Ханты-Мансийский автономный округ - Югра
(Тюменская область)

АДМИНИСТРАЦИЯ НИЖНЕВАРТОВСКОГО РАЙОНА

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ИЗЛУЧИНСКАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ СРЕДНЯЯ ШКОЛА №2 С УГЛУБЛЕННЫМ ИЗУЧЕНИЕМ ОТДЕЛЬНЫХ ПРЕДМЕТОВ»

ПРИКАЗ

ул. Школьная, 7, г.п. Излучинск, Нижневартовский район,
Ханты-Мансийский автономный округ – Югра (Тюменская область), 628634
Тел./Факс: 28-25-60 / 28-39-59, E-mail: mosh-2@mail.ru

___10.01.2017___ № _012__

Об утверждении инструкций

В соответствии с Федеральным законом от 29.12.2012 года № 273-ФЗ «Об образовании в Российской Федерации», Федеральным законом от 27.07.2010г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», распоряжением Правительства РФ от 17.12.2009г. № 1993-р «Об утверждении сводного перечня первоочередных государственных и муниципальных услуг, предоставляемых в электронном виде», Уставом Школы и настоящим Положением:

Приказываю:

1. Утвердить:

1.1 Инструкцию по выполнению режимных мер и допуску к муниципальной информационной системе района «МИС ОО» (Приложение 1);

1.2 Инструкцию пользователю муниципальной информационной системы персональных данных МИС «ОО» в части обеспечения безопасности персональных данных при их обработке в информационной системе (Приложение 2);

1.3 Инструкцию по использованию программных и аппаратных средств защиты информации (Приложение 3);

1.4 Инструкция администратору информационной безопасности муниципальной информационной системы персональных данных МИС «ОО» (Приложение 4);

2. Разместить настоящий приказ на официальном сайте учреждения в течение десяти рабочих дней со дня издания настоящего приказа.

3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор А.Д. Грибецкая

Приложение № 1
к приказу МБОУ «Излучинская ОСШ УИОП № 2»
от «10» _января_ 2017г. № 010

Инструкция по выполнению режимных мер и допуску к муниципальной информационной системе района «МИС ОО»

Обозначения и сокращения

ОО	– образовательные организации;
АРМ	– автоматизированное рабочее место;
МИС	– муниципальная информационная система;
КЗ	– контролируемая зона;
ОТСС	- основные технические средства и системы;
ПДн	– персональные данные;
ПЭВМ	– персональная электронно-вычислительная машина;
СВТ	– средства вычислительной техники;
СЗИ	– средства защиты информации;
СЗПДн	– система (подсистема) защиты персональных данных;
УБПДн	– угрозы безопасности персональных данным.
ЭВМ	– электронно-вычислительная машина.

1. Общие положения.

1.1. Инструкция по выполнению режимных мер и допуску МИС (далее - Инструкция) предназначена для руководящего состава ОО, преподавательского состава ОО, и регулирует порядок допуска пользователей к работе в МИС ОО.

1.2. Правила, устанавливаемые положениями Инструкции обязательны для исполнения.

2. Порядок допуска к МИС и в помещения размещения ОТСС.

2.1. Приведённый в инструкции порядок направлен на достижение следующих задач:

– допуск к информации, обрабатываемой в ИС строго определённого перечня лиц;

– самостоятельный допуск в помещения с установленными в них ОТСС ИС строго определённого перечня лиц;

– закрепление за каждым пользователем определённого ему для работы АРМ ИС и определённых ему информационных ресурсов в ИС.

2.2. Для выполнения задач, обозначенных в п. 2.1 Инструкции, создаются следующие распорядительные инструменты:

– «Перечень лиц, имеющих право доступа к обработке сведений, содержащихся в муниципальной информационной системе «МИС ОО». Содержит перечень лиц (ФИО, должность), имеющих право допуска к каждому АРМ МИС. Разрабатывается и актуализируется администратором информационной безопасности в порядке, описанном данной инструкцией. Копия списка вывешивается в каждом помещении размещения ОТСС МИС в целях исключения допуска к работе с АРМ не закреплённых за ними пользователей;

– «Разрешительная система доступа персонала к информационным ресурсам «МИС ОО». Разрабатывается и актуализируется администратором информационной безопасности в порядке, описанном данной инструкцией. Находится в доступном сотрудникам и техническим специалистам Школы;

– «Перечень лиц, имеющих право самостоятельного (неконтролируемого) пребывания в помещениях размещения ОТСС муниципальной информационной системы персональных данных МИС «ОО». Содержит сведения о помещениях и перечень лиц (ФИО,

должность), имеющих право самостоятельного доступа в помещения, снятия помещения с охраны и получения ключей от него. Готовится и поддерживается в актуальном состоянии администратором информационной безопасности.

Все указанные документы утверждаются директором.

2.3. Для работы в МИС ПДн каждый пользователь должен получить соответствующий допуск. Под допуском к МИС ПДн понимается возможность самостоятельного доступа пользователя к средствам информатизации МИС ПДн (средства электронно-вычислительной техники, системы и сети ЭВМ, системы и сети электросвязи, программные средства). Право допуска предоставляется пользователю только после включения его в «Перечень лиц, имеющих право доступа к обработке сведений, содержащихся в муниципальной информационной системе персональных данных МИС «ОО».

Устные указания кого бы то ни было об установлении права доступа пользователю к МИС ПДн либо об изменении его прав доступа не имеют юридической силы и необязательны для исполнения. Сотрудники Школы и администратор информационной безопасности не могут быть наказаны за невыполнение подобного указания от вышестоящего руководителя.

Процедура получения (лишения прав) соответствующего права допуска пользователя для сотрудника Школы инициируется заявкой начальника отдела, в котором числится сотрудник в адрес директора Школы. (Приложение № 1), только после назначения сотрудника на должность директором Школы, и подписания новым сотрудником обязательства о неразглашении персональных данных (Приложение № 2). Подписание и хранение обязательства о неразглашении персональных данных в личном деле организовывается сотрудниками по кадрам.

Директор школы передает заявку администратору информационной безопасности.

Администратор информационной безопасности:

– Вносит соответствующие изменения в «Перечень лиц, имеющих право доступа к обработке сведений, содержащихся в муниципальной информационной системе персональных данных МИС «ОО» и «Разрешительную систему доступа персонала к информационным ресурсам МИС ПДн МИС «ОО».

– Обновлённый «Перечень лиц, имеющих право доступа к обработке сведений, содержащихся в муниципальной информационной системе персональных данных МИС «ОО» и «Разрешительная система доступа персонала к информационным ресурсам МИС ПДн МИС «ОО» представляется на утверждение директору.

– После утверждения указанных документов администратор информационной безопасности обеспечивает:

1) Регистрацию (удаление) персонального имени (учетная запись пользователя) и пароля, под которым пользователь регистрируется и работает в системе в соответствии с «Инструкцией по организации парольной защиты в муниципальной информационной системе персональных данных МИС «ОО»;

2) Внесение необходимых изменений администратором сети, серверов, баз данных в списки пользователей соответствующих подсистем и СУБД;

3) Настройку средств защиты и программного обеспечения АРМ пользователя, соответствующим категориям защиты.

Заявки хранятся у администратора информационной безопасности.

– Обновлённый «Перечень лиц, имеющих право доступа к обработке сведений, содержащихся в муниципальной информационной системе персональных данных МИС «ОО» рассылается администратором информационной безопасности заинтересованным сотрудникам Школы.

– Начальник отдела, в котором числится пользователь, контролирует внесение изменений в должностные инструкции пользователя и допускает сотрудника к работе в МИС ПДн. Директором Школы утверждаются необходимые изменения в «Перечень лиц, имеющих право самостоятельного (неконтролируемого) пребывания в помещениях

размещения ОТСС муниципальной информационной системы персональных данных МИС «ОО».

– При исключении пользователя МИС ПДн из «Перечня лиц, имеющих право доступа к обработке сведений, содержащихся в муниципальной информационной системе персональных данных МИС «ОО» руководителю отдела, в котором числится пользователь, необходимо направлять заявку в адрес директора школы до момента объявления пользователю о лишении его прав на допуск к МИС ПДн. Обязательным является заведомое уведомление директором школы о планируемом лишении прав доступа или изменения полномочий сотрудника по доступу к ресурсам МИС ПДн администратора информационной безопасности. Администратором информационной безопасности принимаются меры по исключению возможности нарушения данным лицом характеристик безопасности информации МИС ПДн.

2.4. По таким же правилам происходит включение (исключение) в «Перечень лиц, имеющих право самостоятельного (неконтролируемого) пребывания в помещениях размещения ОТСС муниципальной информационной системы персональных данных МИС «ОО».

2.5. Действующими утверждёнными «Перечнем лиц, имеющих право доступа к обработке сведений, содержащихся в муниципальной информационной системе персональных данных МИС «ОО» и «Перечнем лиц, имеющих право самостоятельного (неконтролируемого) пребывания в помещениях размещения ОТСС муниципальной информационной системы персональных данных МИС «ОО» в своей повседневной деятельности руководствуются руководители отделов, эксплуатирующих МИС ПДн, технические специалисты и администратор информационной безопасности. Перечни лиц находятся в рабочем кабинете администратора информационной безопасности, в целях использования сотрудниками Школы в ежедневной деятельности и с целью контроля соблюдения установленных перечней допущенных лиц.

3. Требования по организации режимных мер.

3.1. Состав МИС ПДн должен соответствовать техническому паспорту. Обработка не учтённых в техпаспорте технических средств запрещается. Все технические средства МИС ПДн должны размещаться в соответствии с техническим паспортом.

Изменение состава ОТСС в составе МИС ПДн допускается только после согласования с органом по аттестации. В адрес органа по аттестации направляется письменное уведомление о планируемых изменениях. Изменения осуществляются после получения рекомендаций органа по аттестации. Ответственным за данные мероприятия является директор Школы.

Полный порядок действий при модификации, обновлении программного обеспечения и других изменениях в МИС ПДн приведён в «Инструкции по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств муниципальной информационной системы персональных данных МИС «ОО».

Контроль соблюдения данных требований и ведения учета средств информатизации МИС ПДн возлагается на администратора информационной безопасности.

3.2. Помещения, в которых размещаются ОТСС МИС ПДн, должны исключать возможность бесконтрольного проникновения в него посторонних лиц. Помещения должны быть оборудованы пожарной сигнализацией, находящейся в работоспособном состоянии.

Допуск в здание осуществляется в соответствии с требованиями «Инструкции об организации охраны в МБОУ «Излучинская ОСШ УИОП №2», утвержденную приказом от 1.09.2016 № _____ «Об организации охраны, пропускного режима в здании и на территории МБОУ «Излучинская ОСШ УИОП №2» в 2016-2017 учебном году». Администратор информационной безопасности имеет право контролировать и проверять исполнение данной инструкции всеми сотрудниками Школы и организацией, осуществляющей охрану здания, в котором расположены помещения Школы.

Помещение, в котором размещается ОТСС МИС ПДн, должно исключать возможность бесконтрольного проникновения в него посторонних лиц. Уборка помещения должна осуществляться в присутствии сотрудников, имеющих право самостоятельного допуска в помещение.

Ключи от помещений хранятся у сотрудников, передача ключа посторонним лицам строго запрещена. Вскрытие помещения возможно только в присутствии лиц, имеющих право самостоятельного доступа в помещение в соответствии с утвержденным списком или в присутствии администратора информационной безопасности.

При обнаружении факта несанкционированного проникновения в помещения лиц, не входящих в «Перечень лиц, имеющих право самостоятельного (неконтролируемого) пребывания в помещениях размещения ОТСС муниципальной информационной системы персональных данных МИС «ОО», администратор информационной безопасности или другие лица (в зависимости от обнаружившего данный факт) обязаны немедленно сообщить о происшедшем директору Школы.

По данному происшествию проводится служебная проверка с установлением последствий проникновения для безопасности информации (нарушение целостности, доступности и конфиденциальности), обрабатываемой в МИС ПДн.

При утере ключа от помещения сотрудники, имеющие право допуска в помещение, обязаны сообщить о случившемся администратору информационной безопасности. Руководством принимаются меры по исключению возможности хищения носителей информации и ОТСС МИС ПДн (замена замков или другие меры).

3.3. Технические средства АРМ в помещении размещаются таким образом, чтобы исключить возможность просмотра экрана видеомонитора и распечаток принтера лицами, не имеющими отношения к обрабатываемой информации. Не допускается перемещение АРМ в другие помещения.

3.4. Ключи от сейфа, расположенного в кабинете заместителя директора и используемого для хранения дистрибутивов (резервных копий) средств защиты информации и резервных копий ПДн, хранятся у заместителей директора.

3.5. Техническое обслуживание и ремонт средств информатизации проводится в соответствии с «Инструкцией по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств информационной системы МИС «ОО».

4. Ответственность за нарушение режимных мер.

Ответственность за обеспечение безопасности информации в МИС ПДн, своевременную разработку и осуществление необходимых мероприятий по обеспечению безопасности информации несёт администратор информационной безопасности. Контроль за обеспечением режима безопасности информации и требований настоящей Инструкции возлагается на ответственного за организацию обработки персональных данных.

За соблюдение непосредственно подчинёнными сотрудниками действующего законодательства в области защиты информации, «Инструкции пользователю муниципальной информационной системы персональных данных МИС «ОО», «Инструкции по проведению антивирусного контроля муниципальной информационной системы персональных данных МИС «ОО», «Инструкции по организации парольной защиты в муниципальной информационной системе персональных данных МИС «ОО», «Инструкции по резервному копированию и восстановлению данных в муниципальной информационной системе персональных данных МИС «ОО», «Инструкции по резервному копированию и восстановлению данных в муниципальной информационной системе персональных данных МИС «ОО» и других документов Школы в части обеспечения безопасности информации отвечает ответственный за организацию обработки персональных данных. При методической поддержке администратора информационной безопасности он организуют изучение подчинёнными сотрудниками требований организационно – распорядительных документов Школы при работе в МИС ПДн. Каждому сотруднику Школы должна быть предоставлена возможность изучить свои обязанности и правила работы в МИС ПДн.

Факт нарушения требований настоящей Инструкции является чрезвычайным происшествием. По каждому случаю проводится служебная проверка.

Невыполнение требований настоящей Инструкции рассматривается как нарушение трудовой дисциплины и влечет за собой наложение дисциплинарного взыскания.

Настоящая Инструкция доводится до заинтересованных сотрудников Школы под роспись.

Приложение № 1
к инструкции по выполнению режимных мер и допуску
к муниципальной информационной
системе персональных данных
МИС «ОО»
На имя директора

ЗАЯВКА
на внесение изменений в списки пользователей
МИС ПДн МИС «ОО»
и наделение пользователей полномочиями доступа к ресурсам системы

Прошу зарегистрировать пользователем (исключить из списка пользователей, изменить полномочия пользователя) в МИС ПДн МИС «ОО»

_____ _____
(ненужное зачеркнуть)

_____
(должность с указанием подразделения)

_____
(фамилия имя и отчество сотрудника)

предоставив ему полномочия, необходимые (лишив его полномочий, необходимых)
(ненужное зачеркнуть)
для решения задач:

_____
(список задач согласно формуляров задач)

_____
_____
_____
_____
_____на
следующих рабочих местах (АРМ):

_____
(номер помещения, зав.или инвент.номера АРМ)

«___» _____ 20__ г.

_____ _____
(подпись) (ФИО)

Приложение № 2
к инструкции по выполнению режимных мер и допуску
к муниципальной информационной системе
персональных данных
МИС «ОО»

Обязательство о неразглашении информации, обрабатываемой в муниципальной информационной системе персональных данных МИС «ОО»

Я,_____
(фамилия, имя, отчество, должность)
Муниципального бюджетного учреждения «_____ общеобразовательная средняя школа», далее по тексту – Школа, в период трудовых (служебных) отношений со Школой и в течение 5 лет после их окончания обязуюсь:
1. не разглашать сведения конфиденциального характера, содержащие персональные данные, которые станут мне известны при выполнении служебных (трудовых) обязанностей или иным путем;
2. не передавать третьим лицам и не раскрывать публично сведения конфиденциального характера, содержащие персональные данные, без согласия субъектов персональных данных;
3. выполнять относящиеся ко мне требования приказов, инструкций и положений по обеспечению безопасности персональных данных, обрабатываемых в Школе;
4. в случае попытки посторонних лиц получить от меня персональные данные, обрабатываемые в Школе немедленно сообщить об этом непосредственному руководителю и ответственному за организацию обработки персональных данных в Школе;
5. в случае моего увольнения, все носители персональных данных, которые находились в моем распоряжении в связи с выполнением мною служебных обязанностей во время работы в Школе, сдать лицу, ответственному за учет и хранение;
6. об утрате или недостаче носителей персональных данных, а также о причинах и условиях возможной утечки персональных данных немедленно сообщить непосредственному руководителю и ответственному за организацию обработки персональных данных в Школе.
Я предупрежден(а), что разглашение персональных данных, обрабатываемых в Школе, утрата носителей персональных данных, передача третьим лицам, публикация без согласия субъекта персональных данных, а также использование для занятия любой деятельностью, которая может нанести ущерб субъекту персональных данных, влечет уголовную, административную, гражданско-правовую или иную ответственность в соответствии с действующим законодательством, в виде лишения свободы, денежного штрафа и других наказаний.
До моего сведения также доведены с разъяснениями соответствующие положения, инструкции, приказы по обеспечению безопасности персональных данных.

«___»_____ 20___г. _____
(ФИО)

Один экземпляр обязательств получил _____
(подпись)

Приложение № 1
к приказу МБОУ «Излучинская ОСШ УИОП № 2»
от «10» _января_ 2017г. № 010

Инструкция пользователю муниципальной информационной системы персональных данных МИС «ОО» в части обеспечения безопасности персональных данных при их обработке в информационной системе

Обозначения и сокращения

Школа – МБОУ «_____»
АРМ – автоматизированное рабочее место;
ИБ – информационная безопасность;
МИС ПДн – муниципальная информационная система персональных данных МИС «ОО»;
ЗИ – защита информации;
ОТСС – основные технические средства и системы;
ПДн – персональные данные;
ПЭВМ – персональная электронно-вычислительная машина;
СВТ – средства вычислительной техники;
СЗИ – средства защиты информации;
СЗПДн – система (подсистема) защиты персональных данных;
УБПДн – угрозы безопасности персональным данным;
НСД – не санкционированный доступ.

1. Общие положения

1.1. Инструкция пользователя (далее Инструкция) МИС ПДн предназначена для пользователей всех уровней (руководителей и сотрудников) и регулирует порядок работы пользователей в МИС ПДн, определяет общие обязанности, права и ответственность по обеспечению информационной безопасности при работе в МИС ПДн.

1.2. Пользователем МИС ПДн (далее Пользователь) является сотрудник Школы, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным МИС ПДн, в соответствии с перечнем лиц, допущенных к МИС ПДн. Пользователь должен принимать все необходимые меры по защите информации и контролю за соблюдением прав доступа к ней.

1.3. Положения Инструкции обязательны для исполнения всеми пользователями.

1.4. Все пользователи должны быть ознакомлены под расписку с Инструкцией и предупреждены об ответственности за её нарушение.

1.5. По уровню ответственности и правам доступа к ИС пользователи разделяются на следующие категории: администратор информационной безопасности и пользователи.

2. Основные положения Инструкции

2.1.При первичном допуске к работе в МИС ПДн Пользователь изучает требования настоящей инструкции, разрешительную систему доступа к МИС ПДн и руководящие, нормативно-методические и организационно-распорядительные документы по вопросам обеспечения безопасности информации.

2.2.Каждый пользователь МИС ПДн, имеющий в рамках своих обязанностей доступ к аппаратным средствам, программному обеспечению и данным МИС ПДн, несет персональную ответственность за свои действия и **обязан**:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами МИС ПДн, в том числе положения настоящей Инструкции;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на его рабочей станции;
- располагать ОТСС в соответствии с техническим паспортом;
- хранить в тайне свой пароль (пароли). Парольную защиту организовывать в соответствии с Инструкцией по организации парольной защиты;
- выполнять требования Инструкция по проведению антивирусного контроля;
- немедленно вызывать администратора информационной безопасности и ставить в известность руководителя подразделения при подозрении компрометации личных ключей и паролей или при обнаружении фактов совершения в его отсутствие попыток НСД к ОТСС ИС;
- в случае появления у пользователя сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах или попытках несанкционированного удаленного доступа к информации, размещенной на контролируемом в МИС ПДн компьютере, пользователь должен немедленно сообщить об этом администратору информационной безопасности;
- немедленно сообщать администратору информационной безопасности об обнаруженных фактах нарушения настоящей Инструкции кем-либо;
- сообщать администратору информационной безопасности об отклонениях в нормальной работе установленных на АРМ средств защиты информации;
- при работе в МИС ПДн выполнять только служебные задания;
- при отсутствии необходимости работы выключить компьютер;
- при работе в МИС ПДн использовать только учтенные съемные носители, при обоснованной необходимости использования неучтённых носителей согласовывать использование с администратором информационной безопасности. После того как цель переноса информации на носители достигнута (переданы третьим лицам и т.п.) информация незамедлительно удаляется с носителей;
- осуществлять установленным порядком уничтожение информации (сочетанием клавиш Shift+Del), содержащей сведения конфиденциального характера, с машинных (съемных) носителей информации;
- немедленно выполнять предписания администратора информационной безопасности в части обеспечения безопасности информации;
- экран видеомонитора в помещении располагать во время работы так, чтобы исключалась возможность ознакомления с отображаемой на нем информацией посторонними лицами;
- соблюдать установленный режим разграничения доступа к информационным ресурсам;
- не разглашать известную им информацию, составляющую ПДн лицам, не имеющим допуска к этой информации;
- все изменения конфигурации технических и программных средств МИС ПДн, ремонт, модификация и техническое обслуживание технических средств и систем, входящих в состав МИС ПДн производить только на основании инструкции по модернизации, ремонту, техобслуживанию;

2.3. Пользователю запрещается:

- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств, устанавливать или удалять установленные техническим специалистом (администратором информационной безопасности) сетевые программы на компьютерах, вскрывать компьютеры, сетевое и периферийное оборудование, подключать к компьютеру дополнительное оборудование, вносить какие-либо

изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства без согласования с администратором информационной безопасности;

- привлекать посторонних лиц для производства ремонта ОТСС без письменной заявки и согласования с администратором информационной безопасности;
- запускать любые системные или прикладные программы, не входящие в состав программного обеспечения;
- работать с неучтенными машинными (съемными) носителями информации;
- отключать (блокировать) средства защиты информации;
- производить какие-либо изменения в размещении технических средств;
- обрабатывать на СВТ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам;
- сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам СВТ;
- хранить на учтенных носителях программы и данные, не относящиеся к рабочей информации;
- выполнять работы с документами ограниченного распространения на дому, выносить их за пределы контролируемой зоны;
- передавать свои учтённые носители кому-либо;
- вводить в ОТСС персональные данные под диктовку или с микрофона;
- осуществлять попытки несанкционированного доступа к ресурсам МИС ПДн, проводить или участвовать в сетевых атаках и сетевом взломе;
- производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) рабочих станций и серверов;
- закрывать доступ к информации паролями без согласования с администратором информационной безопасности;
- оставлять без личного присмотра на рабочем месте или где бы то ни было персональное устройство идентификации, машинные (съемные) носители и распечатки, содержащие защищаемую информацию;

2.4.**Пользователь обязан обеспечить:**

- блокирование своей учетной записи в случае кратковременного оставления АРМ (нажатием клавиш Windows+L);
- обязательное выключение компьютера после завершения работы;

2.5.Права пользователя:

- участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов МИС ПДн, если данное нарушение произошло под его идентификационными данными;
- своевременно получать доступ к информационным ресурсам МИС ПДн, необходимым ему для выполнения своих должностных обязанностей;
- требовать от администратора информационной безопасности смены идентификационных данных в случае появления сведений или подозрений на то, что эти данные стали известны третьим лицам.

2.6.Ответственность:

2.6.1.Пользователь несет персональную ответственность за соблюдение установленных требований во время работы. Пользователи, виновные в нарушении законодательства Российской Федерации о защите прав собственности и охраняемых по Закону сведений, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством и организационно распорядительными документами;

2.6.2.Пользователь компьютера отвечает за информацию, хранящуюся на его компьютере, технически исправное состояние компьютера и вверенной техники;

2.6.3.Нарушение данной инструкции, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом компьютерной информации, нарушение работы компьютеров пользователей или МИС ПДн в целом, может повлечь ответственность в соответствии с действующим законодательством.

Порядок использования съемных носителей информации.

Под использованием съемных носителей информации в МИС ПДн понимается их подключение к АРМ с целью обработки, приема/передачи информации между АРМ и носителями информации.

В МИС ПДн допускается использование только учтенных съемных носителей информации, которые являются собственностью Школы и подвергаются регулярной ревизии и контролю.

Съемные носители информации предоставляются пользователям МИС ПДн по инициативе руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у сотрудника Школы производственной необходимости.

Порядок учета, хранения и обращения со съемными носителями, твердыми копиями и их утилизации.

Все находящиеся на хранении и в обращении съемные носители в МИС ПДн подлежат учёту.

Каждый съемный носитель должен иметь этикетку, на которой указывается его уникальный учетный номер.

Для получения электронного внешнего носителя, пользователь обращается к руководителю структурного подразделения, руководитель структурного подразделения пишет служебную записку на имя ответственного за организацию обработки персональных данных о выдаче пользователю внешнего электронного носителя, далее ответственный за организацию обработки персональных данных принимает решение и передает служебную записку администратору информационной безопасности.

Учет и выдачу съемных носителей осуществляет администратор информационной безопасности, на которого возложена эта функция. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей конфиденциальной информации.

При использовании сотрудниками съемных носителей информации необходимо:

- соблюдать требования настоящей Инструкции;
- использовать носители информации исключительно для выполнения своих служебных обязанностей;
- ставить в известность администратора информационной безопасности о любых фактах нарушения требований настоящей Инструкции;
- бережно относиться к носителям информации;
- извещать администратора информационной безопасности о фактах утраты (кражи) носителей информации;

При использовании носителей конфиденциальной информации запрещено:

- использовать носители конфиденциальной информации в личных целях;
- передавать носители конфиденциальной информации другим лицам (за исключением администратора информационной безопасности);
- хранить съемные носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- выносить съемные носители с конфиденциальной информацией (персональными данными) за пределы контролируемой зоны для работы с ними на дому и т. д.

Любое взаимодействие (обработка, прием/передача информации), инициированное пользователем МИС ПДн между АРМ и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев оговоренных с

администратором информационной безопасности). Администратор информационной безопасности оставляет за собой право блокировать или ограничивать использование носителей информации.

В случае выявления фактов несанкционированного и/или нецелевого использовании носителей информации инициализируется служебная проверка, проводимая комиссией, состав которой определяется ответственным за организацию обработки персональных данных.

По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Школы и действующему законодательству.

Информация, хранящаяся на съемных носителях, подлежит обязательной проверке на отсутствие вредоносного ПО.

В случае утраты или уничтожения съемных носителей конфиденциальной информации (персональных данных) либо разглашения содержащихся в них сведений немедленно ставится в известность руководитель структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей конфиденциальной информации (персональных данных).

Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение таких съемных носителей с конфиденциальной информацией осуществляется администратором информационной безопасности после сдачи пользователями, с отметкой в журнале.

В случае увольнения или перевода работника в другое структурное подразделение предоставленные носители конфиденциальной информации сдаются администратору информационной безопасности.

Приложение № 1
к приказу МБОУ «Излучинская ОСШ УИОП № 2»
от «10» _января_ 2017г. № 010

Инструкция по использованию программных и аппаратных средств защиты информации

1. Порядок эксплуатации средств защиты информации

1.1. Антивирусные программные продукты Kaspersky Endpoint Security.

При эксплуатации данных программных продуктов выполнять требования и руководствоваться следующими документами:

- Руководства по установке;
- Руководства пользователя.

Данные документы разрабатываются производителем программного продукта и предоставляются в электронном виде на установочном оптическом диске.

1.2. Средство защиты информации от несанкционированного доступа «Dallas Lock 8.0-К».

При эксплуатации средства защиты информации выполнять требования и руководствоваться следующими документами:

- Описание применения;
- Руководство оператора;
- Руководство по эксплуатации.

Данные документы разрабатываются производителем программного продукта и предоставляются в электронном виде на установочном оптическом диске.

1.3. Персональный межсетевой экран и клиент защищенной почтовой системы «ViPNet Client 3.X».

При эксплуатации данной системы выполнять требования и руководствоваться следующими документами:

- Инструкция по установке и настройке защищённого рабочего места ViPNet Client;
- Настройка параметров безопасности. Руководство пользователя;
- ViPNet Client 3.2. Деловая почта. Руководство пользователя;
- ViPNet Client 3.2. Монитор. Руководство пользователя;
- Контроль приложений. Руководство пользователя;
- Идентификация пользователя ViPNet. Приложение к документации ViPNet;
- Классификация полномочий. Приложение к документации ViPNet;
- Информация о внешних устройствах хранения данных. Приложение к документации ViPNet;
- Основные термины и определения. Приложение к документации ViPNet;
- Инструкция по установке, запуску и первоначальной настройке программного обеспечения ViPNet Client. Приложение к документации ViPNet.

Данные документы разрабатываются производителем программного продукта и предоставляются в электронном виде на установочном оптическом диске.

1.4 Программно-аппаратный комплекс Соболь 3.0.

При эксплуатации программно-аппаратного комплекса выполнять требования и руководствоваться следующими документами:

- Соболь версия 3.0. Руководство администратора;
- Соболь версия 3.0. Быстрая установка;

– ПАК "Соболь". Версия 3.0. Комментарии к версиям 2.0.88 ПО Windows, 3.0.41/40 ПО Linux и 1.0.180 BIOS;

– Соболь версия 3.0. Руководство пользователя.

2. Порядок установки, настройки, модификации и технического обслуживания средств защиты информации

В соответствии с Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» и Постановлением Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» выполнение работ по установке, монтажу, испытаниям, ремонту средств защиты информации отнесены к лицензируемому виду деятельности по технической защите конфиденциальной информации. С учетом этого для выполнения данных работ может привлекаться только организация, имеющая соответствующую лицензию.

Эксплуатация средств защиты информации осуществляется лицами, допущенными к ним в соответствии с разрешительной системой доступа пользователей к сведениям конфиденциального характера в информационной системе.

Контроль по выполнению данными лицами требований документов по эксплуатации средств защиты информации возлагается на администратора информационной безопасности.

Приложение № 1
к приказу МБОУ «Излучинская ОСШ УИОП № 2»
от «10» _января_ 2017г. № 010

Инструкция администратору информационной безопасности муниципальной информационной системы персональных данных МИС «ОО»

Обозначения и сокращения

Школа – МБОУ Излучинская ОСШУИОП №2;
АС – автоматизированная система;
АРМ – автоматизированное рабочее место;
ВТСС – вспомогательные технические средства и системы;
ИБ – информационная безопасность;
МИС ПДн – муниципальная информационная система персональных данных МИС «ОО»;
ОТСС – основные технические средства и системы;
ПДн – персональные данные;
ПЭВМ – персональная электронно-вычислительная машина;
СВТ – средства вычислительной техники;
СЗИ – средства защиты информации;
СЗПДн – система (подсистема) защиты персональных данных;
УБПДн – угрозы безопасности персональным данным;
ПО – программное обеспечение;
ОРД – организационно-распорядительная документация;
ОС – операционная система;
Машинные носители информации (МНИ) –накопители на жестких магнитных дисках (HDD);
Съемные носители информации (СНИ) – USB-флэш-накопители информации.

1.Общие положения

1.1. Настоящий документ определяет основные обязанности, права и ответственность администратора информационной безопасности МИС ПДн.

1.2. Администратор информационной безопасности осуществляет контроль выполнения требований организационных и технических мероприятий по обеспечению безопасности информации в МИС ПДн.

1.3. Методическое руководство и контроль работы администратора информационной безопасности осуществляется ответственным за организацию обработки персональных данных в Школе.

2.Особенности организации работы в МИС ПДн

Администратор информационной безопасности должен знать, что:

МИС ПДн относится к многопользовательским информационным системам с разными правами доступа пользователей к ресурсам информационной системы. Группы пользователей, работающих в МИС ПДн: администратор информационной безопасности, пользователи. Данные группы пользователей имеют права доступа к ресурсам МИС ПДн в соответствии с разрешительной системой доступа пользователей к ресурсам МИС ПДн.

3.Обязанности администратора информационной безопасности

3.1. Администратор информационной безопасности должен:

3.1.1. Знать нормативно-методические документы в области безопасности информации и организационно-распорядительные документы в части его касающейся;

3.1.2. Знать состав ОТСС МИС ПДн и контролировать их соответствие техническому паспорту на МИС ПДн. Вести учет изменений аппаратно-программной конфигурации (архив заявок, на основании которых были произведены данные изменения);

3.1.3.Контролировать процесс управления (заведения, активации, блокирования, уничтожения) учетными записями пользователей МИС ПДн:

- Проверять соответствие прав доступа пользователей к объектам доступа МИС ПДн в соответствии с задачами, решаемыми пользователями в МИС ПДн и взаимодействующими с ней информационными системами и Разрешительной системой доступа к МИС ПДн;
- Контролировать назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование МИС ПДн;
- Проверять отсутствие в МИС ПДн учетных записей уволенных (отстраненных) сотрудников;
- Оповещать администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;
- Проверять своевременность удаления временных учетных записей, предоставленных для однократного (ограниченного по времени) выполнения задач в МИС ПДн;

3.1.4 Контролировать неизменность настроек средств защиты информации:

- Настройки средств защиты информации должны препятствовать передаче защищаемой информации через сеть Интернет (или) другие информационно-телекоммуникационные сети международного информационного обмена по незащищенным линиям связи;
- Средства защиты информации должны ограничивать доступ к МИС ПДн на 10 минут при 5 неудачных попытках входа в МИС ПДн;
- Должен быть запрещен доступ к МИС ПДн до прохождения процедур аутентификации и идентификации;
- Должен обеспечиваться запрет удаленного доступа к МИС ПДн.
- Средства доверенной загрузки должны обеспечивать:
  - блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы;
  - контроль доступа пользователей к процессу загрузки операционной системы.

3.1.5.Контролировать запрет использования в МИС ПДн технологий беспроводного доступа и мобильных технических средств.

3.1.6. Контролировать отсутствие доступа к МИС ПДн со стороны пользователей информационных систем сторонних организаций.

3.1.7.Контролировать установку на АРМ МИС ПДн ПО с целью отсутствия в составе АРМ МИС ПДн стороннего ПО, не связанного с задачами, решаемыми пользователями в МИС ПДн.

3.1.8. Вести учет машинных носителей персональных данных.

3.1.9. Обеспечивать уничтожение (стирание) защищаемой информации с машинных носителей АРМ МИС ПДн, при их передаче в сторонние организации для ремонта или утилизации, либо контролировать процесс уничтожения (стирания). Уничтожение защищаемой информации должно исключать возможность восстановления защищаемой информации.

3.1.10. Контролировать регистрацию в МИС ПДн следующих событий безопасности:

- входа (выхода), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы:

- дата (время) входа/выхода в систему (из системы) или загрузки/останова операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

- подключения машинных носителей информации и вывода информации на носители информации:

- дата и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

- запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации:

- дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

- попыток доступа программных средств к защищаемым объектам доступа:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификация защищаемого файла (логическое имя, тип).

- попыток удаленного доступа:

- дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе.

3.1.11. Контролировать права на доступ к информации о событиях безопасности: доступ должен предоставляться исключительно администраторам МИС ПДн, обеспечивающим функционирование МИС ПДн, а также администратору информационной безопасности.

3.1.12. Обеспечивать постоянный контроль за выполнением пользователями МИС ПДн установленного комплекса мероприятий по обеспечению безопасности информации и соблюдения действующего законодательства в области информационной безопасности, а также инструкции пользователя и других организационно-распорядительных документов в части обеспечения безопасности информации;

3.1.13. Требовать от пользователей МИС ПДн и выполнять самому требования «Инструкции по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств муниципальной информационной системы МИС «ОО» и вести «Журнал учета нештатных ситуаций, выполнения профилактических и ремонтных работ на объекте, установки и модификации аппаратных и программных средств МИС ПДн»;

3.1.14. Контролировать порядок учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов;

3.1.15. Контролировать использование пользователями только учтенных съемных носителей. После того как цель переноса информации на носители достигнута (переданы третьим лицам и т.п.) информация незамедлительно удаляется с носителей;

3.1.16. Контролировать настройки ОС и СЗИ АРМ пользователей;

3.1.17. Проводить инструктаж пользователей по правилам работы с используемыми средствами и системами зашиты информации;

3.1.18. Устанавливать права доступа пользователей к информационным и техническим ресурсам МИС ПДн в соответствии с принятой и утвержденной разрешительной системой доступа;

3.1.19. Следить за изменением программной среды МИС ПДн и полномочиями пользователей;

3.1.20. Хранить дистрибутивы СЗИ, производить при необходимости восстановление программной среды СЗИ или настройки защитных механизмов операционной системы и привилегий пользователей по доступу к ресурсам МИС ПДн. При необходимости для данных мероприятий привлекать других технических специалистов Школы;

3.1.21. Фиксировать и пресекать невыполнение пользователями МИС ПДн требований или норм нормативно-методических документов в области безопасности информации и организационно-распорядительных документов в информационной сфере, а также создания пользователями возможностей утечки информации;

3.1.22. При получении информации о фактах нарушения политики и правил безопасности, а также попыток использования внешними нарушителями атак, в том числе с использованием методов социальной инженерии – немедленно докладывать ответственному за организацию обработки персональных данных, инициировать проведение служебной проверки (при нарушениях со стороны ответственного за организацию обработки персональных данных докладывать необходимо непосредственно вышестоящему руководству), регистрировать в журнале учёта инцидентов ИБ.

3.1.23. Не реже 1 раза в месяц просматривать журналы учёта и регистрации событий СЗИ (в соответствии с инструкцией по использованию программных и аппаратных средств защиты информации, операционной системы на предмет выявления подключения неучтённых носителей, попыток НСД и т.п.

3.1.24. Требовать от пользователей МИС ПДн и выполнять самому порядок пропускного и внутриобъектового режима в здании.

3.1.25. Контролировать отсутствие в составе ПО АРМ, входящих в МИС ПДн, средств разработки и отладки программ.

3.1.26. Реагировать на поступление в МИС ПДн спама (в случае присутствия данной информации в журналах событий межсетевого экрана) путем блокирования атакующего хоста.

3.1.27. Выполнять мероприятия по периодическому резервному копированию защищаемой информации в соответствии с «Инструкцией по резервному копированию и восстановлению данных в муниципальной информационной системе персональных данных МИС «ОО»;

3.1.28. Знать эксплуатационную документацию на применяемые СЗИ. Устанавливать и эксплуатировать СЗИ в соответствии с документацией;

3.1.29. Хранить документацию и дистрибутивы СЗИ в соответствии с техническими условиями. Компакт-диск с программным обеспечением системы должен упаковываться согласно требованиям, предусмотренным для оптических носителей;

3.1.30. Поддерживать настройки СЗИ, соответствующие требованиям нормативных документов по безопасности информации и протоколу аттестационных испытаний, при этом система должна реализовывать в совокупности на каждой АРМ МИС ПДн функции необходимые для выполнения требований по защите от НСД для МИС ПДн;

3.1.31. Контролировать срок действия сертификатов соответствия на СЗИ и обеспечить их продление в соответствии с порядком продления, приведённым ниже.

3.2. Администратор информационной безопасности оказывает методическую помощь и контролирует выполнение руководителем подразделения, эксплуатирующего МИС ПДн следующих действий:

- При смене пользователя руководитель подразделения, эксплуатирующего МИС ПДн, инициирует внесение изменений в перечень лиц, допущенных к работе в МИС ПДн и в разрешительную систему доступа;
- При исключении пользователя МИС ПДн из «Перечня лиц, имеющих доступ к МИС ПДн» руководителем подразделения, эксплуатирующего МИС ПДн, принимаются меры по исключению возможности нарушения данным пользователем характеристик безопасности информации МИС ПДн. Администратору информационной безопасности необходимо до момента доведения до сотрудника информации о прекращении его работы в МИС ПДн, лишить сотрудника возможности доступа к защищаемой информации.

3.3. Администратору информационной безопасности запрещается:

3.3.1. Фиксировать учетные данные пользователя (пароли, идентификаторы, ключи и др.) на твердых носителях, а также сообщать их кому бы то ни было, кроме самого пользователя;

3.3.2. Раскрывать информацию об организации СЗПДн МИС ПДн и любую информацию, которая может создать предпосылки для возникновения канала утечки информации или создания угрозы безопасности информации.

4. Права администратора информационной безопасности

4.1. Требовать от пользователей МИС ПДн соблюдения установленных технологий обработки информации, выполнения нормативно-методических документов в области безопасности информации и организационно-распорядительных документов на МИС ПДн;

4.2. Давать своему непосредственному начальнику свои предложения по совершенствованию мер защиты в МИС ПДн.

5. Ответственность

5.1. Администратор информационной безопасности несет ответственность по действующему законодательству за разглашение сведений ограниченного распространения, ставших известными ему по роду деятельности.

5.2. Ответственность за защиту МИС ПДн от несанкционированного доступа к информации и за неукоснительное соблюдение положений настоящего руководства возлагается на администратора информационной безопасности.

6. Порядок использования съемных и машинных носителей информации

Под использованием съемных носителей информации в МИС ПДн понимается их подключение к АРМ с целью обработки, приема/передачи информации между АРМ и носителями информации.

В МИС ПДн допускается использование только учтенных съемных носителей информации, которые являются собственностью Школы и подвергаются регулярной ревизии и контролю.

Съемные носители информации предоставляются пользователю МИС ПДн по инициативе руководителя структурного подразделения, в котором он числится, в случае:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у сотрудника Школы производственной необходимости.

Порядок учета, хранения и обращения со съемными и машинными носителями, твердыми копиями и их утилизации.

Все находящиеся на хранении и в обращении в МИС ПДн съемные и машинные носители подлежат учёту.

Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера. Учет машинных носителей ведется в журнале учета машинных носителей конфиденциальной информации (Приложение № 1).

Каждый съемный носитель должен иметь этикетку, на которой указывается его уникальный учетный номер.

Для получения электронного внешнего носителя, для использования в МИС ПДн, пользователь обращается к непосредственному руководителю, руководитель пишет служебную записку на имя ответственного за организацию обработки персональных данных о выдаче пользователю съемного электронного носителя, далее ответственный за организацию обработки персональных данных принимает решение и передает служебную записку администратору информационной безопасности.

Учет и выдачу съемных носителей для использования в МИС ПДн осуществляет администратор информационной безопасности, на которого возложена эта функция. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей конфиденциальной информации (Приложение № 2).

При использовании сотрудниками съемных носителей информации необходимо:

- соблюдать требования настоящей Инструкции;
- использовать носители информации исключительно для выполнения своих служебных обязанностей;
- ставить в известность администратора информационной безопасности о любых фактах нарушения требований настоящей Инструкции;
- бережно относиться к носителям информации;
- извещать администратора информационной безопасности о фактах утраты (кражи) носителей информации.

При использовании носителей конфиденциальной информации запрещено:

- использовать носители конфиденциальной информации в личных целях;
- передавать носители конфиденциальной информации другим лицам (за исключением администратора информационной безопасности);
- хранить съемные носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- выносить съемные носители с конфиденциальной информацией (персональными данными) за пределы контролируемой зоны для работы с ними на дому и т. д.

Любое взаимодействие (обработка, прием/передача информации) инициированное пользователем МИС ПДн между АРМ и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев оговоренных с администратором информационной безопасности). Администратор информационной безопасности оставляет за собой право блокировать или ограничивать использование носителей информации.

В случае выявления фактов несанкционированного и/или нецелевого использовании носителей информации инициализируется служебная проверка, проводимая комиссией, состав которой определяется директором Школы.

По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Школы и действующему законодательству.

Информация, хранящаяся на съемных носителях, подлежит обязательной проверке на отсутствие вредоносного ПО.

В случае утраты или уничтожения съемных носителей конфиденциальной информации (персональных данных) либо разглашении содержащихся в них сведений немедленно ставится в известность руководитель соответствующего структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журнал учета съемных носителей конфиденциальной информации (персональных данных).

Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение таких съемных носителей с конфиденциальной информацией осуществляется

администратором информационной безопасности после сдачи пользователями, с отметкой в журнале.

В случае увольнения или перевода работника в другое структурное подразделение предоставленные носители конфиденциальной информации сдаются администратору информационной безопасности.

7. Порядок продления сроков действия сертификатов соответствия на средства защиты информации, программные средства контроля защищенности информации от несанкционированного доступа

1. Организация, эксплуатирующая средства защиты информации или программные средства контроля защищенности информации от несанкционированного доступа, заблаговременно, до окончания срока действия сертификата соответствия, который указан в копии сертификата, а также в Государственном реестре сертифицированных средств защиты информации в Системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00, связывается с производителем, с целью получения информации о продлении сертификата соответствия.

2. В случае получения информации об отсутствии намерений в продлении сертификата соответствия производителем, организация, эксплуатирующая средства защиты информации или программные средства контроля защищенности информации от несанкционированного доступа, направляет в Федеральный орган по сертификации Заявку на продление срока действия сертификата соответствия.

К заявке прикладываются протоколы оценки эффективности применения СЗИ, (для технических средств защиты информации от утечки по физическим каналам) или протоколы оценки защищенности информации, обрабатываемой на объекте информатизации, от несанкционированного доступа (для СЗИ от НСД), оформленные не ранее двенадцати месяцев до дня отправки заявки о продлении срока действия сертификата соответствия.

Указанные протоколы оформляются при проведении аттестационных испытаний или ежегодного периодического контроля состояния защиты информации.

Для объекта информатизации, предназначенного для обработки информации, содержащей сведения, составляющие государственную тайну, протокол оформляется организацией, аккредитованной в качестве органа по аттестации объектов информатизации в Системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 или организацией, имеющей лицензию ФСТЭК России на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации), позволяющей осуществлять деятельность по контролю защищенности информации ограниченного доступа.

Для объекта информатизации, предназначенного для обработки информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, протокол оформляется организацией, имеющей лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации.

Протокол должен содержать оценку применения средства защиты информации, о котором идет речь в письме.

В протоколе обязательно должна содержаться идентификационная информация средства защиты информации, а именно его заводской номер, номер голографического знака соответствия, номер и срок действия сертификата соответствия.

Номер знака соответствия для маркирования сертифицированной продукции можно получить либо с самого знака, либо из формуляра (паспорта) на средство защиты информации, либо от производителя.

Для продления срока действия сертификата соответствия на программное средство контроля защищенности от НСД, к письму прикладывается протокол контрольного суммирования, оформленный не ранее месяца до дня отправки письма о продлении.

Указанный протокол оформляется организацией, эксплуатирующей это СКЗИ и:

- аккредитованной в качестве испытательной лаборатории или органа по аттестации объектов информатизации в Системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00;
- имеющей лицензию ФСТЭК России на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации), позволяющей осуществлять деятельность по контролю защищенности информации ограниченного доступа или деятельность по проведению сертификационных испытаний;
- имеющей лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации.

В протоколе обязательно должна содержаться идентификационная информация программного средства контроля защищенности информации от НСД, а именно его заводской номер, номер голографического знака соответствия, номер и срок действия сертификата соответствия.

В протоколе должна содержаться идентификационная информация о средстве контроля защищенности, с помощью которого проводилось контрольное суммирование, информация о дате проведения контрольного суммирования.

В протоколе должен содержаться вывод о соответствии полученных контрольных сумм, суммам, приведенным в формуляре (паспорте).

3. К заявке прикладываются заверенные копии платежных поручений об уплате:

- государственной пошлины за выдачу сертификата соответствия.
- платежа за специальный защитный знак, наносимый на бланк сертификата, аттестата аккредитации.

Если сертификат соответствия продлевается на партию СЗИ, платить необходимо за один сертификат (разными платежными поручениями).

Если в заявке сказано о продлении разных сертификатов соответствия, то к письму прикладываются копии платежных поручений за каждый продлеваемый сертификат.

С банковскими реквизитами ФСТЭК России, а также наименованиями платежей можно ознакомиться на официальном сайте ФСТЭК России www.fstec.ru.

4. В случае принятия положительного решения по экспертизе представленных материалов Федеральным органом по сертификации выписывается сертификат (сертификаты) соответствия, который в соответствии с указанным в заявке почтовым адресом отправляется заявителю.

8. Установка и обновление программного обеспечения

Установка или обновление подсистем МИС ПДн должны проводиться уполномоченными сотрудниками (администраторы сети (серверов) и администраторы баз данных) обязательно по согласованию с администратором информационной безопасности. После установки модифицированных модулей на сервер (рабочую станцию) администратор информационной безопасности проводит антивирусный контроль.

Установка и обновление общего программного обеспечения (системного, тестового и т.п.) на рабочие станции и сервера производится с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных установленным порядком.

Факты установки или обновления фиксируются в «Журнале учета нештатных ситуаций, выполнения профилактических и ремонтных работ на объекте, установки и модификации аппаратных и программных средств МИС ПДн».

Приложение № 1
к инструкции администратора
информационной безопасности

Журнал учета машинных носителей персональных данных

№ п/п	Серийный/ инвентарный № АРМ	Дата постановки на учет	Подпись администратора информационной безопасности, производившего учет	Сведения об уничтожении носителя	Примечание

Приложение № 2
к инструкции администратора
информационной безопасности

Журнал учета съемных носителей персональных данных

№ п/п	Учетный номер носителя	Дата выдачи	Подпись сотрудника, получившего носитель	Подпись администратора информационной безопасности	Сведения об уничтожении носителя	Примечание