КОМИТЕТ ПО ФИЗИЧЕСКОЙ КУЛЬТУРЕ, СПОРТУ И ОХРАНЕ ЗДОРОВЬЯ АДМИНИСТРАЦИИ Г. МУРМАНСКА
МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ
«СПОРТИВНАЯ ШКОЛА №6» (МАУ ДО СШ № 6)

УТВЕРЖДАЮ
Директор МАУ ДО СШ № 6
_____ Г. Н. Полякова
«___» _____ 2023 г.

Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных в МАУ ДО СШ № 6

1. Назначение и область действия

1.1. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и системы защиты информации информационных систем персональных данных в *МАУ ДО СШ № 6* определяет действия, связанные с функционированием информационных систем персональных данных, используемых в МАУ ДО СШ № 6 (далее соответственно – ТС, ПО, СЗИ, Порядок, ИСПДн, организация), а также меры поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.2. Целью настоящего Порядка является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

1.3. Задачей настоящего Порядка является:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

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

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

1.5. Внесение изменений в настоящее положение осуществляется по мере необходимости.

1.6. В соответствии с распорядительным актом организации назначаются:

- сотрудник, ответственный за реагирование на инциденты безопасности, приводящие к потере защищаемой информации ИСПДн в организации (администратор, ответственный за систему защиты информации);
- сотрудник, ответственный за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации (администратор информационной безопасности ИСПДн).

2. Порядок реагирования на инцидент

2.1. В настоящем Порядке под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей защищаемой информации.

2.2. Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИСПДн;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. Все действия в процессе реагирования на инцидент должны документироваться ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю».

2.4. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники организации (администратор информационной безопасности, администратор и оператор ИСПДн), предпринимают меры по восстановлению работоспособности, которые согласовываются с руководителем организации.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1.Технические меры обеспечения непрерывной работы и восстановления, к которым относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, в том числе:

- системы жизнеобеспечения (пожарные сигнализации и системы пожаротушения, системы вентиляции и кондиционирования, системы резервного питания);
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

3.1.1. Все критичные помещения организации (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.1.2 Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

3.1.3. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания.

3.1.4. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и пр.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

3.1.5. Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться следующие методы кластеризации:

- для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров;

– технология RAID.

3.1.6. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

3.1.7. Система резервного копирования и хранения данных должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

3.2.Организационные меры

3.2.1. Резервное копирование и хранение данных должно осуществляться на периодической основе, ответственными лицами в соответствии с распорядительным актом организации:

– для обрабатываемых персональных данных – не реже раза в неделю;
– для технологической информации – не реже раза в месяц;
– эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

3.2.2. Данные о проведении процедуры резервного копирования должны отражаться в специально созданном журнале учета.

3.2.3. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

3.2.4. Носители должны храниться в несгораемом шкафу в помещении, оборудованном системой пожаротушения.

3.2.5. Носители должны храниться не менее года (для возможности восстановления данных).

КОМИТЕТ ПО ФИЗИЧЕСКОЙ КУЛЬТУРЕ, СПОРТУ И ОХРАНЕ ЗДОРОВЬЯ АДМИНИСТРАЦИИ Г. МУРМАНСКА
МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ
«СПОРТИВНАЯ ШКОЛА №6» (МАУ ДО СШ № 6)

УТВЕРЖДАЮ
Директор МАУ ДО СШ № 6
_____Г. Н. Полякова
«___»_____ 2023 г.

Инструкция
по обработке персональных данных
МАУ ДО СШ № 6 без использования средств автоматизации

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, является дополнением к «Положению об обработке персональных данных в МАУ ДО СШ № 6» и определяет правила работы с персональными данными и их материальными носителями без использования средств автоматизации.

1.2.Обработка персональных данных, полученных от работника, 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.

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

1.5.С настоящей инструкцией должны быть ознакомлены под подпись работники, допускаемые к обработке персональных данных без использования средств автоматизации. Листы ознакомления хранятся у ответственного за систему защиты информации в МАУ ДО СШ № 6.

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 фиксации на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных - использовать отдельный материальный носитель для каждой из категорий.

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

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

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

3.2.При выносе документов, содержащих персональные данные, за пределы территории МАУ ДО СШ № 6 по служебной необходимости сотрудник должен

принять все возможные меры, исключающие утрату (утерю, хищение) таких документов.

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

4. Сотрудникам, допущенным к обработке персональных данных, запрещается:

4.1. Сообщать сведения, являющиеся персональными данными, лицам, не имеющим права доступа к этим сведениям.

4.2. Делать неучтенные копии документов, содержащих персональные данные.

4.3. Оставлять документы, содержащие персональные данные, на рабочих столах без присмотра.

4.4. Покидать помещение, не поместив документы с персональными данными в закрываемые сейфы, шкафы.

4.5. Выносить документы, содержащие персональные данные, из помещений СО без служебной необходимости.

5. Ответственность сотрудников

5.1. Ответственность за неисполнение или ненадлежащее выполнение требований настоящей Инструкции возлагается на работников и руководителей подразделений.

5.2. Контроль за выполнением положений настоящей Инструкции возлагается на ответственного за систему защиты информации (СЗИ) в организации.

5.3. 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.

5.4. 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.

5.5. 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).

Лист ознакомления

с Инструкцией по обработке персональных данных в

____,

(наименование организации)

осуществляемой без использования средств автоматизации

№ п/п	Фамилия, имя, отчество работника	Дата ознакомления с Инструкцией	Подпись работника