Утверждаю:

директор ГКОУ «С(К)ОШ-И № 18

г-к Кисловодска

С.А Кислюк _____

Инструктаж «О особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Государственного казенного общеобразовательного учреждения «Специальная (коррекционная) общеобразовательная школа-интернат № 18» г-к Кисловодска

г-к Кисловодск

1. Общие положения

1.1 Настоящая Инструкция разработана в соответствии с «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным Постановлением Правительства РФ от 15.09.2008 № 687, и определяет правила работы с персональными данными и их материальными носителями без использования средств автоматизации.

1.2 Обработка персональных данных, полученных от работника, содержащихся в информационной системе персональных данных либо извлеченных из такой системы считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов, персональных данных, осуществляются при непосредственном участии человека.

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

2. Порядок обработки персональных данных

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

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

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

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

2.5 Хранение документов, содержащих персональные данные, осуществляется в металлических шкафах или сейфах. 2.6 Уничтожение документов, содержащих персональные данные, осуществляется способом, не позволяющим в дальнейшем ознакомиться с персональными данными.

3. Обязанности сотрудника, допущенного к обработке персональных данных: При работе с документами, содержащими персональные данные, сотрудник обязан исключить возможность ознакомления, просмотра этих документов лицами, не допущенными к работе с ними (в том числе другими работниками своего структурного подразделения). При выносе документов, содержащих персональные данные, за пределы территории Государственного казенного общеобразовательного учреждения «Специальная (коррекционная) общеобразовательная школа-интернат № 18» г-к Кисловодска (далее – Школы-интерната) по служебной необходимости сотрудник должен принять все возможные меры, исключающие утрату (утерю, хищение) таких документов. При утрате (утере, хищении) документов, содержащих персональные данные, работник обязан немедленно доложить о таком факте своему непосредственному начальнику (руководителю). Непосредственный начальник (руководитель) должен сообщить заместителю директора, курирующему вопросы защиты информации о факте утраты (утере, хищении) документов, содержащих персональные данные. По каждому такому факту назначается служебное расследование.

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

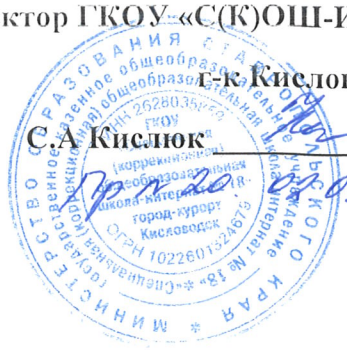
5. Ответственность: Ответственность за неисполнение или ненадлежащее выполнение требований настоящей Инструкции возлагается на работников и руководителей подразделений. Контроль за выполнением положений настоящей Инструкции возлагается на ответственного по защите персональных данных. За нарушение правил обработки персональных данных, их неправомерное разглашение или распространение, виновные лица несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством. В случае если в результате действий работника был причинен подлежащий возмещению работодателем ущерб третьим лицам, работник несет перед работодателем материальную ответственность в соответствии с главой 39 Трудового кодекса РФ. В случае разглашения персональных данных, ставших известными работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника, трудовой договор с работником может быть расторгнут работодателем (подпункт «в» пункта 6 статьи 81 Трудового кодекса РФ).

Утверждаю:

директор ГКОУ «С(К)ОШ-И № 18

г-к Кисловодска

С.А Кислюк _____



Инструктаж по введению парольной защиты информационной системы персональных данных

Государственного казенного общеобразовательного учреждения «Специальная (коррекционная) общеобразовательная школа-интернат № 18» г-к Кисловодска

г-к Кисловодск

1. Общие положения

Настоящая инструкция устанавливает основные правила введения парольной защиты информационной системы персональных данных Государственного казенного общеобразовательного учреждения «Специальная (коррекционная) общеобразовательная школа-интернат № 18» г-к Кисловодска (далее – Школа-интернат). Инструкция регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей в информационной системы персональных данных, а также контроль за действиями пользователей системы при работе с паролями. Настоящая инструкция оперирует следующими основными понятиями: Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов. ИСПДн – информационная система персональных данных. Компрометация- факт доступа постороннего лица к защищаемой информации, а также подозрение на него. Объект доступа - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа. Пароль – уникальный признак субъекта доступа, который является его (субъекта) секретом. Правила доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа. Субъект доступа - лицо или процесс, действия которого регламентируются правилами разграничения доступа. Несанкционированный доступ - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или АС.

2 Правила генерации паролей

2.1 Персональные пароли должны генерироваться специальными программными средствами сотрудниками сетевого администрирования.

2.2 Длина пароля должна быть не менее 6 символов.

2.3 В составе пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы.

2.4 Пароль не должен включать в себя: легко вычисляемые сочетания символов; клавиатурные последовательности символов и знаков; общепринятые сокращения; аббревиатуры; номера телефонов, автомобилей; прочие сочетания букв и знаков, ассоциируемые с пользователем; при смене пароля новое сочетание символов должно отличаться от предыдущего не менее чем на 2 символа.

2.5 Допускается использование единого пароля для доступа субъекта доступа к различным информационным ресурсам одной ИСПДн объекта образования.

3 Порядок смены паролей

3.1 Полная внеплановая смена паролей всех пользователей должна производиться случае прекращения полномочий администраторов средств защиты или других сотрудников, которым по роду службы были предоставлены полномочия по управлению парольной защитой.

3.2 Полная внеплановая смена паролей должна производиться в случае компрометации личного пароля одного из администраторов ИСПДн.

3.3 В случае компрометации личного пароля пользователя надлежит немедленно ограничить доступ к информации с данной учетной записи, до момента вступления в силу новой учетной записи пользователя или пароля.

4 Обязанности пользователей при работе с парольной защитой

4.1 При работе с парольной защитой пользователям запрещается: разглашать кому-либо персональный пароль и прочие идентифицирующие сведения; предоставлять доступ от своей учетной записи к информации, хранящейся в ИСПДн посторонним лицам;

записывать пароли на бумаге, файле, электронных и прочих носителях информации, в том числе и на предметах.

4.2 Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе.

4.3 При вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

5 Случаи компрометации паролей

5.1 Под компрометацией следует понимать: физическая утеря носителя с информацией; передача идентификационной информации по открытым каналам связи; проникновение постороннего лица в помещение физического хранения носителя парольной информации или алгоритма или подозрение на него (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.); перехват пароля при распределении идентификаторов; сознательная передача информации постороннему лицу.

5.2 Действия при компрометации пароля: скомпрометированный пароль сразу же выводится из действия, взамен его вводятся запасной или новый пароль; о компрометации немедленно оповещаются все участники обмена информацией. Пароль вносится в специальные списки, содержащие скомпрометированные пароли и учетные записи.

6 Ответственность пользователей при работе с парольной защитой

6.1 Повседневный контроль за действиями сотрудников Школы-интерната при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на ответственного за систему защиты информации в ИСПДн.

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

6.3 Ответственность за организацию парольной защиты возлагается на ответственного за систему защиты информации в ИСПДн.

6.4 Ответственность в случае несвоевременного уведомлении ответственного за систему защиты информации в ИСПДн о случаях утери, кражи, взлома или компрометации паролей возлагается на владельца взломанной учетной записи.

Утверждаю:

директор ГКОУ «С(К)ОШ-И № 18

г-к Кисловодска

С.А Кислюк

02.03.21г.

Инструктаж по антивирусной защиты информационных систем персональных данных

Государственного казенного общеобразовательного учреждения «Специальная (коррекционная) общеобразовательная школа-интернат № 18» г-к Кисловодска

г-к Кисловодск

Общие положения

1.1 Настоящая инструкция определяет правила и основные требования к организации защиты информационных систем персональных данных (далее – ИСПДн) от разрушающего воздействия компьютерных вирусов в Государственного казенного общеобразовательного учреждения «Специальная (коррекционная) общеобразовательная школа-интернат № 18» г-к Кисловодска
(далее – Школы-интерната) и устанавливает ответственность за их выполнение.
1.2 Компьютерный вирус – это вид вредоносного программного обеспечения (далее – ПО), способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи. Кроме того, часто его сопутствующей функцией является нарушение работы программно-аппаратных комплексов (удаление файлов, приведение в негодность структур размещения данных, блокирование работы пользователей и т. п.).
1.3 Действие настоящей инструкции распространяется в полном объеме на Школу-интернат и обязательна для выполнения всеми сотрудниками.
2. Инструкция по применению средств антивирусной защиты
2.1 Защита программного обеспечения ИСПДн от вредоносного ПО осуществляется путем применения специализированных средств антивирусной защиты.
2.2 К использованию допускаются только лицензионные антивирусные средства, обладающие сертификатами регулирующих органов РФ.
2.3 Установка и настройка средств антивирусного защиты на автоматизированных рабочих местах (далее – АРМ) и серверах осуществляется сотрудниками школьной информационной сети.
2.4 Частота обновления баз данных средств антивирусной защиты, автоматическая проверка и лечения всех файлов должна проходить не реже 1 раза в неделю.
2.5 Все впервые вводимое в эксплуатацию программное обеспечение должно проходить обязательный антивирусный контроль.
2.6 Средства антивирусной защиты устанавливаются на всех АРМ и серверах Школы-интерната.
2.7 Ежедневно в установленное время в автоматическом режиме проводится антивирусный контроль всех дисков и файлов рабочих станций и серверов.
2.8 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивы), получаемая и передаваемая по телекоммуникационным каналам (включая электронную почту), а также информация на съемных носителях.
2.9 Разархивирование и контроль входящей информации, поступающей по каналам электронной почты, осуществляется до передачи поступившей информации исполнителю. До проведения антивирусного контроля файлы запрещается копировать на сетевые диски и в архивы электронной почты. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой.
2.10 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь, обнаруживший проблему, должен провести внеочередной антивирусный контроль АРМ либо обратиться к сотрудникам, осуществляющих сетевое администрирование ИСПДн.
2.11 В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:
приостановить работу; немедленно поставить в известность о факте обнаружения вируса сотрудников сетевого администрирования ИСПДн; провести лечение зараженных файлов; в случае невозможности лечения обратиться к сотрудникам, осуществляющие сетевое

администрирование ИСПДн; не начинать работу до устранения причины заражения вирусом и выполнения антивирусных мероприятий;
2.12 По факту обнаружения зараженных вирусом файлов сотрудник сетевого администрирования ИСПДн должен установить причины заражения вирусом и принять соответствующие меры по предотвращению подобных ситуаций.
2.13 Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.
2.14 Пользователи должны быть ознакомлены с данной инструкцией под роспись.
2.15 Проводить периодическое тестирование функций средств антивирусной защиты.
2.16 Проводить тестирование функций средств антивирусной защиты при изменениях (внедрении новых средств, их обновлении, изменениях в системе).
3. Пользователю запрещается:
вмешиваться в работу системы антивирусной защиты; отключать, выгружать или деинсталлировать средства антивирусной защиты на АРМ; установка ПО, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации;
4. Ответственность
4.1 Ответственность за организацию антивирусного контроля в Школе-интернате возлагается на сотрудников сетевого администрирования.
4.2 За невыполнение требований настоящей инструкции несут ответственность пользователи ИСПДн.

Утверждаю:

директор ГКОУ «С(К)ОШ-И № 18

г-к Кисловодска

С.А. Кислюк _____

20.03.21г.

Инструктаж по антивирусной защиты информационных систем персональных данных

Государственного казенного общеобразовательного учреждения «Специальная (коррекционная) общеобразовательная школа-интернат № 18» г-к Кисловодска

г-к Кисловодск

1. Общие положения
1.1 Настоящая Инструкция устанавливает обязанности пользователя информационных систем персональных данных (далее - ИСПДн) в Государственного казенного общеобразовательного учреждения «Специальная (коррекционная) общеобразовательная школа-интернат № 18» г-к Кисловодска (далее – Школы-интерната) по обеспечению безопасности, обрабатываемых в них персональных данных, запреты на действия пользователя в ИСПДн, а также его права и ответственность.
1.2 Наиболее вероятными каналами утечки информации для ИСПДн являются: несанкционированный доступ к информации, обрабатываемой в ИСПДн; хищение технических средств, с хранящейся в них информацией, или отдельных носителей информации; просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств; воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, через специально внедренные электронные и программные средства.
1.3 Доступ пользователя к ИСПДн осуществляется в соответствии с перечнем сотрудников, допущенных к обработке персональных.
1.4 Привилегии доступа пользователя к автоматизированному рабочему месту (далее - АРМ) назначаются в соответствии с матрицей прав доступа для ИСПДн.
1.5 Контроль за выполнением настоящей Инструкции возлагается на ответственного по защите персональных данных.
2. Обязанности работников Школы-интерната, имеющих доступ к ИСПДн
2.1 Работники, получившие доступ к персональным данным, обязаны хранить в тайне данные сведения, ставшие им известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки информации немедленно информировать руководителя структурного подразделения Школы-интерната, ответственного по защите персональных данных.
2.2 Персональные данные не подлежат разглашению. Прекращение доступа к такой информации не освобождает работника от взятых им обязательств о неразглашении конфиденциальных сведений.
2.3 В случае оставления занимаемой должности работник обязан вернуть все документы и материалы, относящиеся к деятельности Школы-интерната. В том числе отчеты, инструкции, переписку, списки сотрудников, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к деятельности Школы-интерната, полученные в течение срока работы.
2.4 Работники при работе с ИСПДн обязаны: Использовать ИСПДн для выполнения служебных задач в соответствии с должностной инструкцией. Использовать для доступа к ИСПДн собственную уникальную учетную

запись (логин) и пароль. Хранить в тайне уникальную учетную запись (логин) и пароль, обеспечивать физическую сохранность ключевого носителя доступа к ИСПДн. Использовать для работы, только учтенные съемные накопители информации. АРМ используемое для работы с конфиденциальной информацией, должно быть размещено таким образом, чтобы исключалась возможность визуального
просмотра экрана монитора, не имеющими отношения к конкретно обрабатываемой информации сотрудниками. Блокировать экран дисплея АРМ парольной заставкой при оставлении рабочего места. Контролировать обновление антивирусных баз и в случае необходимости обновления сообщить данную информацию сотрудникам, осуществляющим сетевое администрирование Школы-интерната и ответственному по защите персональных данных. В случае обнаружения попыток несанкционированного доступа к ИСПДн немедленно информировать сотрудников, осуществляющих сетевое администрирование Школы-интерната и ответственного по защите персональных данных. При появлении сообщений от программного обеспечения антивирусной защиты о возможном вирусном заражении АРМ или возникновении неисправностей (сбоев) в работе сервисов и информационных ресурсов Школы-интерната немедленно информировать сотрудников, осуществляющих сетевое администрирование. В случае утери носителя с конфиденциальной информацией или при подозрении компрометации логина и пароля немедленно информировать сотрудников, осуществляющих сетевое администрирование Школы-интерната и ответственного по защите персональных данных.

3. Действия, запрещенные пользователю ИСПДн

3.1 Работникам Школы-интерната, имеющих доступ к ИСПДн запрещается: Предоставлять доступ к информации, содержащей персональные данные, лицам, не допущенным к их обработке. Записывать и хранить персональные данные на неучтенных носителях информации. Самостоятельно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн, или устанавливать дополнительно любые программные и аппаратные средства. Оставлять включенным без присмотра АРМ, не активизировав средства защиты от несанкционированного доступа (блокировка экрана дисплея парольной заставкой). Осуществлять действия по преодолению установленных ограничений на доступ к ИСПДн. Отключать или изменять конфигурацию средств защиты информации ИСПДн.

4. Права пользователя ИСПДн

4.1 Пользователь ИСПДн имеет право: Получать помощь по вопросам эксплуатации ИСПДн, от ответственного за СЗИ ИСПДн. Обращаться к сотрудникам, осуществляющим сетевое администрирование Учреждения, по вопросам дооснащения АРМ техническими и программными средствами, не входящими в штатную конфигурацию АРМ и ИСПДн, необходимыми для автоматизации деятельности в соответствии с возложенными на него

должностными обязанностями. Подавать сотрудникам, осуществляющим сетевое администрирование Учреждения, предложения по совершенствованию функционирования ИСПДн.

5. Ответственность пользователя ИСПДн

5.1 Пользователь ИСПДн несет ответственность за: Обеспечение безопасности персональных данных при их обработке в ИСПДн. Нарушение работоспособности или вывод из строя системы защиты ИСПДн. Преднамеренные действия, повлекшие модификацию или уничтожение персональных данных в ИСПДн, и несанкционированный доступ к персональным данным в ИСПДн. □ За соблюдение требований настоящей инструкции, а также других документов в области защиты информации. За нарушение настоящей Инструкции к пользователю могут применяться меры дисциплинарного воздействия. За нарушение правил обработки персональных данных, их неправомерное разглашение или распространение, виновные лица несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

Утверждаю:

директор ГКОУ «С(К)ОШ-И № 18

г-к Кисловодска

С.А Кислюк _____

02.03.21г.

Инструктаж по уничтожению и обезличиванию персональных данных на бумажных и электронных носителях

Государственного казенного общеобразовательного учреждения «Специальная (коррекционная) общеобразовательная школа-интернат № 18» г-к Кисловодска

г-к Кисловодск

1. Общие положения

1.1 Настоящая инструкция определяет порядок уничтожения и обезличивания информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований Государственного казенного общеобразовательного учреждения «Специальная (коррекционная) общеобразовательная школа-интернат № 18» г-к Кисловодска (далее – Школы-интерната).

1.2 Целью настоящей инструкции является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.3 Основные понятия, используемые в Инструкции: Персональные данные (далее – ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных); Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными; Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных; Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных; Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2. Условия и порядок уничтожения, содержащих персональные данные

2.1 Документы, содержащие персональные данные, обрабатываемые в структурных подразделениях Школы-интерната, обязаны храниться в течение сроков, установленных Федеральным законом №125-ФЗ от 22.10.2004г. и перечнем утвержденном приказом Минкультуры России от 25.08. 2010 г. № 558.

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

2.3 В случае отзыва согласия на обработку ПДн оператор обязан прекратить их обработку и в случае, если сохранение ПДн более не требуется для целей обработки, уничтожить ПДн в срок, не превышающий тридцати дней с даты поступления указанного отзыва и письменно известить субъекта ПДн об окончании обработки его ПДн (приложение 3).

2.4 В случае отзыва субъектом ПДн согласия на обработку ПДн оператор вправе продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6 части 2 статьи 10 и части 2 статьи 11 Федерального закона № от 27.07.2006 N 152-ФЗ

2.5 В случае выявления неправомерной обработки ПДн, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить такие персональные данные.

2.6 Отбор носителей ПДн к уничтожению осуществляется по решению руководителя соответствующего подразделения, к деятельности которого относится носитель и ответственного по защите ПДн.
2.7 По итогам создается комиссия и составляется Акт о выделении к уничтожению документов, опись уничтожаемых дел, проверяется их комплектность, акт подписывается председателем и членами комиссии (приложение 1).
2.8 Уничтожение материальных носителей ПДн производится с участием комиссии, в состав которой входят ответственные работники, допущенные к работе с ПДн и сотрудники ответственные за защиту ПДн.
2.9 Уничтожение материальных носителей ПДн производится путем измельчения, сожжения или механического уничтожения. На каждый способ уничтожения составляется отдельный акт.
2.10 Уничтожение съемных машинных носителей информации (Flash, CD и DVD – дисков и др.) производится путем деформирования до состояния, которое исключает их повторное использование с последующим сожжением.
2.11 Перед уничтожением необходимо произвести циклы полного удаления всей информации.
2.12 После уничтожения материальных носителей членами: комиссии подписывается акт об уничтожении носителей, содержащих персональные данные.
2.13 Об уничтожении файлов делаются соответствующие отметки в Журнале уничтожения носителей персональных данных (Приложение 2).
3. Условия и порядок обезличивания документов, содержащие персональные данные
3.1 Оператор может обезличивать персональные данные в статистических или иных исследовательских целях, по достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей.
3.2. Способы обезличивания при условии дальнейшей обработки персональных данных: замена части данных идентификаторами; обобщение, изменение или удаление части данных; деление данных на части, и обработка в разных информационных системах; перемешивание данных;
3.3. В случае достижения целей обработки персональных данных или в случае утраты необходимости в достижении этих целей способом обезличивания является уменьшение перечня обрабатываемых данных.
3.4. Решение о необходимости обезличивания персональных данных и способе обезличивания принимает ответственный по защите персональных данных.
3.5. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

Приложение 1.

Типовая форма акта

об уничтожении носителей, содержащих персональные данные

Акт N _____ об уничтожении носителей, содержащих персональные данные

Комиссия в составе:

Председатель- _____

Члены комиссии - _____

провела отбор бумажных, электронных, магнитных и оптических носителей персональных данных и другой конфиденциальной, информации (далее носители) и установила, что в соответствии с требованиями руководящих документов по защите информации указанные носители и информация, записанная на них в процессе эксплуатации, в соответствии с действующим законодательством Российской Федерации, подлежит гарантированному уничтожению и составила настоящий акт о том, что произведено уничтожение носителей персональных данных в составе:

N п/н	Дата	Тип носителя	Учетный номер носителя	Категории информации	Примечание

Всего носителей_____
(цифрами и прописью количество)

На указанных носителях персональные данные уничтожены путем

_____

(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители ПД уничтожены путем

_____

(разрезания/сжигания/размагничивания/физического уничтожении/механического уничтожения / иного способа)

Председатель комиссии: _____/_____/

Члены комиссии: _____/_____/

_____/_____/

Приложение 2.

Типовая форма журнала уничтожения носителей персональных данных

Журнал уничтожения носителей персональных данных

Журнал начат _____ Журнал завершен _____ Ответственный _____ (Ф.И.О.) На _____ листах

N п/ п	Наименование ИСПД, в которой уничтожаются ПД	Ф.И.О. субъекта, переданные которого подлежащие уничтожению	Обоснование уничтожения	Наименование файла, и его место расположение	Дата уничтожения	Ф.И.О. и подпись Исполнителя	Ф.И.О. и подпись ответственного за обработку ПД