Приложение №1 к приказу
директора МКОУ СОШ № 8
с.Садового
от 22.10.2020 г. № 50

Положение о порядке обработки персональных данных
детей и родителей (законных представителей)
в МКОУ СОШ № 8 с.Садового

I. Общие положения

1. Настоящее Положение разработано на основании Федерального закона от 27 июля 2006 №152-ФЗ «О персональных данных», Федерального закона от 27 июля 2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» и Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным Постановлением Правительства Российской Федерации от 01.11.2012 № 1119, и Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным Постановлением Правительства Российской Федерации от 15.09.2008 № 687 с целью обеспечения прав и основных свобод каждого учащегося, при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

2. Персональные данные учащихся, родителей (законных представителей) - это сведения о фактах, событиях и обстоятельствах жизни учащихся, позволяющие идентифицировать его личность, необходимые администрации МКОУ СОШ № 8 с.Садового (далее – Администрация) в связи с отношениями обучения и воспитания учащихся.

3. К персональным данным учащегося относятся: Фамилия, имя, отчество, Дата, месяц, год рождения, Место рождения, Адрес, Образование, Данные страхового полиса обязательного пенсионного страхования, Сведения о социальных льготах, Паспортные данные или свидетельства о рождении, ИНН, Адрес электронной почты, Телефон (домашний, сотовый), Результаты успеваемости и тестирования; О состоянии здоровья, Фотография.

4. К персональным данным родителей, законных представителей относятся: Фамилия, имя, отчество, Дата, месяц, год рождения, Место рождения, Адрес, Семейное положение, Социальный статус, Профессия, образование, Должность, Сведения о социальных льготах, Паспортные данные, Адрес электронной почты, Телефон (домашний, сотовый),Фамилия, имя отчество, дата рождения детей.

5. Администрация может получить от самого учащегося данные о:

- фамилии, имени, отчестве, дате рождения, месте жительстве

учащегося,

- фамилии, имени, отчестве родителей (законных представителей) учащегося.

6. Иные персональные данные учащегося, необходимые в связи с отношениями обучения и воспитания, администрация может получить только с письменного согласия одного из родителей (законного представителя). К таким данным относятся документы, содержащие сведения, необходимые для предоставления учащемуся гарантий и компенсаций, установленных действующим законодательством.

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

8. Администрация 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.

9. Персональные данные учащегося, родителей (законных представителей) являются конфиденциальной информацией и не могут быть использованы администрацией или любым иным лицом в личных целях.

10. При определении объема и содержания персональных данных учащегося, родителей (законных представителей) администрация руководствуется Конституцией Российской Федерации, федеральными законами и настоящим Положением.

II. Хранение, обработка и передача персональных данных учащегося, родителей (законных представителей)

1. Обработка персональных данных учащегося, родителей (законных представителей) осуществляется для обеспечения соблюдения законов и иных нормативных правовых актов в целях воспитания и обучения учащегося, обеспечения его личной безопасности, контроля качества образования, пользования льготами, предусмотренными законодательством Российской Федерации и локальными актами администрации.

2. Право доступа к персональным данным учащегося (родителей (законных представителей)) имеют:

- Руководитель учреждения;
- ответственный за обработку персональных данных в учреждении;
- должностное лицо, ответственное за ведение личных дел учащихся;
- заместитель директора по учебной части;
- преподаватель учащегося;
- отдел образования администрации Арзгирского муниципального района;

3. Руководитель осуществляет прием учащегося в учреждение.

4. Руководитель может передавать персональные данные учащегося, родителей (законных представителей) третьим лицам, только если это необходимо в целях предупреждения угрозы жизни и здоровья учащегося, а

также в случаях, установленных федеральными законами.

5. Должностное лицо, ответственное за ведение личных дел учащихся:

- принимает личное дело учащегося и вносит в него необходимые данные;
- предоставляет доступ родителям (законным представителям) к персональным данным учащегося на основании письменного заявления.

К заявлению прилагается:

- копия документа, удостоверяющего личность;
- копия документа, подтверждающего полномочия законного представителя.

6. Не имеет права получать информацию об учащемся родитель (законный представитель), лишенный или ограниченный в родительских правах на основании вступившего в законную силу постановления суда.

7. Экономист имеет право доступа к персональным данным учащегося, родителей (законных представителей) в случае, когда исполнение им своих трудовых обязанностей по отношению к учащемуся (предоставление льгот, установленных законодательством) зависит от знания персональных данных учащегося.

8. При передаче персональных данных учащегося ответственные должностные лица обязаны предупредить лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены.

9. Иные права, обязанности, действия работников, в трудовые обязанности которых входит обработка персональных данных учащегося, родителей (законных представителей), определяются трудовыми договорами и должностными инструкциями.

10. Все сведения о передаче персональных данных учащихся регистрируются в Журнале учета передачи персональных данных учащихся образовательного учреждения в целях контроля правомерности использования данной информации лицами, ее получившими.

III. Обязанности работников, имеющих доступ к персональным данным учащегося, по их хранению и защите

1. Работники, имеющие доступ к персональным данным учащегося, обязаны:

- не сообщать персональные данные учащегося третьей стороне без письменного согласия одного из родителей (законного представителя), кроме случаев, когда в соответствии с федеральными законами такого согласия не требуется;
- использовать персональные данные учащегося, полученные только от него лично или с письменного согласия одного из родителей (законного представителя);
- обеспечить защиту персональных данных учащегося от их неправомерного использования или утраты, в порядке, установленном законодательством Российской Федерации;
- ознакомить родителя (родителей) или законного представителя с настоящим Положением и их правами и обязанностями в области защиты

персональных данных, под роспись;

- соблюдать требование конфиденциальности персональных данных учащегося;
- исключать или исправлять по письменному требованию одного из родителей (законного представителя) учащегося его недостоверные или неполные персональные данные, а также данные, обработанные с нарушением требований законодательства;
- ограничивать персональные данные учащегося при передаче уполномоченным работникам правоохранительных органов или работникам отдела образования администрации Арзгирского муниципального района только той информацией, которая необходима для выполнения указанными лицами их функций;
- запрашивать информацию о состоянии здоровья учащегося только у родителей (законных представителей);
- обеспечить учащемуся или одному из его родителей (законному представителю) свободный доступ к персональным данным учащегося, включая право на получение копий любой записи, содержащей его персональные данные;
- предоставить по требованию одного из родителей (законного представителя) учащегося полную информацию о его персональных данных и обработке этих данных.

2. Лица, имеющие доступ к персональным данным учащегося, не вправе:

- получать и обрабатывать персональные данные учащегося о его религиозных и иных убеждениях, семейной и личной жизни;
- предоставлять персональные данные учащегося в коммерческих целях.

3. При принятии решений, затрагивающих интересы учащегося, администрации запрещается основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

IV. Права и обязанности учащегося, родителя (законного представителя)

1. В целях обеспечения защиты персональных данных, хранящихся у администрации, учащихся, родитель (законный представитель) имеют право на:

- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований законодательства. При отказе администрации исключить или исправить персональные данные учащегося родитель (законный представитель) имеет право заявить в письменной форме администрации о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера родитель (законный представитель) имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требование об извещении администрацией всех лиц, которым ранее были сообщены неверные или неполные персональные данные об

учащемся, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжалование в суд любых неправомерных действий или бездействия администрации при обработке и защите персональных данных учащегося;
- возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

2. Родитель (законный представитель) обязан сообщать администрации сведения, которые могут повлиять на принимаемые администрацией решения в отношении учащегося.

V. Хранение персональных данных учащегося

Должны храниться в сейфе на бумажных носителях и на электронных носителях с ограниченным доступом документы:

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

VI. Ответственность администрации и ее сотрудников

1. Защита прав учащегося, установленных законодательством Российской Федерации и настоящим Положением, осуществляется судом в целях пресечения неправомерного использования персональных данных учащегося, восстановления нарушенных прав и возмещения причиненного ущерба, в том числе морального вреда.

2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных учащегося, привлекаются к дисциплинарной и материальной ответственности, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами

Приложение №2 к приказу
директора МКОУ СОШ № 8
с.Садового
от 22.10.2020 г. № 50

ПОЛОЖЕНИЕ
о разграничении прав доступа к персональным данным в МКОУ СОШ № 8 с.Садового

1. Общие положения

1. Настоящее Положение разработано на основании Федерального закона от 27 июля 2006 №152-ФЗ «О персональных данных», Федерального закона от 27 июля 2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» и Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным Постановлением Правительства Российской Федерации от 01.11.2012 № 1119, и Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным Постановлением Правительства Российской Федерации от 15.09.2008 № 687 с целью обеспечения прав и основных свобод каждого обучающегося, при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

2. Основные понятия

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 руководителю учреждения в связи с трудовыми отношениями;
- ***персональные данные учащихся*** - информация, необходимая учреждению в связи с отношениями, возникающими между учащимся, его родителями (законными представителями) и учреждением.
- ***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 Учреждения в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников (учащихся) 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 (учащемуся);
- ***информация*** - сведения (сообщения, данные) независимо от формы их представления;

3. Разграничения прав доступа при автоматизированной обработке персональных данных

1.Разграничение прав осуществляется на основании Отчета по результатам проведения внутренней проверки, а так же исходя из характера и режима обработки персональных данных.

2. Список групп должностных лиц, ответственных за обработку персональных данных в информационных системах персональных данных, а так же их уровень прав доступа в базы данных), представлен в таблице № 1

Таблица №1:

№ п/п	Группа/уровень доступа	Занимаемая должность	Цели обработки персональных данных	Перечень информационных автоматизированных систем обработки персональных данных	Перечень персональных данных, подлежащих обработке
1	Администратор/Обладает полной информацией о системном и прикладном программном обеспечении. - Обладает полной информацией о технических средствах и конфигурации. - Имеет доступ ко всем техническим средствам обработки информации и данным. - Обладает правами конфигурирования и административной настройки технических средств.	Администрация школы , секретарь	Исполнение закона об (предоставление родителям (законным представителям) информации о школе, данных успеваемости учащихся в электронном виде)	электронная база школы.	Персональные данные работников и персональные данные учащихся
2	Пользователи/ Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к определённым группам ПДн.(школа, класс)	Администрация школы, преподаватели, социальный педагог	Исполнение закона об (предоставление родителям (законным представителям) информации о школе, данных успеваемости учащихся в электронном виде)	электронная база школы	Персональные данные работников и персональные данные учащихся
3	Отдел кадров/ Обладает всеми необходимыми	секретарь	Исполнение закона об (предоставление	электронная база школы,	Персональные данные работников и персональные данные

	атрибутами и правами, обеспечивающими доступ ко всем ПДн.		родителям (законным представителям) информации о школе, данных успеваемости учащихся в электронном виде)	кадры	учащихся
4	Бухгалтерия	Директор, завхоз, кладовщик, бухгалтер	Формирование платежных поручений, содержащих персональные данные, исполнение договоров, стороной по которому является субъект персональных данных, отправка бухгалтерской и налоговой отчетности	Электронная отчётность, кадры	Персональные данные работников и персональные данные учащихся

4.Разграничения прав доступа при неавтоматизированной обработке персональных данных

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

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

Таблица № 2:

№	Группа	Занимаемая должность	Цели обработки персональных данных	Перечень информационных и неавтоматизированных систем персональных данных	Перечень персональных данных, подлежащих обработке
	Делопроизводство Уровень доступа к ПДн	секретарь	Исполнение трудового законодательства, организация кадрового учета на предприятии, табельный учет	кадровый учет	Персональные данные работников и персональные данные учащихся

	Администрация школы/ Уровень доступа к ПДн: Обладает полной информацией о персональных данных учащихся и их родителей, работников школы. - Имеет доступ к личным делам учащихся и работников, информации на материальных носителях, содержащей персональные данные учащихся, их родителей (законных представителей) и работников школы	Директор, заместители директора по учебной и воспитательной работе	Управление учебным процессом. Осуществление контакта с родителями (законными представителями). Исполнение трудового законодательства. Сбор и обработка персональных данных связанных изменениями квалификационных характеристик работников школы. Передача данных в ОО АА МР СК	Движение. Расписание. Посещаемость. Успеваемость. Сайт школы.	Персональные данные работников и персональные данные учащихся.
			Сбор и подготовка документов учащихся для участия в мероприятиях различного уровня.	Воспитательная работа	Персональные данные работников и персональные данные учащихся: ФИО, дата и место рождения, адрес, образование, паспортные данные,
		заместитель директора по учебной работе, секретарь	Организация кадрового учета в учреждении.	Информационные технологии в школе.	ФИО, дата и место рождения, адрес, образование и специальность, профессия, должность, паспортные данные, ИНН, данные страхового полиса обязательного пенсионного страхования, трудовой и общий стаж, данные о предыдущих местах работы, курсах повышения квалификации.
		Завхоз	Исполнение трудового законодательства. Заключение договоров о материальной ответственности.	Учет материальных ценностей.	Персональные данные работников: Ф.И.О., дату, месяц, год рождения, занимаемую должность. Паспортные данные.
	Преподаватели/ Уровень	Классные руковод	Организация работы класса, осуществление связи с родителями	Бумажный и электронный журнал.	Персональные данные учащихся и родителей (законных

	доступа к ПДн - Имеют доступ к личным делам учащихся, информации на материальных носителях, содержащей персональные данные учащихся, их родителей.	ители, социальный педагог, библиотекарь, преподаватель-организатор ОБЖ	(законными представителями), оказание социальной защиты учащихся.	Личные дела .Учёт и контроль успеваемости и посещаемости.	представителей)
	Профком/ Уровень доступа к ПДн	Председатель профсоюзного комитета	Деятельность профсоюзного комитета	Деятельность профсоюзного комитета	Персональные данные работников: Ф.И.О., дата, месяц, год и место рождения, адрес, профессия, должность, фамилия, имя отчество, дата, месяц и год рождения детей.

Приложение №3 к приказу
директора МКОУ СОШ № 8
с.Садового
от 22.10.2020 г. №50

Регламент антивирусной защиты в
МКОУ СОШ № 8 с.Садового

1.Общие положения

1. Целью создания системы антивирусной защиты является обеспечение защищенности информационно-коммуникационной системы (далее ИКС) от воздействия различного рода вредоносных программ и несанкционированных массовых почтовых рассылок, предотвращения их внедрения в информационные системы, выявления и безопасного удаления из систем в случае попадания, а также фильтрации доступа пользователей МКОУ СОШ № 8 с.Садового к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

2. Основополагающими требованиями к системе антивирусной защиты МКОУ СОШ № 8 с.Садового являются:

- решение задачи антивирусной защиты должно осуществляться в общем виде. Средство защиты не должно оказывать противодействие только конкретному вирусу или группе вирусов, противодействие должно оказываться в предположениях, что вирус может быть занесен на компьютер и о вирусе (о его структуре (в частности, сигнатуре) и возможных действиях) ничего неизвестно;

- решение задачи антивирусной защиты должно осуществляться в реальном времени.

3. Мероприятия, направленные на решение задач по антивирусной защите:

- установка только лицензированного программного обеспечения либо бесплатного антивирусного программного обеспечения;
- регулярное обновление и еженедельные профилактические проверки;
- непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах ИКС;
- ежедневный анализ, ранжирование и предотвращение угроз распространения и воздействия вредоносных программ путем выявления уязвимостей используемого в ИКС операционного программного обеспечения и сетевых устройств и устранения обнаруженных дефектов в соответствии с данными поставщика программного обеспечения и других специализированных экспертных антивирусных служб;
- проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий, включающих загрузку и развертывание специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными службами до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур;
- проведение регулярных проверок целостности критически важных программ и данных.
- наличие лишних файлов и следов несанкционированного внесения изменений должно быть зарегистрировано в журнале и расследовано: внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования;
- необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения;
- следует иметь планы обеспечения бесперебойной работы Школы для случаев вирусного заражения, в том числе планы резервного копирования всех необходимых данных и программ и их восстановления. Эти меры особенно важны для сетевых файловых серверов, поддерживающих большое количество рабочих станций.

2.Технологические инструкции

1. Директор МКОУ СОШ № 8 с.Садового назначается лицо, ответственное за антивирусную защиту.

2. В МКОУ СОШ № 8 с.Садового может использоваться только лицензионное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение.

3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, почтовые сообщения), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация, находящаяся на съемных носителях (CDROM, DVD, flash-накопителях и т.п.).

4. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

5. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

3.Требования к проведению мероприятий по антивирусной защите

1. В начале работы при загрузке компьютера в автоматическом режиме должно выполняться обновление антивирусных баз и серверов.

2. Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю, данные, расположенные на рабочих станциях пользователей - ежедневно, в ночное время по расписанию.

3. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

4. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка на серверах и персональных компьютерах школы.

5. 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.).

6. При отправке и получении электронной почты оператор электронной почты обязан проверить электронные письма и их вложения на наличие вирусов.

7. В случае обнаружения зараженных вирусами файлов или электронных писем пользователи обязаны:

- Приостановить работу.
- Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты (в случае его отсутствия - директора) МКОУ СОШ № 8 с.Садового.
- Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования.
- Провести лечение или уничтожение зараженных файлов.

4. Ответственность

1 . Ответственность за организацию антивирусной защиты возлагается на директора МКОУ СОШ № 8 с.Садового или лицо, им назначенное.

2.Ответственность за проведение мероприятий антивирусного контроля в

МКОУ СОШ № 8 с.Садового возлагается на ответственного за обеспечение антивирусной защиты, соблюдение требований настоящей Инструкции при работе на персональных рабочих станциях возлагается на пользователей данных станций или педагога, отвечающего за работу компьютерного класса.

3. Периодический контроль состояния антивирусной защиты в МКОУ СОШ № 8 с.Садового по вопросам регламентации доступа к информации в сети Интернет два раза в год (ноябрь, апрель) и фиксируется в Журнале проверок антивирусной защиты.

Приложение №4 к приказу
директора МКОУ СОШ № 8
с.Садового
от 22.10.2020 г. № 50

ИНСТРУКЦИЯ ответственного за обеспечение безопасности персональных данных информационных систем персональных данных в МКОУ СОШ № 8 с.Садового

I. Общие положения

1. Настоящая инструкция (далее - Инструкция) определяет общие функции, ответственность, права и обязанности ответственного за обеспечение безопасности персональных данных информационных систем персональных данных (далее - Ответственный) в с.Садового.

2. Настоящая инструкция разработана в соответствии с руководящими и нормативными документами регуляторов Российской Федерации в области защиты персональных данных.

3. Ответственный назначается приказом по Школе на основании «Положения о разграничении прав доступа к обрабатываемым персональным данным» в Школе из числа штатных сотрудников.

Ответственный подчиняется непосредственно директору МКОУ СОШ № 8 с.Садового

4. На время отсутствия Ответственного (отпуск, болезнь, пр.) его обязанности исполняет лицо, назначенное в установленном порядке, которое приобретает соответствующие права и несет ответственность за надлежащее исполнение возложенных на него обязанностей.

Ответственный в своей работе руководствуется настоящей Инструкцией, и другими регламентирующими документами МКОУ СОШ № 8 с.Садового , руководящими и нормативными документами регуляторов Российской Федерации в области обеспечения безопасности персональных данных.

Методическое руководство работой Ответственного осуществляется ответственным за организацию обработки персональных данных в МКОУ СОШ № 8 с.Садового.

Ответственный является ответственным лицом, уполномоченным на проведение работ по технической защите информации и поддержанию необходимого уровня защищенности ИСПДн МКОУ СОШ № 8 с.Садового и их ресурсов на этапах эксплуатации и модернизации.

II. Организация работы

1.Ответственный должен иметь специальное рабочее место, размещённое на территории контролируемой зоны, установленной приказом директора Школы, чтобы исключить несанкционированный доступ к нему посторонних лиц и других сотрудников МКОУ СОШ № 8 с.Садового.

2.Рабочее место Ответственного должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое), подключением к

ИСПДн, а так же средствами контроля технических средств защиты информации (далее - СЗИ).

III. Обязанности

Ответственный должен:

1. Соблюдать требования законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, «Правил обработки персональных данных» и других нормативных документов в области обработки и защиты персональных данных.
2. Поддерживать необходимый уровень защищенности (режим безопасности) персональных данных при их обработке в ИСПДн согласно «Инструкции по обеспечению безопасности персональных данных».
3. Наделять и изменять права доступа всех групп пользователей ИСПДн к персональным данным и защищаемым программным ресурсам и портам ввода-вывода ИСПДн.
4. Осуществлять установку, настройку и сопровождение программных и технических СЗИ.
5. Осуществлять методическое руководство всех групп пользователей МКОУ СОШ № 8 с.Садового в вопросах функционирования СЗИ и введенного режима защиты.
6. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.
7. Участвовать в приемке новых программных и технических средств, в том числе СЗИ.
8. Участвовать в проведении расследований случаев несанкционированного доступа к персональным данным и других нарушений «Правил обработки персональных данных».
9. Обеспечить доступ к защищаемой информации всем группам пользователей ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.
10. Уточнять в установленном порядке обязанности всех групп пользователей ИСПДн по обеспечению безопасности персональных данных.
11. Вести контроль над процессом осуществления резервного копирования баз данных и настроек комплекса средств автоматизации ИСПДн согласно «Инструкции по порядку резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и СЗИ».
12. Осуществлять контроль порядка учёта, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.
13. Осуществлять контроль выполнения «Плана мероприятий по обеспечению защиты персональных данных в МКОУ СОШ № 8 с.Садового.
14. Анализировать состояние защиты ИСПДн и их отдельных подсистем.
15. Контролировать неизменность состояния СЗИ, их параметров и режимов защиты.
16. Контролировать физическую сохранность СЗИ и оборудования ИСПДн.

17. Контролировать исполнение всеми группами пользователей ИСПДн введённого режима защищенности, а так же правильность работы с элементами ИСПДн и СЗИ.

18. Контролировать исполнение всем группами пользователей ИСПДн парольной политики согласно «Инструкции по организации парольной защиты»

19. Организовывать антивирусную защиту всех элементов ИСПДн согласно «Инструкции по организации антивирусной защиты».

20. Своевременно анализировать журнал учёта событий, регистрируемых СЗИ, с целью выявления возможных нарушений.

21. Недопускать установку, использование, хранение и размножение в ИСПДн ПО, не связанных с выполнением функциональных задач.

22. Не допускать к работе на элементах ИСПДн посторонних лиц.

23. Регистрировать факты выдачи внешних носителей в «Журнале учета мобильных технических средств».

24. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования СЗИ ИСПДн.

25. Периодически представлять руководству отчёт о состоянии и о нештатных ситуациях на объектах ИСПДн и допущенных всеми группами пользователей нарушениях и установленных требований по защите информации.

26. В случае отказа работоспособности СЗИ ИСПДн, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

27. Принимать меры по реагированию в случае возникновения нештатных или аварийных ситуаций с целью ликвидации их последствий.

28. Предлагать руководству мероприятия по совершенствованию работы по защите персональных данных.

IV. Права

Ответственный имеет право

1. Требовать от всех групп пользователей ИСПДн соблюдения законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, «Правил обработки персональных данных» и других нормативных документов МКОУ СОШ № 8 с.Садового в области обработки и защиты персональных данных.

2. Запрещать всем группам пользователей ИСПДн доступ к персональным данным при нарушении «Правил обработки персональных данных», при неисправностях в работе СЗИ и с целью предотвращения несанкционированного доступа к охраняемой информации.

3. Участвовать в анализе ситуаций, касающихся функционирования СЗИ, и в расследованиях по случаям несанкционированного доступа к персональным данным и другим случаям нарушения режима обработки персональных данных.

4. Вносить предложения руководству по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями.

5. В пределах своей компетенции сообщать руководству о недостатках, выявленных в процессе исполнения должностных обязанностей, и вносить

предложения по их устранению.

6. Требовать от руководства оказания содействия в исполнении своих должностных обязанностей и прав.

7. Привлекать с разрешения руководства сотрудников всех структурных подразделений к решению задач, возложенных на него.

8. Запрашивать лично или через директора Школы информацию и документы, необходимые для выполнения своих должностных обязанностей.

V. Ответственность

Ответственный несет ответственность:

1. За качество проводимых работ по контролю всех групп пользователей ИСПДн в вопросах обеспечения безопасности персональных данных.

2. За обеспечение устойчивой работоспособности СЗИ ИСПДн.

3. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим трудовым законодательством Российской Федерации.

4. За правонарушения, совершенные в процессе осуществления своей деятельности, в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

5. За причинение материального ущерба - в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

VI. Порядок пересмотра инструкции

1. Настоящая Инструкция пересматривается, изменяется и дополняется по мере необходимости, но не реже одного раза в три года.

2. С приказом о внесении изменений (дополнений) в настоящую Инструкцию знакомятся под расписку все сотрудники МКОУ СОШ № 8 с.Садового, на которых распространяется действие этой инструкции.

Приложение №5 к приказу
директора МКОУ СОШ № 8
с.Садового
от 22.10.2020 г. № 50

ИНСТРУКЦИЯ пользователя ИСПДн по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций
в МКОУ СОШ № 8 с.Садового

1. Назначение и область действия

1. Настоящая инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн МКОУ СОШ № 8 с.Садового , меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

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

Задачей настоящей Инструкции является:

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

3. Действие настоящей Инструкции распространяется 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.

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

2. Порядок реагирования на аварийную ситуацию

1. **Действия при возникновении аварийной ситуации:**

- В настоящем документе под аварийной 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
1	Сильный снегопад
1	Сильные морозы
12	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
1	Затопление водой в период паводка
1	Наводнение, вызванное проливным дождем
15	Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)
	Телекоммуникационные и ИТ угрозы
1	Сбой системы кондиционирования
1	Сбой ИТ - систем
	Угроза, связанная с человеческим фактором
1	Ошибка персонала, имеющего доступ к серверной
19	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
	Угрозы, связанные с внешними поставщиками
2	Отключение электроэнергии
2	Сбой в работе Интернет-провайдера
2	Физический разрыв внешних каналов связи

- Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю».
- В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники МКОУ СОШ № 8 с.Садового 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. **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.

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

1. Технические меры:

- 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.
- Все критические помещения МКОУ СОШ № 8 с.Садового (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации.
- 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.

2. Организационные меры:

- Ответственные за реагирование сотрудники ознакомляют всех сотрудников МКОУ СОШ № 8 с.Садового , 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.
- Должно быть проведено обучение должностных лиц МКОУ СОШ № 8 с.Садового , 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.

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 №6 к приказу
директора МКОУ СОШ № 8
с.Садового
от 22.10.2020 г. № 50

ИНСТРУКЦИЯ по обработке персональных данных без использования средств автоматизации в МКОУ СОШ № 8 с.Садового

1. Общие положения

1. Настоящая Инструкция разработана в соответствии с «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным Постановлением Правительства РФ от 15.09.2008 № 687, является дополнением к «Положению об обработке персональных данных в МКОУ СОШ № 8 с.Садового и определяет правила работы с персональными данными и их материальными носителями без использования средств автоматизации.

2. Обработка персональных данных, полученных от работника, 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.

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

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

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

2. Порядок обработки персональных данных

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

2. 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, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

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

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

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

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

3. Обязанности сотрудника, допущенного к обработке персональных данных

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

2. При выносе документов, содержащих персональные данные, за пределы территории МКОУ СОШ № 8 с.Садового по служебной необходимости сотрудник должен принять все возможные меры, исключающие утрату (утерю, хищение) таких документов.

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

4. Сотрудникам, допущенным к обработке персональных данных

запрещается:

- Сообщать сведения, являющиеся персональными данными, лицам, не имеющим права доступа к этим сведениям.
- Делать неучтенные копии документов, содержащих персональные данные.
- Оставлять документы, содержащие персональные данные, на рабочих столах без присмотра.
- Покидать помещение, не поместив документы с персональными данными в закрываемые сейфы, шкафы.
- Выносить документы, содержащие персональные данные, из помещений Учреждения без служебной необходимости.

5. Ответственность сотрудников, допущенных к обработке персональных данных:

- Ответственность за неисполнение или ненадлежащее выполнение требований настоящей Инструкции возлагается на работников и администрацию МКОУ СОШ № 8 с.Садового .
- Контроль за выполнением положений настоящей Инструкции возлагается на ответственного за систему защиты информации в информационной системе персональных данных.
- За нарушение правил обработки персональных данных, их неправомерное разглашение или распространение, виновные лица несут дисциплинарную, административную, гражданско- правовую или уголовную ответственность в соответствии с действующим законодательством.
- В случае если в результате действий работника был причинен подлежащий возмещению работодателем ущерб третьим лицам, работник несет перед работодателем материальную ответственность в соответствии с главой 39 Трудового кодекса РФ.
- В случае разглашения персональных данных, ставших известными работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника, трудовой договор с работником может быть расторгнут работодателем (подпункт «в» пункта 6 статьи 81 Трудового кодекса РФ).

Приложение №7 к приказу
директора МКОУ СОШ № 8
с.Садового
от 22.10.2020 г. № 50

ИНСТРУКЦИЯ
по организации парольной защиты информационных систем персональных данных в МКОУ СОШ № 8 с.Садового

1. Общие положения

1. Данная инструкция регламентирует организационно -техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее - ИСПДн) МКОУ СОШ № 8 с.Садового , а также контроль действий пользователей и обслуживающего персонала системы при работе с паролями.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн Школы и контроль действий исполнителей и обслуживающего персонала ИСПДн при работе с паролями возлагается на ответственного за обеспечение безопасности ПДн, содержащих механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

3. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИСПДн самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- 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 предыдущего не менее чем в 6 позициях;

- личный пароль пользователь не имеет права сообщать никому.

4. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

5. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления самих уполномоченных сотрудников, а также ответственных за информационную безопасность в подразделениях с паролями других сотрудников МКОУ СОШ № 8 с.Садового .

6. При наличии в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте передавать на хранение ответственному за информационную безопасность подразделения. Опечатанные конверты с паролями исполнителей должны храниться в недоступном месте.

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

8. Удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение), должна производиться ответственным за обеспечение безопасности ПДн немедленно после окончания последнего сеанса работы данного пользователя с системой.

9. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри Школы и другие обстоятельства ответственного за информационную безопасность и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем ИСПДн.

10. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры в соответствии с п.6 или п.7 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

11. Повседневный контроль действий исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственного за информационную безопасность.

Приложение №8 к приказу
директора МКОУ СОШ № 8
с.Садового
от 22.10.2020 г. № 50

Модель угроз безопасности персональных данных
МКОУ СОШ № 8 с.Садового

I. Перечень обозначений и сокращений

1. АРМ - автоматизированное рабочее место;
2. ИР - информационный ресурс;
3. ИСПДн - информационная система персональных данных;
4. КЗ - контролируемая зона;
5. ПДн - персональные данные;
6. ПО - программное обеспечение;
7. ПТС - программно-технические средства;
8. ПЭМИН - побочные электромагнитные излучения и наводки;
9. СЗИ - средства защиты информации;
10. СКЗИ - средства криптографической защиты информации;
11. ФСБ - Федеральная служба безопасности;
12. ФСО - Федеральная служба охраны;
13. ФСТЭК - Федеральная служба по техническому и экспертному контролю.

II. Общие положения

1. Настоящая модель угроз безопасности персональных данных (далее - Модель) содержит систематизированный перечень угроз безопасности персональных данных при их обработке (далее - Учреждение). Указанные угрозы могут исходить от источников, имеющих антропогенный, техногенный и стихийный характер и воздействующих на уязвимости ИСПДн, характерные для данной ИСПДн, реализуя тем самым угрозы информационной безопасности.

2. В Модели дается обобщенное описание ИСПДн, состав, категории и

предполагаемый объем обрабатываемых ПДн с последующей классификацией ИСПДн.

3. Модель описывает потенциального нарушителя безопасности ПДн и подходы по определению актуальности угроз с учетом возможностей нарушителя и особенностей конкретной ИСПДн.

4. Настоящая Модель разработана в соответствии с требованиями Федерального законодательства и федеральных органов по защите персональных данных.

III. Характеристика объекта информатизации

В МКОУ СОШ № 8 с.Садового существуют следующие типы ИСПДн:

1 . ИСПДн передачи информации, в том числе ПДн, в целях исполнения Федеральных законов.

3. Состав ИСПДн и обрабатываемых в них персональных данных приведен в Приложении №1 к настоящему документу.

4. В качестве объекта информатизации Школы выступают:

1. Автономные автоматизированные рабочие места (АРМ).
2. Локальные вычислительные сети.

5. В зависимости от характеристик и особенностей отдельных объектов часть вычислительных средств данных предприятий подключена к сетям связи общего пользования и (или) сетям международного информационного обмена.

6. Ввод персональных данных осуществляется как с бумажных носителей (например, документов, удостоверяющих личность субъекта ПДн), так и с электронных носителей информации.

7. ИСПДн предполагают распределенную (на АРМ) обработку и хранение ПДн.

8. Персональные данные субъектов ПДн могут выводиться из ИСПДн с целью передачи персональных данных субъектов Учреждения, как в электронном, так и в бумажном виде.

9. Контролируемой зоной (КЗ) ИСПДн являются отдельные помещения. В пределах контролируемой зоны находятся рабочие места пользователей и места хранения архивных копий данных, сетевое и телекоммуникационное оборудование ИСПДн. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

IV. Состав, категории и объем персональных данных, определение уровня защищенности персональных данных

1. На основе характеристик и особенностей используемых ИСПДн и обрабатываемых в них персональных данных, можно констатировать, что персональные данные субъектов ПДн, обрабатываются в Учреждении информационной системой, обрабатывающей общедоступные персональные

данные, а также системой, обрабатывающей иные категории персональных данных. Специальные категории персональных данных и биометрические персональные данные в ИСПДн Учреждения не обрабатываются.

2.Для ИСПДн МКОУ СОШ № 8 с.Садового актуальны угрозы 2 типа - угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе. Согласно «Требованиям к защите персональных данных при их обработке в информационных системах персональных данных» для ИСПДн Школы требуется обеспечить 4 -ий уровень защищенности персональных данных при их обработке в информационной системе.

V. Способы нарушения характеристик безопасности персональных данных

1. Исходя из перечня персональных данных, обрабатываемых в ИСПДн, существуют следующие способы нарушения характеристик безопасности ПДн:

- хищение персональных данных сотрудниками Учреждения для использования в корыстных целях;
- передача финансовой, адресной, юридической и прочей информации о субъекте ПДн третьим лицам;
- несанкционированное публичное разглашение персональных данных, ставших известными сотрудникам МКОУ СОШ № 8 с.Садового ;
- несанкционированное получение персональных данных третьими лицами;
- уничтожение финансовой, адресной и прочей информации о субъекте ПДн;
- модификация финансовой, адресной и прочей информации о субъекте ПДн;
- блокирование финансовой, адресной и прочей информации о субъекте ПДн;
- ввод некорректной финансовой, адресной и прочей информации о субъекте ПДн;
- передача некорректной финансовой, адресной и прочей информации о субъекте ПДн;
- искажение архивной информации по субъекту ПДн.
- уничтожение архивной информации по субъекту ПДн.

VI. Угрозы безопасности персональных данных, при их обработке в информационных системах персональных данных

1. Под угрозами безопасности персональных данных при их обработке в ИСПДн понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными

воздействиями на нее. Таким образом, угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн, так и со специально осуществляемыми неправомерными действиями отдельных организаций и граждан, а также иными источниками угроз. Неправомерные действия могут исходить также и от сотрудников Учреждения в случае, когда они рассматриваются в качестве потенциального нарушителя безопасности ПДн.

2. В целях формирования систематизированного перечня угроз безопасности ПДн при их обработке в ИСПДн и разработке на их основе частных (детализированных) моделей применительно к конкретному виду ИСПДн, угрозы безопасности персональным данным в ИСПДн можно классифицировать в соответствии со следующими признаками:

по видам возможных источников угроз;

по типу ИСПДн, на которые направлена реализация угроз;

повиду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн);

по способам реализации угроз;

по используемой уязвимости;

по объекту воздействия.

3. Для ИСПДн существуют следующие классы угроз безопасности ПДн:

- **По видам возможных источников угроз безопасности персональных данных**

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющими доступ к ИР ИСПДн, включая пользователей, реализующие угрозы непосредственно в ИСПДн;

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;

- угрозы, возникновение которых напрямую зависит от свойств техники, используемой в ИСПДн;

- угрозы, связанные со стихийными природными явлениями.

Кроме этого, угрозы могут возникать в результате внедрения аппаратных закладок и вредоносных программ.

- **По типу ИСПДн, на которые направлена угроза:**

По структуре ИСПДн, на которые направлена угроза, необходимо рассматривать следующие классы угроз:

- угрозы безопасности данных, обрабатываемых в ИСПДН на базе автоматизированных рабочих мест;

- угрозы безопасности данных, обрабатываемых в ИСПДН на базе локальных информационных систем.

- **По способам реализации угроз**

По способам реализации угроз выделяют следующие классы угроз:

- угрозы, связанные с несанкционированным доступом к ПДн (в том числе угрозы внедрения вредоносных программ);
- угрозы утечки ПДн по техническим каналам утечки информации (ТКУИ);
- угрозы специальных воздействий на ИСПДн.
- **По виду нарушаемого свойства информации (несанкционированных действий, осуществляемых с персональными данными)**

По виду несанкционированных действий, осуществляемых с персональными данными, можно выделить следующий класс угроз:

- угрозы, приводящие к нарушению конфиденциальности ПДн (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;
- угрозы, приводящие к несанкционированному воздействию на содержание информации, в результате которого происходит изменение данных или их уничтожение;
- угрозы, приводящие к несанкционированному воздействию на программные или программно-аппаратные элементы ИСПДн, в результате которого осуществляется блокирование данных.
- **По используемой уязвимости выделяются следующие классы угроз:**
- угрозы, реализуемые с использованием уязвимости системного программного обеспечения (ПО);
- угрозы, реализуемые с использованием уязвимости прикладного ПО; - угрозы, возникающие в результате использования уязвимости, вызванной наличием в ИСПДн аппаратной закладки;
- угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;
- угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации технической защиты информации от несанкционированного доступа;
- угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;
- угрозы, реализуемые с использованием уязвимостей средств защиты информации.
- **По объекту воздействия выделяются следующие классы угроз:**
- угрозы безопасности ПДн, обрабатываемых на АРМ;
- угрозы безопасности ПДн, передаваемых по сетям связи;

- угрозы прикладным программам, с помощью которых обрабатываются ПДн;
- угрозы системному ПО, обеспечивающему функционирование ИСПДн.

VII. Характеристика источников угроз безопасности персональных данных в ИСПДн

1. В отношении ИСПДн могут существовать три типа источников угроз безопасности

ПДн:

1. Антропогенные источники угроз безопасности ПДн.
2. Техногенные источники угроз безопасности ПДн.
3. Стихийные источники угроз безопасности ПДн.

- **Антропогенные источники угроз безопасности ПДн**

В качестве антропогенного источника угроз для ИСПДн необходимо рассматривать субъекта (личность), имеющего санкционированный или несанкционированный доступ к работе со штатными средствами ИСПДн, действия которого могут привести к нарушению безопасности персональных данных. Антропогенные источники угроз по отношению к ИСПДн могут быть как внешними, так и внутренними

Среди внешних антропогенных источников можно выделить случайные и преднамеренные источники.

Случайные (непреднамеренные) источники могут использовать такие уязвимости, как ошибки, совершенные при проектировании ИСПДн и ее элементов, ошибки в программном обеспечении; различного рода сбои и отказы, повреждения, проявляемые в ИСПДн. К таким источникам можно отнести персонал поставщиков различного рода услуг, персонал надзорных организаций и аварийных служб и т.п. Действия (угрозы), исходящие от данных источников, совершаются по незнанию, невнимательности или

халатности, из любопытства, но без злого умысла.

Преднамеренные источники проявляются в корыстных устремлениях нарушителей. Основная цель таких источников - умышленная дезорганизация работы, вывод систем Организации из строя, искажение информации за счет проникновения в ИСПДн путем несанкционированного доступа.

Внутренними источниками, как правило, являются специалисты в области программного обеспечения и технических средств, в том числе средств защиты информации, имеющие возможность использования штатного оборудования и программнотехнических средств ИСПДн. К таким источникам можно отнести основной персонал, представителей служб безопасности, вспомогательный и технический персонал.

Для внутренних источников угроз особое место занимают угрозы в виде ошибочных действия и (или) нарушений требований эксплуатационной и иной

документации сотрудниками Учреждения, имеющих доступ к ИР ИСПДн. К подобным угрозам, в частности, относятся:

- непредумышленное искажение или удаление программных компонентов;
- внедрение и использование неучтенных программ;
- игнорирование организационных ограничений (установленных правил) при работе с ресурсами ИСПДн, включая средства защиты информации. В частности:
- нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (ключевой, парольной и аутентифицирующей информации);
- предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований;
- настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов;
- несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа.

Наибольшую опасность представляют преднамеренные угрозы, исходящие как от внешних, так и от внутренних антропогенных источников.

Необходимо рассматривать следующие классы таких угроз:

- угрозы, связанные с преднамеренными действиями лиц, имеющими доступ к ИСПДн, включая пользователей ИСПДн и иных сотрудников Учреждения, реализующими угрозы непосредственно в ИСПДн (внутренний нарушитель);
- угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к ИСПДн и реализующими угрозы из внешних сетей связи общего пользования или сетей международного информационного обмена (внешний нарушитель);
- угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к ИСПДн и реализующими угрозы по ТКУИ.
- **Техногенные источники угроз безопасности ПДн**

Техногенные источники угроз напрямую зависят от свойств техники. Данные источники также могут быть как внешними, так и внутренними.

К внешним источникам относятся инфраструктурные элементы ИСПДн: средства связи (телефонные линии, линии передачи данных и т.п.), сети инженерных коммуникаций (водоснабжение, канализация, отопление и пр.).

К внутренним источникам относятся некачественные технические и программные средства обработки информации, вспомогательные средства (охраны, сигнализации, телефонии), другие технические средства, применяемые в ИСПДн, а также вредоносное программное обеспечение и аппаратные закладки.

Аппаратная закладка

Аппаратные закладки могут быть конструктивно встроенными и автономными. Аппаратные закладки могут реализовать угрозы:

- сбора и накопления ПДн, обрабатываемых и хранимых в ИСПДн;
- формирования ТКУИ.

В силу отмеченных свойств аппаратных закладок эффективная защита от них может быть обеспечена только за счет тщательного учета их специфики и соответствующей организации технической защиты информации на всех стадиях жизненного цикла ИСПДн.

Носитель вредоносной программы

В качестве носителя вредоносной программы в ИСПДн может выступать аппаратный элемент средств вычислительной техники из состава ИСПДн или ПО, выполняющее роль программного контейнера.

Если вредоносная программа не ассоциируется с какой-либо прикладной программой из состава системного или общего ПО ИСПДн, в качестве ее носителя выступают:

- внешний машинный (отчуждаемый) носитель, т.е. дискета, оптический диск, лазерный диск, флэш-память, внешний жесткий диск и т.п.;
- встроенные носители информации (жесткие диски, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок устройства - видеоадаптера, сетевой платы, устройств ввода/вывода и т . д .)
- микросхемы внешних устройств (монитора, клавиатуры, принтера, плоттера, сканера и т.п.).

В том случае, если вредоносная программа может быть проассоциирована с системным или общим ПО, с файлами различной структуры или с сообщениями, передаваемыми по сети, то ее носителем являются:

- пакеты передаваемых по сети ИСПДн сообщений;
- файлы (исполняемые, текстовые, графические и т.д.).

При возникновении угроз из данной группы появляется потенциальная возможность нарушения конфиденциальности, целостности, доступности и других характеристик безопасности ПДн.

- **Стихийные источники угроз безопасности ПДн**

Стихийные источники угроз отличается большим разнообразием и непредсказуемостью и являются, как правило, внешними по отношению к Учреждению. Под ними, прежде всего, рассматриваются различные природные

катаклизмы: пожары, землетрясения, ураганы, наводнения. Возникновение этих источников трудно спрогнозировать и им тяжело противодействовать, но при наступлении подобных событий нарушается штатное функционирование самой ИСПДн и ее средств защиты, что потенциально может привести к нарушению конфиденциальности, целостности, доступности и других характеристик безопасности ПДн.

Защита от угроз, исходящих от техногенных и стихийных источников угроз безопасности ПДн, регламентируется инструкциями, разработанными и утвержденными оператором с учетом особенностей эксплуатации ИСПДн.

VIII. Модель нарушителя безопасности персональных данных

1. Анализ возможностей, которыми может обладать нарушитель, проводится в рамках модели нарушителя.

При разработке модели нарушителя зафиксированы следующие положения:

- Безопасность ПДн в ИСПДн обеспечивается средствами защиты информации ИСПДн, а также используемыми в них информационными технологиями, техническими и программными средствами, удовлетворяющими требованиям по защите информации, устанавливаемым в соответствии с законодательством Российской Федерации;
- Средства защиты информации (СЗИ) штатно функционируют совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к СЗИ требований;
- СЗИ не могут обеспечить защиту ПДн от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СЗИ не может обеспечить защиту ПДн от раскрытия лицами, которым предоставлено право на доступ к этим данным).

2 .Описание нарушителей.

С точки зрения наличия права постоянного или разового доступа в контролируемую зону (КЗ) объектов размещения ИСПДн все физические лица могут быть отнесены к следующим двум категориям:

- категория I - лица, не имеющие права доступа в контролируемую зону ИСПДн;
- категория II - лица, имеющие право доступа в контролируемую зону ИСПДн.

Все потенциальные нарушители подразделяются на:

- внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны ИСПДн;
- внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны ИСПДн.

В качестве внешнего нарушителя кроме лиц категории I должны рассматриваться также лица категории II, находящиеся за пределами КЗ.

В отношении ИСПДн в качестве внешнего нарушителями из числа лиц категории I могут выступать:

- бывшие сотрудники Учреждения;
- посторонние лица, пытающиеся получить доступ к ПДн в инициативном порядке;
- представители преступных организаций.

Внешний нарушитель может осуществлять:

- перехват обрабатываемых техническими средствами ИСПДн ПДн за счет их утечки по ТКУИ с использованием портативных, возимых, носимых, а также автономных автоматических средств разведки серийной разработки;
- деструктивные воздействия через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами КЗ;
- несанкционированный доступ к информации с использованием специальных программных воздействий посредством программы вирусов, вредоносных программ, алгоритмических или программных закладок;
- перехват информации, передаваемой по сетям связи общего пользования или каналам связи, не защищенным от несанкционированного доступа (НСД) к информации организационно- техническими мерами;
- атаки на ИСПДн путем реализации угроз удаленного доступа.

Внутренний нарушитель (лица категории II) подразделяется на восемь групп в зависимости от способа и полномочий доступа к информационным ресурсам (ИР) ИСПДн.

-К первой группе относятся сотрудники Учреждения, не являющиеся зарегистрированными пользователями и не допущенные к ИР ИСПДн, но имеющие санкционированный доступ в КЗ.

Лицо данной группы может:

- располагать именами и вести выявление паролей зарегистрированных пользователей ИСПДн;
- изменять конфигурацию технических средств обработки ПДн, вносить программноаппаратные закладки в ПТС ИСПДн и обеспечивать съем информации, используя непосредственное подключение к техническим средствам обработки информации.
- Ко второй группе относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ИР ИСПДн с рабочего места. К этой категории относятся сотрудники Учреждения, имеющие право доступа к локальным ИР ИСПДн для выполнения своих должностных обязанностей.

Лицо данной группы:

- обладает всеми возможностями лиц первой категории;
- знает, по меньшей мере, одно легальное имя доступа;

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающим доступ к ИР ИСПДн;
- располагает ПДн, к которым имеет доступ.

- К третьей группе относятся зарегистрированные пользователи подсистем ИСПДн, осуществляющие удаленный доступ к ПДн по локальной сети Учреждения.

Лицо данной группы:

- обладает всеми возможностями лиц второй категории;
- располагает информацией о топологии сети ИСПДн и составе технических средств ИСПДн;
- имеет возможность прямого (физического) доступа к отдельным техническим средствам (ТС) ИСПДн.

- К четвертой группе относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности ИСПДн.

Лицо данной группы:

- обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте ИСПДн;
- обладает полной информацией о технических средствах и конфигурации сегмента ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте ИСПДн;
- имеет доступ ко всем техническим средствам сегмента ИСПДн;
- обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента ИСПДн.

- К пятой группе относятся зарегистрированные пользователи с полномочиями системного администратора, выполняющего конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства мониторинга, резервного копирования, антивирусного контроля, защиты от несанкционированного доступа.

Лицо данной группы:

- обладает полной информацией о системном, специальном и прикладном ПО, используемом в ИСПДн;
- обладает полной информацией о ТС и конфигурации ИСПДн
- имеет доступ ко всем ТС ИСПДн и данным;
- обладает правами конфигурирования и административной настройки ТС ИСПДн.
- К шестой группе относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности Учреждения, отвечающего за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей, криптографическую защиту информации.

Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор.

Лицо данной группы:

- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

-К седьмой группе относятся лица из числа программистов - разработчиков сторонней организации, являющихся поставщиками ПО и лица, обеспечивающие его сопровождение на объекте размещения ИСПДн.

Лицо данной группы:

- обладает информацией об алгоритмах и программах обработки информации в ИСПДн;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в ПО ИСПДн на стадии его разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о ТС обработки и защиты информации в ИСПДн.

-К восьмой группе относятся персонал, обслуживающий ТС ИСПДн, а также лица, обеспечивающие поставку, сопровождение и ремонт ТС ИСПДн.

Лицо данной группы:

- обладает возможностями внесения закладок в ТС ИСПДн на стадии их разработки, внедрения и сопровождения;
- может располагать фрагментами информации о топологии ИСПДн, автоматизированных рабочих местах, серверах и коммуникационном оборудовании, а также о ТС защиты информации в ИСПДн.

3. Предположения о возможностях нарушителя.

Для получения исходных данных о ИСПДн нарушитель (как I категории, так и II категории) может осуществлять перехват зашифрованной информации и иных данных, передаваемых по каналам связи сетям общего пользования и (или) сетям международного информационного обмена, а также по локальным сетям ИСПДн.

Любой внутренний нарушитель может иметь физический доступ к линиям связи, системам электропитания и заземления.

Предполагается, что возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны объектов размещения ИСПДн ограничительных факторов, из которых основными являются режимные мероприятия и организационно-технические меры, направленные на:

- предотвращение и пресечение несанкционированных действий;

- подбор и расстановку кадров;
- допуск физических лиц в контролируемую зону и к средства вычислительной техники;
- контроль за порядком проведения работ.

В силу этого внутренний нарушитель не имеет возможности получения специальных знаний о ИСПДн в объеме, необходимом для решения вопросов создания и преодоления средств защиты ПДн, и исключается его возможность по созданию и применению специальных программно-технических средств реализации целенаправленных воздействий данного нарушителя на подлежащие защите объекты и он может осуществлять попытки несанкционированного доступа к ИР с использованием только штатных программно-технических средств ИСПДн без нарушения их целостности.

Возможность сговора внутренних нарушителей между собой, сговора внутреннего нарушителя с персоналом организаций-разработчиков подсистем ИСПДн, а также сговора внутреннего и внешнего нарушителей должна быть исключена применением организационно-технических и кадрово-режимных мер, действующих на объектах размещения ИСПДн.

4. Предположения об имеющихся у нарушителя средствах атак

Предполагается, что нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства.

Внешний нарушитель (лица категории I, а также лица категории II при нахождении за пределами КЗ) может использовать следующие средства доступа к защищаемой информации:

- доступные в свободной продаже аппаратные средства и программное обеспечение, в том числе программные и аппаратные компоненты криптосредств;
- специально разработанные технические средства и программное обеспечение;
- средства перехвата и анализа информационных потоков в каналах связи;
- специальные технические средства перехвата информации по ТКУИ;
- штатные средства ИСПДн (только в случае их расположения за пределами КЗ).

Внутренний нарушитель для доступа к защищаемой информации, содержащей ПДн, может использовать только штатные средства ИСПДн. При этом его возможности по использованию штатных средств зависят от реализованных в ИСПДн организационнотехнических и режимных мер.

5. Описание каналов атак.

Возможными каналами атак, которые может использовать нарушитель для доступа к защищаемой информации в ИСПДн, являются:

- каналы непосредственного доступа к объекту (визуально-оптический, акустический, физический);
- электронные носители информации, в том числе съемные, сданные в ремонт и вышедшие из употребления;
- бумажные носители информации;
- штатные программно-аппаратные средства ИСПДн;
- кабельные системы и коммутационное оборудование, расположенные в пределах контролируемой зоны и не защищенные от НСД к информации организационнотехническими мерами;
- незащищенные каналы связи; ТКУИ.

6. Тип нарушителя при использовании в ИСПДн криптографических средств защиты информации

При обмене информацией между ИСПДн и внешними по отношению к предприятию информационными системами необходимо использование средств криптографической защиты информации (СКЗИ).

Уровень криптографической защиты персональных данных, обеспечиваемой СКЗИ, определяется путем отнесения нарушителя, действиям которого должно противостоять СКЗИ, к конкретному типу, и базируется на подходах, описанных в «Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации».

Тип нарушителя и класс СКЗИ должен определяться в соответствии с таблицей Таблица - Соответствие типов нарушителя и класса СКЗИ

Группа внутреннего нарушителя	Тип нарушителя	Класс СКЗИ
Группа 1	Н2	КС2
Г руппа 2	Н3	КС3
Г руппа 3	Н3	КС3
Г руппа 4	Н3	КС3
Г руппа 5	Н3	КС3
Г руппа 6	Н3	КС3
Г руппа 7	Н5	КВ2
Г руппа 8	Н4	КВ1

Внешний нарушитель относится к типу Н1. При этом, если он обладает

возможностями по созданию способов и подготовки атак, аналогичными соответствующим возможностям внутреннего нарушителя типа Нi (за

исключением возможностей, предоставляемых пребыванием в момент атаки в контролируемой зоне), то этот нарушитель также будет обозначаться как нарушитель типа Hi.

IX. Актуальные угрозы безопасности персональных данных в информационных системах персональных данных

1. Для выявления из всего перечня угроз безопасности ПДн актуальных для ИСПДн оцениваются два показателя:

- уровень исходной защищенности ИСПДн;
- частота (вероятность) реализации рассматриваемой угрозы.

2. Уровень исходной защищенности информационной системы персональных данных

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель,

зависящий от технических и эксплуатационных характеристик ИСПДн. Перечень данных характеристик и показатели защищенности ИСПДн, зависящие от них, показаны в таблице.

3. Показатели, относящиеся к Учреждению выделены жирным курсивом.

Для определения исходной защищенности ИСПДн должно быть рассчитано процентное соотношение каждого уровня защищенности ко всем характеристикам, имеющим место для ИСПДн.

Приложение №9 к приказу
директора МКОУ СОШ №8
с.Садового
от 22.10.2020 г. № 50

Должностная инструкция лица, ответственного за организацию обработки персональных данных в МКОУ СОШ №8 с.Садового

I. Общие положения

1. Должностная инструкция лица, ответственного за организацию обработки персональных данных в МКОУ СОШ №8 с.Садового (далее - Инструкция), разработана в соответствии с Постановлением Правительства Российской Федерации N 1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», «Положения о порядке обработки персональных данных работников МКОУ СОШ №8 с.Садового .

2. Настоящая Инструкция закрепляет обязанности, права и ответственность лица, ответственного за организацию обработки персональных данных в МКОУ СОШ №8 с.Садового.

3. Ответственный за организацию обработки и обеспечение безопасности персональных данных назначается из числа сотрудников МКОУ СОШ №8 с.Садового и обеспечивает правильность использования и нормальное функционирование установленной системы защиты информации (СЗИ).

4. Лицо, ответственное за организацию обработки персональных данных, в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными нормативными правовыми актами, настоящей Инструкцией, а также иными локальными нормативными актами организации, регламентирующими вопросы обработки персональных данных.

II. Основные функции Ответственного за организацию обработки и обеспечение безопасности персональных данных

1. Контроль за выполнением требований действующих нормативных документов по вопросам обеспечения режима конфиденциальности и защиты персональных данных при проведении работ в ИСПДн МКОУ СОШ №8 с.Садового.

2. Настройка и сопровождение в процессе эксплуатации подсистемы управления доступом в ИСПДн:

- реализация полномочий доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру, сетевым ресурсам и т.д.);
- ввод описаний пользователей ИСПДн в информационную базу СЗИ от несанкционированного доступа (НСД).
- своевременное удаление описаний пользователей из базы данных СЗИ при изменении списка допущенных к работе в ИСПДн лиц.

3. Контроль за периодическим проведением смены паролей для доступа к ИСПДн пользователями.

4. Настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе в ИСПДн:

- введение в базу данных СЗИ от НСД, внедренной в ИСПДн, описания событий, подлежащих регистрации в системном журнале;
- регулярное проведение анализа системного журнала для выявления попыток НСД к защищаемым ресурсам;
- своевременное информирование руководителя, ответственного за эксплуатацию ИСПДн МКОУ СОШ № 8 с.Садового о несанкционированных действиях персонала и проведение расследования попыток НСД.

5. Сопровождение антивирусной подсистемы и системы защиты от программно - математических воздействий:

- поддержание установленного порядка и правил антивирусной защиты информации в ИСПДн от компьютерных вирусов;
- периодическое обновление антивирусных средств (баз данных), внедрённых в ИСПДн, контроль за соблюдением пользователями порядка и правил проведения антивирусного тестирования ИСПДн Школы».

III. Обязанности лица, ответственного за организацию обработки персональных данных в организации

Лицо, ответственное за организацию обработки персональных данных в организации обязано:

- осуществлять внутренний контроль за соблюдением работниками организации законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников организации положения

законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой указанных обращений и запросов.

IV. Права лица, ответственного за организацию обработки персональных данных в организации

Лицо, ответственное за организацию обработки персональных данных, имеет право:

- принимать решения в пределах совей компетенции; требовать от работников организации соблюдения действующего законодательства, а также локальных нормативных актов организации о персональных данных;
- контролировать в Службе осуществление мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами;
- взаимодействовать с управлениями и иными структурными подразделениями организации по вопросам обработки персональных данных.

V. Ответственность лица, ответственного за организацию обработки персональных данных в организации

За ненадлежащее исполнение или неисполнение настоящей Инструкции, а также за нарушение требований законодательства о персональных данных лицо, ответственное за организацию обработки персональных данных в организации, несет предусмотренную законодательством Российской Федерации ответственность.

Приложение №10 к приказу
директора МКОУ СОШ №8
с.Садового
от 22.10.2020 г. № 50

ПОРЯДОК уничтожения носителей персональных данных
в МКОУ СОШ №8 с.Садового

Носителями персональных данных являются:

- Бумажные носители (документы);
- Машинные носители:

- накопители на жестких магнитных дисках (НЖМД), установленные в системных блоках автоматизированных рабочих мест обработки персональных данных;

- съемные носители (дискеты, CD-DVD диски, USB-носители, съемные НЖМД).

1. Носители уничтожаются в случаях:
- истек срок хранения носителя;
- носитель пришел в негодность.

2. Для уничтожения носителей приказом директора назначается экспертная комиссия.

3. Бумажные носители персональных данных, CD-DVD диски и дискеты уничтожаются путем сожжения или измельчения шредером (уничтожителем бумаги).

4. НЖМД и USB-носители уничтожаются при помощи специальных устройств или физического повреждения, исключающего возможность восстановления носителя.

5. В том случае, если необходимо уничтожить персональные данные на

машинном носителе и сохранить носитель для последующего использования необходимо произвести 3 цикла полного форматирования носителя.

6. После уничтожения носителей комиссия составляет Акт об уничтожении и делает отметку в Журнале учета носителей.

Приложение №11 к приказу
директора МКОУ СОШ №8
с.Садового
от 22.10.2020 г. № 50

ИНСТРУКЦИЯ осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МКОУ СОШ №8 с.Садового

I. Общие положения

1. Настоящая Инструкция осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МКОУ СОШ №8 с.Садового (далее Оператора) разработана с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и Постановлением Правительства Российской Федерации N 1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

2. Настоящая Инструкция определяет порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

II. Тематика внутреннего контроля

1. Тематика проверок обработки персональных данных с использованием средств автоматизации:

- соответствие полномочий пользователя матрице доступа;
- соблюдение пользователями информационных систем

персональных данных парольной политики;

- соблюдение пользователями информационных систем персональных данных антивирусной политики;
- соблюдение пользователями информационных систем персональных данных правил работы со съемными носителями персональных данных;
- соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных;
- соблюдение порядка резервирования баз данных и хранения резервных копий;
- соблюдение порядка работы со средствами защиты информации;
- знание пользователями информационных систем персональных данных о своих действиях во внештатных ситуациях.
- Тематика проверок обработки персональных данных без использования средств автоматизации:
- хранение бумажных носителей с персональными данными;
- доступ к бумажным носителям с персональными данными;
- доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными.

1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям Оператор организует проведение периодических проверок условий обработки персональных данных.
2. Проверки осуществляются ответственным за организацию обработки персональных данных (далее Ответственный) либо комиссией, назначаемой директором школы.
3. Внутренние проверки проводятся в соответствии с Планом внутренних проверок, составленным Ответственным либо Председателем комиссии и утвержденным директором школы.
4. План внутренних проверок составляется в декабре текущего года на следующий год.
5. Очередность и объем проверок определяется Ответственным либо Председателем комиссии.
6. По результатам каждой проверки составляется Протокол проведения внутренней проверки.
7. При выявлении в ходе проверки нарушений, Ответственным либо Председателем комиссии в Протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.
8. Протоколы хранятся у Ответственного либо Председателя комиссии. Срок хранения протокола - 1 год.
9. О результатах проверки и мерах, необходимых для устранения нарушений докладывает директору школы Ответственный либо Председатель

комиссии.

10. Инструкция осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

Приложение №12 к приказу
директора МКОУ СОШ №8
с.Садового
от 22.10.2020 г. № 50

Инструкция пользователя информационной системы
персональных данных МКОУ СОШ №8 с.Садового

I. Общие положения

1. Пользователь информационной системы персональных данных (далее по тексту - ИСПДн) МКОУ СОШ №8 с.Садового осуществляет обработку персональных данных в ИСПДн.

2. Пользователем является каждый сотрудник МКОУ СОШ №8 с.Садового, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

3. Пользователь несет персональную ответственность за свои действия.

4. Пользователь в своей работе руководствуется настоящей инструкцией, Концепцией информационной безопасности, Политикой информационной безопасности, руководящими и нормативными документами ФСТЭК России и регламентирующими документами Оператора.

5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных МКОУ СОШ №8 с.Садового .

II. Должностные обязанности

1. Пользователь обязан:

- 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.
- 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.
- Соблюдать требования парольной политики. (раздел 3).
- Соблюдать правила при работе в сетях общего - Интернет и других (раздел 4).
- 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).
- Обо всех выявленных нарушениях, связанных с информационной

безопасностью Оператора, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться к лицу ответственному за обеспечение информационной безопасности ИСПДн.

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

2. 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.

3. 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>

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

III. Организация парольной защиты

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

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

3. Правила формирования пароля:

- Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.
- Пароль должен состоять не менее чем из 8 символов.
- Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа "123", "111", "qwerty" и им подобные, а так же 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.

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.).

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.
- Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

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.
-

IV. Правила работы в сетях общего доступа

1. Работа в сетях общего доступа (сети Интернет и других) (далее - Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.
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.