УТВЕРЖДАЮ:
Директор МКУДО «ЦРТДиЮ»
_____ / С.И.Бурмистр /
(подпись) (инициалы, фамилия)
«30» августа 2021 г.

Положение
по организации и проведению работ в
Муниципальном казенном учреждении дополнительного образования «Центр развития творчества детей и юношества»
по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных

1.

Общие положения

1.1.Настоящее Положение разработано в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федераций от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

1.2. Положение регламентирует вопросы обеспечения безопасности персональных данных (ПДн) при их обработке в информационной(ых) системе(ах) персональных данных (ИСПДн) в МКУДО «ЦРТДиЮ» и определяет порядок организации работ по созданию и эксплуатации системы защиты персональных данных (СЗПДн).

1.3.В МКУДО «ЦРТДиЮ» назначаются администратор безопасности и ответственный за обеспечение безопасности персональных данных в информационной системе.

2. Порядок работы пользователей ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн

2.1. Допуск пользователей для работы на персональной электронной вычислительной машине (далее - ПЭВМ) осуществляется в соответствии с «Перечнем должностей работников, доступ которым к персональным данным необходим для выполнения трудовых обязанностей в МКУДО «ЦРТДиЮ».

2.2. Пользователь несет ответственность за правильность включения и выключения ПЭВМ, входа в систему и все совершаемые действия при работе в ИСПДн.

2.3. Вход пользователя в систему может осуществляться по выдаваемому ему электронному идентификатору или по персональному паролю.

2.4. Запись информации, содержащей ПДн, может осуществляться пользователем на съемные машинные носители информации, соответствующим образом учтенные в журнале учета машинных носителей.

2.5. Каждый работник, участвующий в силу трудовых обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет ответственность за свои действия и ***обязан***:

- соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
- знать и выполнять правила работы со средствами защиты информации, установленными на ПЭВМ (если такие имеются);
- хранить в тайне свой(и) пароль (пароли);
- хранить в установленном порядке свое индивидуальное устройство идентификации (ключ) и другие реквизиты в недоступном для других работников месте;
- немедленно поставить в известность администратора безопасности об утере индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ПЭВМ, выхода из строя или неустойчивого функционирования узлов ПЭВМ или периферийных устройств (принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на ПЭВМ технических средств защиты;
- непредусмотренных отводов кабелей и подключенных новых устройств.

2.6. Пользователю ПЭВМ категорически ***запрещается***:

-использовать компоненты программного и аппаратного обеспечения ПЭВМ в нерабочих целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения ПЭВМ;

- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);

- оставлять включенной без присмотра ПЭВМ, не активизировав средства защиты от несанкционированного доступа (далее – НСД) - временную блокировку экрана и клавиатуры;

- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

- размещать технические средства ИСПДн таким образом, чтобы возникала возможность визуального считывания информации.

3. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения баз данных и средств защиты информации

3.1.Процесс резервного копирования обеспечивает сохранение на резервных носителях информации, с целью ее восстановления при потере или порче на основном носителе, и является ключевым элементом защиты от умышленной и неумышленной потери данных.

3.2. Конкретные информационные ресурсы, подлежащие резервному копированию, порядок их копирования приводятся в регламенте резервного копирования (далее – Регламент).

3.3. Регламент составляется администратором безопасности. Регламент должен содержать перечень информационных ресурсов, подлежащих резервному копированию, и график осуществления резервного копирования, составленный с учетом требований руководителей структурных подразделений и администратора безопасности.

3.4.Резервное копирование осуществляется администратором безопасности и контролируется ответственным за обеспечение безопасности ПДн при их обработке в информационных системах персональных данных.

3.5.При осуществлении резервного копирования используется два типа копирования: полное резервное копирование и инкрементальное резервное копирование.

3.6. Резервное копирование информационных ресурсов МКУДО «ЦРТДиЮ».
осуществляется по трехуровневой схеме ротации, в соответствии с которой:

- полное резервное копирование информационных ресурсов выполняется 15-16 числа каждого месяца (архив хранится в течение года и является архивом Уровня 1);
- полное резервное копирование информационных ресурсов выполняется в конце каждой недели (в пятницу) (архив хранится в течение календарного месяца и является архивом Уровня 2);
- полное резервное копирование информационных ресурсов выполняется в начале каждой недели (в ночь с воскресенья на понедельник), затем ежедневно на эту копию выполняется инкрементальное копирование (архив хранится в течение недели и является архивом Уровня 3).

3.7.Администратор безопасности настраивает задания для программного обеспечения, осуществляющего резервное копирование, на автоматическое выполнение в соответствии с перечнем информационных ресурсов, подлежащих резервному копированию и графиком резервного копирования.

3.8.Перед выполнением задания резервного копирования администратор безопасности проверяет доступность резервного носителя, а также наличие на нем свободного места для записи данных.

3.9. Хранение резервных копий должно быть организовано в отдельном от копируемых информационных ресурсов помещении или на отдельном информационном ресурсе, которые должны обеспечивать конфиденциальность сведений, содержащихся в резервных копиях.

3.10. Носители резервных копий должны храниться в специально отведенных для этого надежно запираемых хранилищах (шкафах, сейфах) или отдельных ячейках таких хранилищ. Доступ к хранилищу резервных копий должны иметь только администратор безопасности и ответственный за обеспечение безопасности персональных данных при их обработке в информационной системе персональных данных в МКУДО «ЦРТДиЮ».

3.11.В случае потери данных на основном носителе из хранилища извлекается накопитель с резервной копией информационных ресурсов, нуждающихся в восстановлении, от последнего произведенного резервного копирования. Данные восстанавливаются в исходное место расположения.

3.12.В зависимости от характера и уровня повреждения информационных ресурсов администратор безопасности восстанавливает либо весь массив резервных данных либо отдельные поврежденные или уничтоженные файлы и папки.

4. Порядок контроля за защитой информации в ИСПДн

4.1.**Контроль за защитой информации в ИСПДн** - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-

технических воздействий, вызывающих нарушение целостности информации или работоспособности систем информатизации.

4.2. Основными задачами контроля являются:

— проверка организации выполнения мероприятий по защите информации в структурных подразделениях МКУДО «ЦРТДиЮ» и учета требований по защите информации, содержащихся в локальных актах организации и разрабатываемых проектах документов;

— оценка достаточности и эффективности мероприятий по защите информации;

— проверка выполнения требований по защите ИСПДн от несанкционированного доступа и программно-технических воздействий на информацию;

— проверка выполнения требований по антивирусной защите автоматизированных систем;

— оперативное принятие мер по пресечению возможных или выявленных нарушений требований (норм) защиты информации в ИСПДн организации.

4.3.Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей на объектах обработки ПДн в МКУДО «ЦРТДиЮ», и осуществляется по объектовому принципу при котором на объекте проверяется вся система защиты информации.

4.4. В ходе контроля проверяются:

— соответствие принятых мер по обеспечению безопасности персональных данных (далее - ОБ ПДн) требованиям нормативно-методических документов ФСТЭК России;

— своевременность и полнота выполнения требований настоящего Положения и других руководящих документов по ОБ ПДн;

— эффективность применения организационных мероприятий по защите информации;

— устранение ранее выявленных недостатков.

4.5. Основными видами контроля являются визуально-оптический контроль, контроль несанкционированного доступа к информации и программно-технических воздействий на информацию.

4.6. Невыполнение предписанных мероприятий по защите ПДн считается предпосылкой к утечке информации (далее - предпосылка).

По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию *директору* проводится расследование.

4.7. Контроль защиты информации осуществляется путем проведения периодических, плановых и внеплановых проверок системы защиты объектов ИСПДн.

4.8. Одной из форм контроля защиты информации является обследование объектов ИСПДн. Оно проводится не реже одного раза в 2 года. В ходе обследования проверяется:

— соблюдение организационно-режимных требований обеспечения безопасности ПДн при их обработке в ИСПДн;

— выполнение требований по защите автоматизированных систем от несанкционированного доступа;

— выполнение требований по антивирусной защите.

5. Порядок проверки электронного журнала обращений к ИСПДн

5.1.Проверка электронного журнала обращений проводится с целью выявления несанкционированного доступа к конфиденциальной информации, содержащейся в ИСПДн.

5.2. Право проверки электронного журнала обращений имеют:

— ответственный за обеспечение безопасности персональных данных в информационной системе персональных данных;

— администратор безопасности.

5.3. В ИСПДн, где установлены средства защиты информации (далее - СЗИ), проверка электронного журнала производится в соответствии с прилагаемым к указанным СЗИ руководством.

6. Правила антивирусной защиты

Система антивирусной защиты информации предназначена для предотвращения заражения программными вирусами информационно-вычислительных ресурсов ИСПДн.

Антивирусная защита информации в МКУДО «ЦРТДиЮ»
осуществляется посредством применения организационных мер и средств антивирусной защиты информации.

6.1.Организационная структура системы антивирусной защиты информации в МКУДО «ЦРТДиЮ» включает:

- администратора безопасности;

- лиц, назначенных приказом *директора,* ответственными за защиту информации в МКУДО «ЦРТДиЮ»;

- должностных лиц структурных подразделений;

- пользователей средств вычислительной техники (далее - пользователи).

6.2.Общее руководство организацией, обеспечением антивирусной защиты информации в МКУДО «ЦРТДиЮ» осуществляет администратор безопасности, в том числе:

- планирование мероприятий по антивирусной защите информации;

- рассмотрение и анализ заявок подразделений на установку средств антивирусной защиты информации;

- планирование оснащения структурных подразделений средствами антивирусной защиты информации;

- организацию и сопровождение эксплуатации системы антивирусной защиты информации;

- контроль состояния антивирусной защиты информации в структурных подразделениях;

- анализ состояния антивирусной защиты информации и разработку предложений о совершенствовании системы антивирусной защиты информации в МКУДО «ЦРТДиЮ»;

- организацию служебных проверок по фактам заражения компьютерными вирусами информации в автоматизированных системах;

- обеспечивает периодическое обновление баз данных средств антивирусной защиты информации.

6.3.Руководители осуществляют контроль за выполнением мероприятий по антивирусной защите информации на средствах вычислительной техники, эксплуатируемых в подразделении.

6.4.Пользователям запрещается отключать средства антивирусной защиты информации во время работы.

6.5. Состояние антивирусной защиты отражается в отчете администратора безопасности о состоянии информационной безопасности в МКУДО «ЦРТДиЮ».

6.6.Порядок применения средств антивирусной защиты информации устанавливается с учетом соблюдения следующих требований:

- обязательный входной контроль за отсутствием программных вирусов во всех поступающих на объект информатизации машинных носителях информации, информационных массивах, программных средствах общего и специального назначения;

- периодическая проверка на предмет отсутствия программных вирусов жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка используемых в работе гибких магнитных дисков перед началом работ с ними;

- внеплановая проверка магнитных носителей информации в случае подозрения на наличие программных вирусов.

6.7.Средства антивирусной защиты информации должны устанавливаться на всех средствах вычислительной техники, эксплуатируемых в МКУДО «ЦРТДиЮ». В первую очередь их устанавливают на серверах баз данных.

6.8.Инсталляция и настройка средств антивирусной защиты информации осуществляются в соответствии с программной и эксплуатационной документацией, поставляемой в комплекте с ними.

6.9.В случае обнаружения программных вирусов при входном контроле гибких магнитных носителей, файлов, поступивших в структурное подразделение, пользователь обязан:

- прекратить процесс приема-передачи информации;

- сообщить администратору безопасности и ответственному за обеспечение безопасности персональных данных в информационной системе о факте обнаружения программного вируса;

- принять меры для локализации и удаления программных вирусов с использованием средств антивирусной защиты информации;

- сообщить о факте обнаружения программных вирусов в организацию, из которой поступили зараженные гибкие магнитные носители или файлы.

6.10.При обнаружении программных вирусов в процессе обработки информации пользователь обязан:

- немедленно прекратить все работы;

-сообщить администратору безопасности и ответственному за обеспечение безопасности персональных данных в информационной системе о факте обнаружения программных вирусов;

- принять меры для локализации и удаления программных вирусов с использованием средств антивирусной защиты информации.

6.11.Программные средства общего и специального назначения объекта информатизации, используемые для обработки информации ограниченного распространения, в случае невозможности удаления вирусов не подлежат дальнейшей эксплуатации.

В случае невозможности удаления тел вирусов из программ необходимо осуществить полную переустановку программного обеспечения с форматированием жесткого диска на зараженной ПЭВМ.

6.12.Ответственность за выполнение мероприятий по антивирусной защите информации на средствах вычислительной техники, эксплуатируемых подчиненными лицами в подразделении, работающем с ИСПДн, в соответствии с требованиями настоящего Положения, возлагается на руководителя подразделения.

6.13.Ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты информации на своих рабочих местах, в том числе за обновление антивирусных баз и получение новых лицензионных ключей, несут пользователи.

6.14.Ответственность за проведение профилактических мероприятий по обеспечению антивирусной защиты, периодический контроль за состоянием антивирусной защиты,

уничтожение выявленных вирусов, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящего Положения работниками подразделений МКУДО «ЦРТДиЮ» возлагается на администратора безопасности.

7.Правила парольной защиты

7.1.Настоящий раздел регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

Организационное, методическое и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ИСПДн возлагается на администратора безопасности, контроль действий которого осуществляет ответственный за обеспечение безопасности персональных данных в информационной системе.

7.2.**Первичный пароль** - комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливаемая администратором безопасности при создании новой учетной записи. Ответственность за сохранность первичного пароля лежит на администраторе безопасности.

7.3.Первичный пароль может содержать несложную комбинацию символов либо повторяющиеся символы.

7.4.При создании первичного пароля администратор безопасности обязан установить опцию, требующую смены пароля при первом входе в систему, а также уведомить владельца учетной записи о необходимости произвести смену пароля.

7.5.Первичный пароль так же используется при сбросе забытого пароля на учетную запись. В любом случае, при использовании первичного пароля все требования настоящего документа сохраняются.

7.6.**Основной пароль** – комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная только пользователю, используемая для подтверждения подлинности владельца учетной записи.

7.7. Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью.

7.8. При выборе пароля необходимо руководствоваться следующим:

7.8.1.пароли **НЕ ДОЛЖНЫ** состоять:

- из имени, отчества или фамилии работника ни в каком виде (т.е. написаны в строчном, прописном, смешанном виде, задом наперед, два раза и т.д.);
- из идентификатора работника (login) ни в каком виде;
- из личной информации о работнике: номер телефона, номер в пропусках и других документах, номер или марка автомобиля, почтовый адрес и т.п.;
- только из цифр или одинаковых букв;
- меньше чем из шести символов.

7.8.2. пароли **ДОЛЖНЫ**:

- содержать строчные и заглавные буквы;
- содержать небуквенные символы (т.е. цифры, знаки пунктуации, специальные символы).

7.9. Пользователь несет персональную ответственность за сохранение конфиденциальности основного пароля. Запрещается сообщать пароль другим лицам, в том числе сотрудникам подразделения, записывать его, а так же пересылать открытым текстом в электронных

сообщениях и по телефону.

7.10.Администратор безопасности обязан настроить механизм обязательной смены основного пароля не реже одного раза в 90 дней, соблюдая требования настоящего документа.

7.11. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом администратору безопасности и изменить основной пароль.

7.12.Восстановление забытого основного пароля пользователя осуществляется администратором безопасности путем изменения (сброса) основного пароля пользователя на первичный пароль на основании письменной либо электронной заявки пользователя. Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений. Копия заявки направляется администратору безопасности.

7.13.Для предотвращения угадывания паролей администратор безопасности обязан настроить механизм блокировки учетной записи при трехкратном неправильном вводе пароля.

7.14.Разблокирование учетной записи пользователя осуществляется администратором безопасности на основании заявки владельца учетной записи. Копия заявки направляется администратору безопасности.

7.15.**Административный пароль** - комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная администратору безопасности, используемая при настройке служебных учетных записей, учетных записей служб и сервисов, а также специальных учетных записей.

7.16.Администратор безопасности несет персональную ответственность за сохранение конфиденциальности административного пароля. Запрещается сообщать пароль другим лицам, в том числе работникам, записывать его, а также пересылать открытым текстом в электронных сообщениях и по телефону.

7.17.Администратор безопасности обязан не реже одного раза в 90 дней производить смену административного пароля, соблюдая требования настоящего документа.

7.18.В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно изменить административный пароль.

7.19.Копии административных паролей должны храниться в опечатанном конверте в сейфе.

8. Действия при обнаружении фактов несанкционированного доступа к ИСПДн

8.1. К попыткам несанкционированного доступа относятся:

- сеансы работы с персональными данными незарегистрированных пользователей или пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;

- действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.

8.2.При обнаружении фактов несанкционированного доступа работники МКУДО «ЦРТДиЮ» обязаны доложить об этом администратору безопасности.

8.3. Администратор безопасности обязан:

- прекратить несанкционированный доступ к ПДн;

- доложить *Директору* МКУДО «ЦРТДиЮ» служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

- известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа.

9.Правила технического обслуживания, обновления общесистемного и прикладного программного обеспечения (ПО)

9.1. Все изменения конфигураций технических и программных средств ПЭВМ должны производиться только на основании заявок ответственного за эксплуатацию данной ПЭВМ.

9.2.Право внесения изменений в конфигурацию аппаратно-программных средств защищенных ПЭВМ предоставляется:

- в отношении системных и прикладных программных средств - администратору безопасности;

- в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты - ответственному за обеспечение безопасности персональных данных в информационной системе.

9.3.Изменение конфигурации аппаратно-программных средств ПЭВМ кем-либо, кроме вышеуказанного работника, ***запрещено***.

9.4.Процедура внесения изменений в конфигурацию системных и прикладных программных средств ПЭВМ инициируется заявкой ответственного за обеспечение безопасности персональных данных в информационной системе.

9.5. В заявке могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств ПЭВМ:

— установка (развертывание) на ПЭВМ программных средств, необходимых для решения определенной задачи (расширение возможностей для решения данной задачи в данной ИСПДн);

— обновление (замена) на ПЭВМ программных средств, необходимых для решения определенной задачи (обновление версий используемых для решения определенной задачи программ);

— удаление из ПЭВМ программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данной ПЭВМ).

Также в заявке указывается условное наименование объекта ПЭВМ.

9.6.Заявку рассматривает ответственный за обеспечение безопасности персональных данных в информационной системе, который определяет производственную необходимость проведения указанных в заявке изменений и принимает по ней решение.

При положительном решении заявка передается администратору безопасности для непосредственного исполнения работ по внесению изменений в конфигурацию ПЭВМ, указанной в заявке.

9.7. Подготовка обновления, модификации общесистемного и прикладного программного обеспечения ИСПДн, тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов установленного программного обеспечения, внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов на ПЭВМ, обновление и

удаление системных и прикладных программных средств производится администратором безопасности. Работы производятся в присутствии ответственного за эксплуатацию данной ПЭВМ.

9.8.Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

9.9.Установка или обновление ПО (системного, тестового и т.п.) производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных установленным порядком, прикладного ПО - с эталонных копий программных средств, полученных из архива дистрибутивов установленного программного обеспечения.

9.10.Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены в установленном порядке на работоспособность, а также отсутствие опасных функций.

9.11.После установки (обновления) ПО, администратор безопасности должен произвести требуемые настройки средств управления доступом к компонентам ПЭВМ, проверить работоспособность ПО и правильность их настройки, произвести соответствующую запись в журнале учета нештатных ситуаций ПЭВМ, выполнения профилактических работ, установки и модификации программных средств ПЭВМ, примерная форма которого указана в приложении к настоящему Положению, сделать отметку о выполнении работ (на обратной стороне заявки).

9.12. При возникновении ситуаций, требующих передачи ПЭВМ на ремонт, ответственный за ее эксплуатацию докладывает об этом ответственному за обеспечение безопасности персональных данных в информационной системе в МКУДО «ЦРТДиЮ». В данном случае администратор безопасности обязан предпринять необходимые меры для уничтожения защищаемой информации, которая хранилась на дисках ПЭВМ.

9.13.Факт уничтожения данных, находившихся на диске ПЭВМ, оформляется составлением акта в порядке, предусмотренном инструкцией по уничтожению персональных данных в МКУДО «ЦРТДиЮ».

9.14.С целью соблюдения принципа персональной ответственности за свои действия каждому работнику, допущенному к работе на ПЭВМ конкретной ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать на данной ПЭВМ.

9.15. Использование несколькими пользователями при работе на ПЭВМ одного и того же имени пользователя («группового имени») ***запрещено.***

9.16. Процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой ответственного за обеспечение безопасности персональных данных в информационной системе.

10. Порядок контроля соблюдения условий использования средств защиты информации (СЗИ)

10.1. Порядок работы с техническими СЗИ определен в соответствующих инструкциях, руководствах по настройке и использованию СЗИ, обязательных для исполнения как работниками, обрабатывающими конфиденциальную информацию, так и администратором безопасности ИСПДн.

10.2. Право проверки соблюдения условий использования СЗИ имеют:

— ответственный за обеспечение безопасности персональных данных в информационной системе;

— администратор безопасности.

10.3. Пользователю ИСПДн категорически **запрещается**:

— обработка ПДн с отключенными СЗИ;

— менять настройки СЗИ.

11. Порядок допуска посторонних лиц в защищаемые помещения

11.1 Вскрытие и закрытие помещений осуществляется работниками, чьи рабочие места расположены в данных помещениях.

11.2.Ответственный за обеспечение безопасности персональных данных в информационной системе и администратор безопасности организуют проверку объекта ИСПДн на предмет несанкционированного доступа к персональным данным, наличие документов и машинных носителей информации, о чём докладывается Директору МКУДО «ЦРТДиЮ».

Приложение

Журнал учета нештатных ситуаций ПЭВМ, выполнения профилактических работ, установки и модификации программных средств ПЭВМ

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО исполнителей и их подписи	ФИО ответственного за эксплуатацию ПЭВМ, подпись	Подпись специалиста по защите информации	Примечание (ссылка на заявку)
1	2	3	4	5	6	7