Муниципальное бюджетное общеобразовательное учреждение
«Средняя школа № 3 имени А.Н. Першиной»
г. Енисейска Красноярского края
(«МБОУ «СШ № 3 им. А.Н. Першиной»)

663180, г. Енисейск, Красноярский край, ул. Ленина 102
ИНН 2447004263, КПП 244701001, ОГРН 1022401273498
т.8 (39195)2-23-06, e-mail:mousosh_102@mail.ru, http://lehrer.3dn.ru

П Р И К А З

08.02.2021 03-10-43

Об утверждении локальных актов
по защите персональных данных

В соответствии со ст. 19 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, приказываю:

1. Утвердить прилагаемые:

Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных в муниципальном бюджетном общеобразовательном учреждении «Средняя школа № 3 имени А.Н. Першиной» г. Енисейска Красноярского края (приложение № 1);

Меры по обеспечению безопасности персональных данных в муниципальном бюджетном общеобразовательном учреждении «Средняя школа № 3 имени А.Н. Першиной» г. Енисейска Красноярского края (приложение № 2);

Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в муниципальном бюджетном общеобразовательном учреждении «Средняя школа № 3 имени А.Н. Першиной» г. Енисейска Красноярского края (приложение № 3);

Порядок осуществления контроля за принимаемыми мерами по обеспечению безопасности персональных данных при их обработке в информационных системах и уровня защищённости информационных систем персональных данных в муниципальном бюджетном общеобразовательном учреждении «Средняя Школа № 3 имени А.Н. Першиной» г. Енисейска Красноярского края (приложение № 4);

Порядок учета машинных носителей персональных данных в муниципальном бюджетном общеобразовательном учреждении «Средняя Школа № 3 имени А.Н. Першиной» г. Енисейска Красноярского края (приложение № 5).

2. Ознакомить лиц, непосредственно осуществляющих обработку персональных данных с прилагаемыми документами.
3. Контроль за исполнением приказа оставляю за собой.

Директор С.В. Тараторкина

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат:
2BB4ADAE2B6EAAC05482D16F92E0B7BC221DB2DA
Владелец: Тараторкина Светлана Викторовна
Действителен: с 28.01.2022 до 28.04.2023

Приложение № 1
к приказу Об утверждении локальных актов по защите персональных данных

Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных в муниципальном бюджетном общеобразовательном учреждении «Средняя школа № 3 имени А.Н. Першиной» г. Енисейска Красноярского края

1.Общие положения

Модель актуальных угроз муниципального бюджетного общеобразовательного учреждения «Средняя школа № 3 имени А.Н. Першиной» г. Енисейска Красноярского края (далее Школа) разработана в соответствии с нормативными документами ФСТЭК России:

- Базовая модель безопасности персональных данных при их обработке в информационных системах персональных данных, 2008г.;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, 2008г.

Частная модель угроз содержит описание возможных угроз безопасности персональных данных и расчет актуальных угроз для ИСПДн Школы.

Частная модель угроз направлена на определение возможных каналов утечки, путем анализа защищенности ИСПДн Школы.

Под угрозами безопасности ПДн при их обработке в ИСПДн понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

В соответствии со статьей 19 Федерального закона №152-ФЗ от 27 июля 2006 г. «О персональных данных», ПДн должны быть защищены от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий. Угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн и (или) потребителей, пользующихся услугами, предоставляемыми ИСПДн в соответствии с ее назначением, так и со специально осуществляемыми неправомерными действиями иностранных государств, криминальных сообществ, отдельных организаций и граждан, а также иными источниками угроз.

Угрозы безопасности ПДн могут быть реализованы за счет утечки ПДн по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при ее передаче по каналам связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа с использованием соответствующего программного обеспечения.

2. Описание ИСПДн

2.1. Общие характеристики ИСПДн

№ п/н	Характеристика	Значение характеристики
1	Состав ИСПДн	**КИАСУО**
2	Назначение	Для проведения государственной итоговой аттестации учеников и осуществления образовательного процесса
3	Категория обрабатываемых в ИСПДн персональных данных	ИСПДн «Ученики» является информационной системой, обрабатывающей иные категории персональных данных, т.е. в ней не обрабатываются специальные категории персональных данных, биометрические персональные данные, общедоступные персональные данные.
4	Объем обрабатываемых ПДн (количество субъектов персональных данных, ПДн которых обрабатываются в ИСПДн)	Объем обрабатываемых в ИСПДн «Ученики» персональных данных менее 100000 субъектов персональных данных
5	Субъекты персональных данных	ИСПДн «Ученики» является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора персональных данных.
6	Структура ИСПДн	Локальная информационная система (используются комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа).
7	Подключение ИСПДн к сетям связи общего пользования и (или) сетям международного обмена	Имеет подключение к сетям международного информационного обмена.
8	Режим обработки персональных данных	Многопользовательский
9	Разграничение доступа	ИСПДн с разграничением прав доступа
10	Местонахождение технических средств ИСПДн	Все средства находятся в пределах Российской Федерации.
№ п/н	Характеристика	Значение характеристики
1	Состав ИСПДн	**Элжур**
2	Назначение	Для проведения государственной итоговой аттестации учеников и осуществления образовательного процесса
3	Категория обрабатываемых в ИСПДн персональных данных	ИСПДн «Ученики» является информационной системой, обрабатывающей иные категории персональных данных, т.е. в ней не обрабатываются специальные категории персональных данных, биометрические персональные данные, общедоступные персональные данные.
4	Объем обрабатываемых ПДн (количество субъектов персональных данных, ПДн которых обрабатываются в ИСПДн)	Объем обрабатываемых в ИСПДн «Ученики» персональных данных менее 100000 субъектов персональных данных
5	Субъекты персональных	ИСПДн «Ученики» является информационной системой,

	данных	обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора персональных данных.
6	Структура ИСПДн	Локальная информационная система (используются комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа).
7	Подключение ИСПДн к сетям связи общего пользования и (или) сетям международного обмена	Имеет подключение к сетям международного информационного обмена.
8	Режим обработки персональных данных	Многопользовательский
9	Разграничение доступа	ИСПДн с разграничением прав доступа
10	Местонахождение технических средств ИСПДн	Все средства находятся в пределах Российской Федерации.
№ п/н	Характеристика	Значение характеристики
1	Состав ИСПДн	**Питание**
2	Назначение	Для проведения государственной итоговой аттестации учеников и осуществления образовательного процесса
3	Категория обрабатываемых в ИСПДн персональных данных	ИСПДн «Ученики» является информационной системой, обрабатывающей иные категории персональных данных, т.е. в ней не обрабатываются специальные категории персональных данных, биометрические персональные данные, общедоступные персональные данные.
4	Объем обрабатываемых ПДн (количество субъектов персональных данных, ПДн которых обрабатываются в ИСПДн)	Объем обрабатываемых в ИСПДн «Ученики» персональных данных менее 100000 субъектов персональных данных
5	Субъекты персональных данных	ИСПДн «Ученики» является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора персональных данных.
6	Структура ИСПДн	Локальная информационная система (используются комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа).
7	Подключение ИСПДн к сетям связи общего пользования и (или) сетям международного обмена	Имеет подключение к сетям международного информационного обмена.
8	Режим обработки персональных данных	Многопользовательский
9	Разграничение доступа	ИСПДн с разграничением прав доступа
10	Местонахождение технических средств ИСПДн	Все средства находятся в пределах Российской Федерации.

4. Определение актуальных угроз безопасности персональных данных в ИСПДн

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн.

Актуальность угрозы определяется следующими параметрами:

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

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн.

Характеристики ИСПДн приведены в таблице:

№	Параметр	Значение	Уровень защищенности
1	Территориальное размещение	локальная ИСПДн, развернутая в пределах одного здания	Высокий
2	Наличие соединений с сетями общего пользования	ИСПДн, имеющая одноточечный выход в сеть общего пользования;	Средний
3	Встроенные (легальные) операции с записями баз персональных данных	Запись, удаление, сортировка	Средний
4	Разграничение доступа к персональным данным	ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	Средний
5	Наличие соединений с другими базами ПДн иных ИСПДн	ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	Высокий
6	Уровень обобщения (обезличивания) ПДн	ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	Средний
7	Объем ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	ИСПДн, предоставляющая часть ПДн;	Средний

Соотношение характеристик ИСПДн, соответствующих разным уровням защищенности:

- 29% характеристик ИСПДн соответствуют ***высокому*** уровню защищенности;
- 71% характеристик ИСПДн соответствуют ***среднему*** уровню защищенности;
- 0% характеристик ИСПДн соответствуют ***низкому*** уровню защищенности.

Уровень исходной защищенности ИСПДн – средний (Y_1=5).

По каждому виду угрозы, экспертным путем (опрос специалистов) определены:

- опасность (ущерб) в соответствии с правилами, приведенными в таблице 2.

Таблица 2

Опасность (ущерб) угрозы и её характеристики

Опасность (ущерб) угрозы		
Низкая	**Средняя**	**Высокая**
Реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных	Реализация угрозы может привести к негативным последствиям для субъектов персональных данных	Реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных

- вероятность реализации угрозы ($Y_{2)}$ в соответствии с правилами, приведенными в таблице 3.

Таблица 3

Вероятность угрозы и её характеристики

Вероятность	**Y2**
Маловероятно	0
Низкая	2
Средняя	5
Высокая	10

С учетом полученных числовых коэффициентов Y_1 и Y_2 по каждому виду угрозы безопасности ПДн рассчитывается числовой коэффициент реализуемости угрозы Y по формуле:

$$Y = (Y_1 + Y_2)/20$$

Соответствие значения числового коэффициента реализуемости угрозы Y и его возможной реализации приведено в таблице 4.

Таблица 4

Значения реализуемости

Значение числового коэффициента реализуемости угрозы Y	**Возможность реализации угрозы**
YЄ [0 ; 0.3]	Низкая
YЄ (0.3 ; 0.6]	Средняя
YЄ (0.6 ; 0.8]	Высокая
YЄ (0.8 ; 1]	Очень высокая

Актуальность угрозы безопасности ПДн определяется на основании значения коэффициента реализуемости угрозы (Y) и показателя опасности (ущерба) угрозы по каждому ее виду. Вывод об актуальности угрозы происходит в соответствии с правилами, представленными в таблице 5.

Таблица 5

Актуальность реализации угрозы

Возможн ость реализации угрозы	**Опасность угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Угрозы и их характеристики представлены в таблице 6. Таблица угроз и их характеристик приведена ниже.

5. Модель вероятного нарушителя

По наличию права постоянного или разового доступа в ИСПДн нарушители подразделяются на два типа:

- нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена – внешние нарушители;
- нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн – внутренние нарушители.

Внешними нарушителями могут быть:

- криминальные структуры;
- недобросовестные партнеры;
- внешние субъекты (физические лица).

Внешний нарушитель имеет следующие возможности:

- осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
- осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;
- осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
- осуществлять несанкционированные доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами контролируемой зоны.

Наименование угрозы	Вероятность (Y2)	Реализуемость (Y)	Опасность	Актуальность
Угрозы утечки информации по техническим каналам				
Угрозы утечки акустической (речевой) информации	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы утечки видовой информации	низкая вероятность (2)	низкая (0.35)	низкая	неактуальная
Угрозы утечки информации по каналу ПЭМИН	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы НСД к ПДн, обрабатываемым на автоматизированном рабочем месте				
Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	средняя вероятность (5)	средняя (0.5)	средняя	актуальная
Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	средняя вероятность (5)	средняя (0.5)	средняя	актуальная
Сетевые угрозы				
Угрозы "Анализа сетевого трафика" с перехватом передаваемой по сети информации	низкая вероятность (2)	низкая (0.35)	низкая	неактуальная
Угрозы выявления паролей	низкая вероятность (2)	низкая (0.35)	средняя	неактуальная
Угрозы удаленного запуска приложений	маловероятно (0)	низкая (0.25)	средняя	неактуальная
Угрозы внедрения по сети вредоносных программ	средняя вероятность (5)	средняя (0.5)	средняя	актуальная
Угрозы из внешних сетей				
Угрозы "Анализа сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	маловероятно (0)	низкая (0.25)	низкая	неактуальная

Угрозы выявления паролей	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы получения НСД путем подмены доверенного объекта	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы типа "Отказ в обслуживании"	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы удаленного запуска приложений	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы внедрения по сети вредоносных программ	средняя веро-ятность (5)	средняя (0.5)	средняя	актуальная

Категории нарушителей

№	Описание	Нарушитель может	Возможный нарушитель
1	Лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн.	– иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн; – располагать фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах; – располагать именами и вести выявление паролей зарегистрированных пользователей; – изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.	Сотрудники, не участвующие в обработке ПДн
2	Зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.	– обладает всеми возможностями лиц первой категории; – знает по меньшей мере одно легальное имя доступа; – обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн; – располагает конфиденциальными данными, к которым имеет доступ.	Сотрудники, обрабатывающие ПДн
3	Зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам	– обладает всеми возможностями лиц первой и второй категорий; – располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системам, через которую он осуществляет доступ, и составе технических средств ИСПДн; – имеет возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.	Отсутствует
4	Зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.	– обладает всеми возможностями лиц предыдущих категорий; – обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИСПДн; – обладает полной информацией о тех-	Отсутствует

		нических средствах и конфигурации сегмента (фрагмента) ИСПДн; – имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн; – имеет доступ ко всем техническим средствам сегмента (фрагмента) ИСПДн; – обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИСПДн.	
5	Зарегистрированные пользователи с полномочиями системного администратора ИСПДн	– обладает всеми возможностями лиц предыдущих категорий; – обладает полной информацией о системном и прикладном программном обеспечении ИСПДн; – обладает полной информацией о технических средствах и конфигурации ИСПДн; – имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн; – обладает правами конфигурирования и административной настройки технических средств ИСПДн.	Системный администратор ИСПДн
6	Зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн	– обладает всеми возможностями лиц предыдущих категорий; – 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).	Администратор безопасности ИСПДн
7	Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте	– обладает информацией об алгоритмах и программах обработки информации на ИСПДн; – обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения; – может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых	Отсутствует

		в ИСПДн.	
8	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн	– обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения; – может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.	Отсутствует

5. Выводы

5.1 В результате анализа возможных угроз безопасности персональных данных выявлено 3 актуальные угрозы безопасности:

№ п/п	Угроза	Вероятность	Опасность
1	Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	средняя вероятность (5)	средняя
2	Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	средняя вероятность (5)	средняя
3	Угрозы внедрения по сети вредоносных программ	средняя вероятность (5)	средняя

5.2 Выявленные актуальные угрозы безопасности ПДн в ИСПДн при их реализации могут привести к незначительным последствиям для субъектов ПДн. Необходимо провести мероприятия по устранению указанных угроз или снижению их уровня.

Приложение № 2
к приказу Об утверждении локальных актов по защите персональных данных

Меры по обеспечению безопасности персональных данных, обработка которых осуществляется без средств автоматизации в муниципальном бюджетном общеобразовательном учреждении «Средняя школа № 3 имени А.Н. Першиной» г. Енисейска Красноярского края

1.Меры по обеспечению безопасности персональных данных, обработка которых осуществляется без средств автоматизации (далее – Меры) в муниципальном бюджетном общеобразовательном учреждении «Средняя школа № 3 имени А.Н. Першиной» г. Енисейска Красноярского края (далее – Школа) разработано в соответствии со ст. 19 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", постановлением Правительства РФ от 15.09.2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

2. Меры определяют особенности обработки персональных данных осуществляемой без использования средств автоматизации, а так же меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а так же от иных неправомерных действий в отношении персональных данных.

3. Обработка персональных данных, осуществляемая без использования средств автоматизации, осуществляется таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

4. Обработка и доступ к персональным данным, в соответствии с категориями персональных данных, осуществляется в следующем порядке:

Биометрические персональные данные		Доступ
Приемная	Ведущий специалист по кадрам	Директор, заместитель директора по УР, заместитель директора по ВР, классные руководители, социальный педагог, педагог- психолог
	Документовед	
Специальные категории персональные данных		
Медицинский кабинет	Медицинский работник,	Директор, заместитель директора по УР, заместитель директора по ВР, классные руководители, социальный педагог, педагог - психолог, ведущий специалист по кадрам, документовед
Персональные данные работников		
Приемная	Ведущий специалист по	Директор, заместитель директора по

	кадрам	АХЧ, медицинский работник
Иные персональные данные		
Холл Школы	Вахтер	Директор, заместитель директора по АХЧ
Общедоступные персональные данные		
Все помещения Школы	Все работники Школы	Все работники Школы

5. Персональные данные, обработка которых осуществляется в различных целях, хранятся раздельно.

Персональные данные обработка, которых осуществляется в целях приема граждан на обучение по образовательным программам начального общего, основного общего и среднего общего образования в том числе, среднего общего образования с заочной формой обучения, контроля освоения обучающимися общеобразовательных программ хранятся в кабинете приемной в специально отведенном шкафу и находятся в делопроизводстве документоведа.

Персональные данные обработка, которых осуществляется в целях заключения, исполнения гражданско-правовых договоров хранятся в кабинете библиотеки в специально отведенном шкафу и находится в делопроизводстве заместителя директора по АХЧ.

Персональные данные обработка, которых осуществляется в целях соблюдения пропускного режима хранятся в холле Школы на специально отведенном столе и находится в делопроизводстве вахтера.

Персональные данные обработка, которых осуществляется в целях ведения кадрового делопроизводства, установления педагогической нагрузки педагогическим работникам, повышения профессиональных компетенций работников, определения размера заработной платы работника хранятся кабинете приемной в специально отведенном сейфе и находятся в делопроизводстве ведущего специалиста по кадрам.

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

7. Лицо в делопроизводстве которого находятся персональные данные принимает все необходимые организационные и технические меры, исключающие возможность несанкционированного доступа к материальным носителям ПД лиц, не допущенных к их обработке. Материальные носители с ПД хранятся в запирающихся на ключ помещениях, металлических шкафах, сейфах, иных шкафах, имеющих запираемые блоксекции.

8. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

9. Лицам, осуществляющим обработку персональных данных, запрещается разглашать информацию, содержащую персональные данные, устно или письменно кому бы то ни было.

10. Лицо, осуществляющие обработку персональных данных без использования средств автоматизации: - определяет места хранения персональных данных (материальных носителей);

- осуществляет контроль наличия в подразделении условий, обеспечивающих сохранность ПД и исключающих несанкционированный к ним доступ;

- организует раздельное хранение материальных носителей персональных данных (документов, дисков, USB флеш-накопителей, пр.), обработка которых осуществляется в различных целях.

Приложение № 3
к приказу Об утверждении локальных актов по защите персональных данных

Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в муниципальном бюджетном общеобразовательном учреждении «Средняя школа № 3 имени А.Н. Першиной» г. Енисейска Красноярского края

Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее – Меры) в муниципальном бюджетном общеобразовательном учреждении «Средняя школа № 3 имени А.Н. Першиной» г. Енисейска Красноярского края (далее – Школа) разработаны в соответствии с пп. 2 ч. 2 ст. 19 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных", постановление Правительства РФ от 01.11.2012 № 1119 « Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, копирования, предоставления, распространения персональных данных, а так же от иных неправомерных действий в отношении персональных данных и направлены на нейтрализацию актуальных угроз безопасности персональных данных.

Уровни защищенности персональных данных

Тип ИСПДн	Сотрудники Школы	Количество субъектов	Тип актуальных угроз		
			1 НДВ ОС	2 НДВ ПО	3 Без НДВ
Специальные			1		
	+			2	
		< 100000		2	
		> 100000			2
	+				3
		< 100000			3
Биометрические			1		
				2	
					3
Иные			1		
		> 100000		2	
	+			3	
		< 100000			3
		> 100000			3
	+				4
		< 100000			4
Общедоступные			2		
		> 100000		2	
	+			3	
		< 100000		3	
					4

Анализ уровня защищенности персональных данных показывает, что для информационных систем, используемых в Школе, актуальны угрозы 2-го типа и информационные системы обрабатывают иные категории персональных данных сотрудников Школы или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками Школы, что соответствует 3 уровню защищенности персональных данных.

Для обеспечения 3 уровня защищенности персональных данных применяются:
средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса защиты в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса защиты в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

межсетевые экраны не ниже 3 класса в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и межсетевые экраны не ниже 4 класса в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена.

Для обеспечения 3-го уровня защищённости персональных данных при их обработке в информационных системах выполняются следующие требования:

- Организован режим обеспечения безопасности помещений, в которых размещены информационные системы, препятствующий возможность неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- Обеспечена сохранность носителей персональных данных;

- Определён перечень лиц, доступ к которым к персональным данным, обрабатываемым в информационных системах, необходим для выполнения ими трудовых обязанностей;

- Используются средства защиты персональных данных.

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

регистрация событий безопасности;

антивирусная защита;

контроль (анализ) защищенности персональных данных;

защита среды виртуализации;

защита технических средств;

защита информационной системы, ее средств, систем связи и передачи данных;

управление конфигурацией информационной системы и системы защиты персональных данных.

Меры по идентификации и аутентификации субъектов доступа и объектов доступа заключаются в присвоении субъектам и объектам доступа уникального признака (идентификатора), сравнении предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также в проверке принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

Меры по управлению доступом субъектов доступа к объектам доступа заключаются в управлении правами и привилегиями субъектов доступа, разграничении доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также в обеспечении контроля за соблюдением этих правил.

Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) заключаются в исключении возможности несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированного использования съемных машинных носителей персональных данных.

Меры по регистрации событий безопасности заключаются в обеспечении сбора, записи, хранения и защиты информации о событиях безопасности в информационной системе, а также возможности просмотра и анализа информации о таких событиях и реагирование на них.

Меры по антивирусной защите заключаются в обеспечении обнаружения в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации.

Меры по контролю (анализу) защищенности персональных данных заключаются в

обеспечении контроля уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестировании работоспособности системы защиты персональных данных.

Меры по защите среды виртуализации заключаются в исключении несанкционированного доступа к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействия на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

Меры по защите технических средств заключаются в исключении не санкционированного доступа к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защите технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны заключаются в обеспечении защиты персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

Меры по управлению конфигурацией информационной системы и системы защиты персональных данных заключаются в обеспечении управления изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

Приложение № 4
к приказу Об утверждении локальных актов по защите персональных данных

Порядок осуществления контроля за принимаемыми мерами по обеспечению безопасности персональных данных при их обработке в информационных системах и уровня защищённости информационных систем персональных данных в муниципальном бюджетном общеобразовательном учреждении «Средняя Школа № 3 имени А.Н. Першиной» г. Енисейска Красноярского края

1. Порядок осуществления контроля за принимаемыми мерами по обеспечению безопасности персональных данных при их обработке в информационных системах и уровня защищённости информационных систем персональных данных (далее - Порядок) в муниципальном бюджетном общеобразовательном учреждении «Средняя школа № 3 имени А.Н. Першиной» г. Енисейска Красноярского края (далее – Школа) определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок и формы проведения контроля в Школе.

2. В целях осуществления контроля за принимаемыми мерами по обеспечению безопасности персональных данных при их обработке в информационных системах (далее – Меры) и уровня защищённости информационных систем персональных данных (далее-УЗ) в Школе организуется проведение плановых и внеплановых проверок соблюдения Мер и УЗ.

3. Проверки осуществляются лицом ответственным за организацию обработки персональных данных в Школе.

4. Плановая проверка проводится в соответствии с планом, утвержденным директором.

5. Плановые проверки должны проводиться не реже одного раза в год. Срок проведения плановой проверки составляет не более 1 месяца.

6. В плане по каждой проверке устанавливаются объекты внутреннего контроля, проверяемый период, срок проведения проверки, ответственные исполнители.

7. Внеплановая проверка проводится по решению директора:

на основании письменного указания вышестоящих органов;

на основании поступившего заявления субъекта персональных данных или его законного представителя о нарушении законодательства в области персональных данных;

в связи с проведением государственного контроля (надзора) за соответствием защиты персональных данных требованиям законодательства Российской Федерации в области защиты персональных данных;

на основании докладной либо служебной записки ответственного за организацию обработки персональных данных о выявленных фактах нарушения работниками требований к защите персональных данных, установленных Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами;

по иным основаниям, на усмотрение директора.

8. Проведение внеплановой проверки организуется в течение пяти рабочих дней с момента возникновения соответствующего основания. Срок проведения внеплановой проверки не может превышать месяца со дня принятия решения о ее проведении.

9. Результаты проверки оформляются в виде заключения.

10. При выявлении в ходе проверки нарушений в заключении отражается перечень

мероприятий по устранению выявленных нарушений с указанием сроков.

11. О результатах проверки и мерах, необходимых для устранения выявленных нарушений, директору докладывает лицо ответственное за организацию обработки персональных данных.

12. В рамках мероприятий по контролю проверяется:

- уровень защищённости персональных данных;
- применение организационно-технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
- применение средств защиты персональных данных;
- проведение оценки эффективности принимаемых Мер;
- ведение учёта машинных носителей персональных носителей;
- соблюдение правил доступа к персональным данным обрабатываемым в информационных системах.

Приложение № 5
к приказу Об утверждении локальных актов по защите персональных данных

Порядок учета машинных носителей персональных данных в муниципальном бюджетном общеобразовательном учреждении «Средняя Школа № 3 имени А.Н. Першиной» г. Енисейска Красноярского края

В целях соблюдения требований п. 5 ч. 2 ст. 19 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, в Школе установлен следующий порядок учёта машинных носителей персональных данных.

Учету подлежат:

- съемные машинные носители персональных данных (флэш-накопители, внешние накопители на жестких дисках и иные устройства);
- портативные вычислительные устройства, имеющие встроенные носители персональных данных (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);
- машинные носители персональных данных, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

Учет машинных носителей персональных данных включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей персональных данных, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители персональных данных, и иные номера.

Учет машинных носителей персональных данных ведется в журнале учета машинных носителей персональных данных (Приложение 1).

Учет встроенных в портативные или стационарные технические средства машинных носителей персональных данных может вестись в журналах материально-технического учета в составе соответствующих технических средств. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей персональных данных, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

Приложение № 1 к Порядку учета машинных носителей персональных данных утверждённому приказом Об утверждении локальных актов по защите персональных данных от №

ЖУРНАЛ УЧЁТА МАШИННЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

№ пп	Наименование	Регистрационный номер	Тип и ёмкость	Место использования	Ответственное лицо (должность, ФИО)	Информация об уничтожении	Роспись в получении	Роспись в приёме