ст. 86, п. 5.
[7] ТК РФ, гл. 14, ст. 86, п. 1.
[8] ТК РФ, гл. 14, ст. 86, п. 2.
[9] ТК РФ, гл. 14, ст. 86, п. 6.
[10] ТК РФ, гл. 14, ст. 86, п. 7.
[11] ТК РФ, гл. 14, ст. 86, п. 8.
[12] ТК РФ, гл. 14, ст. 86, п. 9.
[13] ТК РФ, гл. 14, ст. 88.
[14] ТК РФ, гл. 14, ст. 87.
[15] Дата проставляется работником собственноручно.
[16] Регистрационный номер заявления проставляется сотрудником организации после регистрации документа.

Директору МОУ «КСОШ № 8»
Королевой Елене Анатольевне

от _____
(должность работника)

_____
(фамилия И.О. работника)

ЗАЯВЛЕНИЕ на обработку персональных данных

Я, _____
(фамилия, имя, отчество)

даю согласие *муниципальному общеобразовательному учреждению «Киришская средняя общеобразовательная школа № 8»* на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно - совершение действий, предусмотренных п. 3 ч. 1 ст. 3 Федерального закона от 27.07.2006 г. № 152 ФЗ «О персональных данных», содержащихся в настоящем заявлении, в целях обеспечения соблюдения трудового законодательства и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижения по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, а именно:
использовать все нижеперечисленные данные для оформления кадровых документов и для выполнения ОУ всех требований трудового законодательства; использовать мои персональные данные в информационной системе для осуществления расчетов работодателя со мной как работником; размещать мои фотографию, фамилию, имя и отчество на доске почета, на стендах в помещении ОУ, на сайте ОУ;

1. Ф.И.О. _____
2. Дата рождения, место рождения: _____
3. Паспорт: серия _____ № _____ выдан (когда) _____
   (кем) _____
4. Адрес регистрации: _____
   _____
5. Адрес фактического проживания: _____
   _____
6. Контактный телефон (домашний, мобильный): _____
7. E-mail: _____
8. ИНН: _____
9. СНИЛС: _____
10. Документ об образовании _____
    _____
11. Военный билет (при наличии): _____
    _____
12. Иные документы: _____
    _____
    _____
    _____
    _____

Об ответственности за достоверность представленных сведений предупрежден(а).

Настоящее согласие действительно со дня его подписания до окончания срока работы или до дня отзыва согласия в письменной форме.

_____ _____
(дата) (подпись)

Приложение №4

Отзыв согласия на обработку персональных данных

Директору МОУ «КСОШ № 8»
Королевой Елене Анатольевне

_____
Ф.И.О. субъекта персональных данных

_____
Адрес, где зарегистрирован субъект персональных данных

_____
Номер основного документа, удостоверяющего его личность

_____
Дата выдачи указанного документа

_____
Наименование органа, выдавшего документ

Заявление

Прошу Вас прекратить обработку моих персональных данных в связи с

_____
(указать причину)

«__»_____ 20__ г. _____ _____
(подпись) (расшифровка подписи)

ПОЛОЖЕНИЕ
о защите, хранении, обработке и передаче персональных данных обучающихся
МОУ «КСОШ № 8»

Настоящее Положение разработано на основании Конституции Российской Федерации, Федерального закона от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных», Федерального закона от 27 июля 2006 г. № 152-ФЗ «Об информации, информационных технологиях и о защите информации» и Постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» с целью обеспечения уважения прав и основных свобод каждого обучающегося при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1. Общие положения

1.1. Персональные данные обучающегося – сведения о фактах, событиях и обстоятельствах жизни обучающегося, позволяющие идентифицировать его личность, необходимые администрации МОУ «КСОШ № 8» (далее – администрация школы) в связи с отношениями обучения и воспитания обучающегося и касающиеся обучающегося.

1.2. К персональным данным обучающегося относятся:

- сведения, содержащиеся в свидетельстве о рождении, паспорте или ином документе, удостоверяющем личность;
- информация, содержащаяся в личном деле обучающегося;
- информация, содержащаяся в личном деле обучающегося, лишенного родительского попечения;
- сведения, содержащиеся в документах воинского учета (при их наличии);
- информация об успеваемости;
- информация о состоянии здоровья;
- документ о месте проживания;
- иные сведения, необходимые для определения отношения обучения и воспитания.

1.3. Администрация школы может получить от самого обучающегося данные о:

- фамилии, имени, отчестве, дате рождения, месте жительства обучающегося;
- фамилии, имени, отчестве родителей (законных представителей) обучающегося.

Иные персональные данные обучающегося, необходимые в связи с отношениями обучения и воспитания, администрация школы может получить только с письменного согласия одного из родителей (законного представителя). К таким данным относятся документы, содержащие сведения, необходимые для предоставления обучающемуся гарантий и компетенций, установленным действующим законодательством:

- документы о составе семьи;
- документы о состоянии здоровья (сведения об инвалидности, о наличии хронических заболеваний и т.п.);
- документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (родители-инвалиды, неполная семья, ребенок-сирота и т.п.).

В случаях, когда администрация школы может получить необходимые персональные данные обучающегося только у третьего лица, администрация школы должна уведомить об этом одного из родителей (законного представителя) заранее и получить от него письменное согласие.

1.4. Администрация школы обязана сообщить одному из родителей (законному представителю) о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа одного из родителей (законного представителя) дать письменное согласие на их получение.

1.5. Персональные данные обучающегося являются конфиденциальной информацией и не могут быть использованы администрацией школы или любым иным лицом в личных целях.
1.6. При определении объема и содержания персональных данных обучающегося администрация руководствуется Конституцией Российской Федерации, федеральными законами и настоящим Положением.

2. Хранение, обработка и передача персональных данных обучающегося

2.1. Обработка персональных данных обучающегося осуществляется для обеспечения соблюдения законов и иных нормативных правовых актов в целях воспитания и обучения обучающегося, обеспечения его личной безопасности, контроля качества образования, пользования льготами, предусмотренными законодательством Российской Федерации и локальными актами школы.
2.2. Право доступа к персональным данным обучающегося имеют:
- работники управления образования (при наличии соответствующих полномочий, установленных приказом управления образования);
- директор школы;
- заместители директора по учебно-воспитательной, учебно-методической, воспитательной работе;
- секретарь-делопроизводитель школы;
- классные руководители (только к персональным данным обучающихся своего класса);
- библиотекарь, социальный педагог, педагог-психолог, преподаватель-организатор ОБЖ, допризывной подготовки, старшая вожатая;
- медицинский работник.

2.3. Директор школы осуществляет приём обучающегося в школу. Директор школы может передавать персональные данные обучающегося третьим лицам, только если это необходимо в целях предупреждения угрозы жизни и здоровья обучающегося, а также в случаях, установленных федеральными законами.
2.4. Секретарь-делопроизводитель:
- принимает или оформляет вновь личное дело обучающегося и вносит в него необходимые данные;
- предоставляет свободный доступ родителям (законным представителям) обучающегося к персональным данным на основании письменного заявления, к которому прилагается копия документа, удостоверяющего личность, и копия документа, подтверждающего полномочия законного представителя;
- не имеет права предоставлять информацию об обучающемся родителю (законному представителю) лишенному или ограниченному в родительских правах на основании вступившего в законную силу постановления суда.

2.5. При передаче персональных данных обучающихся сотрудники школы, имеющие право доступа к персональным данным, обязаны не сообщать персональные данные обучающегося или его родителей (законных представителей) без письменного согласия одного из родителей (законного представителя), за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью обучающегося, а также в случаях, установленных федеральным законом.
2.6. Все сотрудники школы, имеющие доступ к персональным данным обучающихся и их родителей (законных представителей) предупреждаются об ответственности за их разглашение.
2.7. При передаче персональных данных обучающегося директор, секретарь-делопроизводитель, заместители директора по учебно-воспитательной, учебно-методической, воспитательной работе, классные руководители, социальный педагог, педагог-психолог, преподаватель-организатор ОБЖ, допризывной подготовки, старшая вожатая, медицинский работник школы обязаны:
- предупредить лиц, получающих данную информация, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены;
- потребовать от этих лиц письменное подтверждение соблюдения этого условия.

2.8. Иные права, обязанности, действия работников, в трудовые обязанности которых входит обработка персональных данных обучающегося, определяются трудовыми договорами и должностными инструкциями.
2.9. Все сведения о передаче персональных данных обучающихся регистрируются в Журнале учета передачи персональных данных обучающихся школы в целях контроля правомерности использования данной информации лицами, её получившими.

3. Обязанности работников, имеющих доступ к персональным данным обучающегося, по их хранению и защите

3.1. Работники, имеющие доступ к персональным данным обучающегося, обязаны:
3.1.1. Не сообщать персональные данные обучающегося третьей стороне без письменного согласия одного из родителей (законного представителя), кроме случаев, когда в соответствии с федеральными законами такого согласия не требуется;
3.1.2. Использовать персональные данные обучающегося, полученные только от него лично или с письменного согласия одного из родителей (законного представителя);
3.1.3. Обеспечить защиту персональных данных обучающегося от их неправомерного использования или утраты, в порядке, установленном законодательством Российской Федерации;
3.1.4. Ознакомить родителя (родителей) или законного представителя с настоящим Положением и их правами и обязанностями в области защиты персональных данных, под роспись; соблюдать требования конфиденциальности персональных данных обучающегося;
3.1.5. Исключать или исправлять по письменному требованию одного из родителей (законного представителя) обучающегося его недостоверные или неполные персональные данные, а также данные, обработанные с нарушением требований законодательства;
3.1.6. Ограничивать персональные данные обучающегося при передаче уполномоченным работникам правоохранительных органов или работникам управления образования только той информацией, которая необходима для выполнения указанными лицами их функций;
3.1.7. Запрашивать информацию о состоянии здоровья обучающегося только у родителей (законных представителей);
3.1.8. Обеспечить обучающемуся или одному из его родителей (законному представителю) свободный доступ к персональным данным обучающегося, включая право на получение копий любой записи, содержащей его персональные данные;
3.1.9. Предоставлять по требованию одного из родителей (законного представителя) обучающегося полную информацию о его персональных данных и обработке этих данных.
3.2. Лица, имеющие доступ к персональным данным обучающегося, не вправе:
3.2.1. Получать и обрабатывать персональные данные обучающегося о его религиозных и иных убеждениях, семейной или личной жизни;
3.2.2. Предоставлять персональные данные обучающегося в коммерческих целях.
3.3. При принятии решений затрагивающих интересы обучающегося, администрации школы запрещается основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

4. Права и обязанности обучающегося, родителя (законного представителя)

4.1. В целях обеспечения защиты персональных данных, хранящихся у администрации школы, обучающийся, родитель (законный представитель) имеют право на;
4.1.1. Требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований законодательства. При отказе администрации школы исключить или исправить персональные данные обучающегося родитель (законный представитель) имеет право заявить в письменной форме администрации школы о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера родитель (законный представитель) имеет право дополнить заявлением, выражающим его собственную точку зрения;
4.1.2. Требование об извещении администрацией школы всех лиц, которым ранее были сообщены неверные или неполные персональные данные обучающегося, обо всех произведенных в них исключениях, исправлениях или дополнениях;
4.1.3. Обжалование в суд любых неправомерных действий или бездействий администрации школы при обработке и защите персональных данных обучающегося;

4.1.4. Возмещение убытков и (или) компенсацию морального вреда в судебном порядке.
4.2. Родитель (законный представитель) обязан сообщать администрации школы сведения, которые могут повлиять на принимаемые администрацией школы решения в отношении обучающегося.

5. Хранение персональных данных обучающегося

5.1. Должны храниться в запирающемся шкафу на бумажных носителях и на электронных носителях с ограниченным доступом документы:

- поступившие от родителя (законного представителя);
- сведения об обучающемся, поступившие от третьих лиц с письменного согласия родителя (законного представителя);
- иная информация, которая касается отношений обучения и воспитания обучающегося.

6. Ответственность администрации школы и её сотрудников.

6.1. Защита прав обучающегося, установленных законодательством Российской Федерации и настоящим Положением, осуществляется судом в целях пресечения неправомерного использования персональных данных обучающегося, восстановления нарушенных прав и возмещения причиненного ущерба, в том числе морального вреда.
6.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных обучающегося, привлекаются к дисциплинарной и материальной ответственности, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Приложение № 6

Соглашение о неразглашении
персональных данных субъекта
(обучающегося или родителя (законного представителя))

Я,_____ ,
(фамилия, имя, отчество)
паспорт серия_____ номер _____, выданный _____
_____ «____» _____ _____ года, понимаю, что получаю доступ к персональным данным обучающихся и их родителей (законных представителей) МОУ «КСОШ № 8».

Я также понимаю, что во время исполнения своих обязанностей, мне приходится заниматься сбором, обработкой и хранением персональных данных.

Я понимаю, что разглашение такого рода информации может нанести ущерб субъектам персональных данных, как прямой, так и косвенный.

В связи с этим, даю обязательство, при работе (сбор, обработка и хранение) с персональными данными соблюдать все описанные в «Положении об обработке и защите персональных данных» требования.

Я подтверждаю, что не имею права разглашать сведения:

- ✓ ФИО;
- ✓ домашний адрес;
- ✓ адрес электронной почты;
- ✓ фото;
- ✓ номер мобильного телефона;
- ✓ сведения об успеваемости и достижениях учащегося;
- ✓ сведения о соблюдении учащимися внутреннего распорядка школы;
- ✓ сведения о жилищно-бытовых условиях проживания;
- ✓ номер медицинского полиса;
- ✓ сведения о состоянии здоровья;
- ✓ данные медицинских осмотров, заключения и рекомендации врачей;
- ✓ сведения об установлении инвалидности.

Я подтверждаю, что не имею право разглашать сведения о родителях (законных представителях) обучающихся Школы:

- ✓ ФИО;
- ✓ домашний адрес;
- ✓ номера телефонов (домашний, служебный, мобильный);
- ✓ место работы и занимаемой должности.

Я предупрежден (а) о том, что в случае разглашения мной сведений, касающихся персональных данных или их утраты я несу ответственность в соответствии со ст. 90 Трудового Кодекса Российской Федерации.

« ___ » _____ 20__ г. _____
(подпись)

Инструкция
по обеспечению безопасности персональных данных

1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии со ст. 19 Федерального закона РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных», на основании Федерального закона РФ от 27.07.2007 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановления Правительства РФ от 17.01.2007 г. № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности РФ (ФСБ России), Министерства информационных технологий и связи РФ (Мининформсвязи России) от 13.02.2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных», Письма Федерального агентства по образованию № ФАО-6748/52/17-02-09/72 «Об обеспечении безопасности персональных данных», Положения о работе с персональными данными работников и учащихся.

1.2. Для обеспечения безопасности персональных данных необходимо исключить несанкционированный, в том числе случайный, доступ к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

1.3. Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров.

1.4. Ответственность за безопасность персональных данных возлагается на лиц, допущенных к их обработке.

2. Обеспечение безопасности перед началом обработки персональных данных

2.1. Перед началом обработки персональных данных необходимо изучить настоящую Инструкцию.

2.2. Перед началом обработки персональных данных необходимо убедиться в том, что:

- средства защиты персональных данных соответствуют классу информационной системы;
- в помещении, в котором ведется работа с персональными данными, отсутствуют посторонние лица;
- носители персональных данных не повреждены;
- к персональным данным не был осуществлен несанкционированный доступ;
- персональные данные не повреждены;
- технические средства автоматизированной обработки и защиты персональных данных находятся в исправном состоянии.

3. Обеспечение безопасности во время обработки персональных данных

3.1. Во время обработки персональных данных необходимо обеспечить:

- недопущения воздействия на технические средства автоматизированной обработки персональных данных, способного нарушить их функционирование;
- недопущение нахождения в помещении, в котором ведется работа с персональными данными, посторонних лиц;
- постоянный контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- недопущение несанкционированного доступа к персональным данным;
- конфиденциальность персональных данных.

4. Обеспечение безопасности в экстремальных ситуациях

4.1. При модификации или уничтожения персональных данных, вследствие несанкционированного доступа к ним необходимо обеспечить возможность их незамедлительного восстановления.

4.2. При нарушении порядка предоставления персональных данных пользователям информационной системы необходимо приостановить их предоставление.
4.3. При обнаружении несанкционированного доступа к персональным данным необходимо немедленно прервать этот доступ.
4.4. В случае несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных необходимо произвести разбирательство и составление заключений по данным фактам, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.
4.5. Обо всех экстремальных ситуациях необходимо немедленно поставить в известность директора школы и произвести разбирательство.

5. Обеспечение безопасности при завершении обработки персональных данных

5.1. После завершения сеанса обработки персональных данных необходимо обеспечить:
- исключение возможности несанкционированного проникновения или нахождения в помещении, в котором размещены информационные системы и ведется работа с персональными данными;
- работоспособность средств защиты информации, функционирующих при отсутствии лиц, допущенных к обработке персональных данных;
- фиксацию всех случаев нарушения данной инструкции в журнале.

6. Заключительные положения

6.1. Проверка и пересмотр настоящей инструкции осуществляются в следующих случаях:
- при пересмотре межотраслевых и отраслевых требований обеспечения безопасности персональных данных;
- при внедрении новой техники и (или) технологий;
- по результатам анализа материалов расследования нарушений требований законодательства об обеспечении безопасности персональных данных;
- по требованию представителей Федеральной службы безопасности.

Ответственность за своевременную корректировку настоящей инструкции возлагается на директора школы.

ИНСТРУКЦИЯ
администратора информационных систем персональных данных МОУ «КСОШ № 8»

1. Общие положения

1.1. Администратор информационных систем персональных данных (ИСПДн) (далее – Администратор) назначается приказом директора МОУ «КСОШ № 8», на основании Положение о разграничении прав доступа к обрабатываемым персональным данным.
1.2. Администратор подчиняется директору школы.
1.3. Администратор в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами МОУ «КСОШ № 8».
1.4. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты при обработке персональных данных.

2. Должностные обязанности

Администратор обязан:
2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.
2.2. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:
- программного обеспечения автоматизированных рабочих мест (АРМ) и серверов (операционные системы, прикладное и специальное программное обеспечение (ПО));
- аппаратных средств;
- аппаратных и программных средств защиты.

2.3. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.
2.4. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.
2.5. Обеспечивать функционирование и поддерживать работоспособность средств защиты.
2.6. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.
2.7. Проводить периодический контроль принятых мер по защите, в пределах, возложенных на него функций.
2.8. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля Оператором ИСПДн.
2.9. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.
2.10. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.
2.11. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.
2.12. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и

хранения информации. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку.

2.13. Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.

2.14. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3. Права и ответственность администратора ИСПДн

3.1. Администратор ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн, в том числе производить установку и настройку элементов ИСПДн, контролировать и поддерживать работоспособность ИСПДн и выполнять прочие действия в рамках должностных обязанностей.

3.2. Администраторы ИСПДн, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального закона РФ 27.07.2006 г. N 152-ФЗ "О персональных данных" и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных (ИСПДн) в МОУ «КСОШ № 8»

1. Общие положения

1.1. Пользователь информационных систем персональных данных (ИСПДн) (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

1.2. Пользователем является каждый сотрудник МОУ «КСОШ № 8», участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами МОУ «КСОШ № 8».

1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

2. Должностные обязанности

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики.

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других.

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью МОУ «КСОШ № 8», а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться в МОУ «КСОШ № 8» по электронной почте: school8_kirishi@mail.ru или по телефону 587-41.

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн.

2.9. Пользователям запрещается:

- разглашать защищаемую информацию третьим лицам;
- копировать защищаемую информацию на внешние носители без разрешения своего руководителя;
- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- несанкционированно открывать общий доступ к папкам на своей рабочей станции;
- запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;
- отключать (блокировать) средства защиты информации;

- обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;
- привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

2.10. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

2.11. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

3. Организация парольной защиты

3.1. Личные пароли доступа к элементам ИСПДн выдаются пользователям Администратором информационной безопасности, Администратором ИСПДн или создаются самостоятельно.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3. Правила формирования пароля:

- пароль не может содержать имя учетной записи пользователя или какую-либо его часть;
- пароль должен состоять не менее чем из 6 символов;
- в пароле должны присутствовать символы трех категорий из числа следующих четырех:

1) прописные буквы английского алфавита от A до Z;
2) строчные буквы английского алфавита от a до z;
3) десятичные цифры (от 0 до 9);
4) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

- запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;
- запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
- запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
- запрещается выбирать пароли, которые уже использовались ранее.

3.4. Правила ввода пароля:

- ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;
- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.5. Правила хранение пароля:

- запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;
- запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.6. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;
- своевременно сообщать Администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. Правила работы в сетях общего доступа и (или) международного обмена

4.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

4.2. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус и других);
- передавать по Сети защищаемую информацию без использования средств шифрования;
- запрещается скачивать из Сети программное обеспечение и другие файлы;
- запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты, содержащие нелегально распространяемое ПО и другие);
- запрещается нецелевое использование подключения к Сети.

5. Права и ответственность пользователей ИСПДн

5.1. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.

5.2. Пользователи, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального закона РФ 27.07.2006 г. N 152-ФЗ "О персональных данных" и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Приложение 10

ИНСТРУКЦИЯ
пользователя ИСПДн по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций

1. Назначение и область действия

1.1. Настоящая инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн МОУ «КСОШ № 8», меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

1.2. Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

1.3. Задачей настоящей Инструкции является:

- определение мер защиты от прерывания;
- определение действий восстановления в случае прерывания.

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

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

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

2. Порядок реагирования на аварийную ситуацию

2.1. Действия при возникновении аварийной ситуации

2.1.1. В настоящем документе под аврийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн. Аварийная ситуации становится возможной в результате реализации одной из угроз, приведенных в таблице «Источники угроз».

Источники угроз

	Технологические угрозы
1	Пожар в здании
2	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
3	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
4	Химический выброс в атмосферу
	Внешние угрозы
5	Массовые беспорядки
6	Сбои общественного транспорта
7	Эпидемия
8	Массовое отравление персонала
	Стихийные бедствия
9	Удар молнии
10	Сильный снегопад
11	Сильные морозы
12	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
13	Затопление водой в период паводка
14	Наводнение, вызванное проливным дождем

15	Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)
	Телекоммуникационные и ИТ угрозы
16	Сбой системы кондиционирования
17	Сбой ИТ – систем
	Угроза, связанная с человеческим фактором
18	Ошибка персонала, имеющего доступ к серверной
19	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
	Угрозы, связанные с внешними поставщиками
20	Отключение электроэнергии
21	Сбой в работе Интернет-провайдера
22	Физический разрыв внешних каналов связи

2.1.2. Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю».
2.1.3. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Школы (Администратор безопасности, Администратор и Оператор ИСПДн) предпринимают меры по восстановлению работоспособности системы. Принимаемые меры по возможности согласуются с вышестоящим руководством. По мере необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

2.2. Уровни реагирования на инцидент

При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

- **Уровень 1 – Незначительный инцидент.** Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.
- **Уровень 2 – Авария.** Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:
1. Отказ элементов ИСПДн и средств защиты из-за:
   - повреждения водой (провыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;
   - сбоя системы кондиционирования.
2. Отсутствие Администратора ИСПДн и Администратора безопасности более чем на сутки из-за:
   - химического выброса в атмосферу;
   - сбоев общественного транспорта;
   - эпидемии;
   - массового отравления персонала;
   - сильного снегопада;
   - сильных морозов.

- **Уровень 3 – Катастрофа.** Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относятся обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к неработоспособности ИСПДн и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты:
- пожар в здании;
- взрыв;
- просадка грунта с частичным обрушением здания;

- массовые беспорядки в непосредственной близости от объекта.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций

3.1. Технические меры

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

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

Системы жизнеобеспечения ИСПДн включают:

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

3.1.2. Все критические помещения МБОУ - СОШ № 2 (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.1.3. Порядок предотвращения потерь информации и организации системы жизнеобеспечения ИСПДн описан в Порядке резервирования и восстановления работоспособности технических систем и программного обеспечения, баз данных и средств защиты информации.

3.2. Организационные меры

3.2.1. Ответственные за реагирование сотрудники ознакомляют всех сотрудников МБОУ - СОШ № 2, находящихся в их зоне ответственности, с данной Инструкцией в срок, не превышающий трех рабочих дней с момента выхода нового сотрудника на работу. По окончании ознакомления сотрудник расписывается в листе ознакомления. Подпись сотрудника должна соответствовать его подписи в документе, удостоверяющем его личность.

3.2.2. Должно быть проведено обучение должностных лиц МБОУ - СОШ № 2, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

- оказание первой медицинской помощи;
- пожаротушение;
- эвакуация людей;
- защита материальных и информационных ресурсов;
- методы оперативной связи со службами спасения и лицами, ответственными за реагирование на аварийную ситуацию;
- выключение оборудования, электричества, водоснабжения.

3.2.3. Администраторы ИСПДн и Администраторы безопасности должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.

Приложение 11

ИНСТРУКЦИЯ
по организации антивирусной защиты в МОУ «КСОШ № 8»

1. Настоящая Инструкция определяет требования к организации защиты по организации антивирусной защиты в МОУ «КСОШ № 8» (далее Школа) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников Школы за их выполнение.
2. К использованию в Школе допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.
3. Установка средств антивирусного контроля на компьютерах осуществляется уполномоченным сотрудником Школы. Настройка параметров средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств.
4. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов.
5. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, CD-ROM и т.п.).
6. Контроль входящей и исходящей информации на защищаемых серверах и персональных компьютерах (далее ПК) осуществляется непрерывно посредством постоянно работающего компонента антивирусного программного обеспечения («монитора»). Полная проверка информации, хранящейся на серверах и ПК должна осуществляться не реже одного раза в месяц.
7. Обновление баз вирусов антивирусного программного обеспечения, установленного на ПК и серверах, должно осуществляться еженедельно.
8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена антивирусная проверка:

- на защищаемом автоматизированном рабочем месте (АРМ) - ответственным за обеспечение информационной безопасности.

9. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник Школы самостоятельно или вместе с ответственным за антивирусную защиту Школы должен провести внеочередной антивирусный контроль своей рабочей станции.
10. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и ответственного за антивирусную защиту Школы, владельца зараженных файлов, а также сотрудников, использующих эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

11. Ответственность за организацию антивирусного контроля в Школе, в соответствии с требованиями настоящей Инструкции возлагается на руководителя Школы.
12. Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на ответственного за антивирусную защиту Школы и всех сотрудников, являющихся пользователями ПК Школы.
13. Периодический контроль за состоянием антивирусной защиты в Школе, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками подразделений Школы осуществляется ответственным за антивирусную защиту Школы.