МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ «ДОМ ДЕТСКОГО ТВОРЧЕСТВА» МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ – МИХАЙЛОВСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН РЯЗАНСКОЙ ОБЛАСТИ

391710, Рязанская обл., г. Михайлов, ул. Победы, д.3А, тел.: 8-(49130)- 2-21-12

ПРИКАЗ

«09» февраля 2021 г. № 06

«Об утверждении инструкций по защите персональных данных»

Во исполнение Федерального закона Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона №152-ФЗ от 27.07.2006 г. «О персональных данных» и прочих нормативных документов по защите информации, а также с целью обеспечения безопасности персональных данных в МБУ ДО «ДДТ»,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Инструкцию пользователя информационных систем персональных данных МБУ ДО «ДДТ» согласно Приложению 1 к настоящему приказу.
2. Утвердить и ввести в действие Инструкцию по парольной защите информации в МБУ ДО «ДДТ» согласно Приложению 2 к настоящему приказу.
3. Утвердить и ввести в действие Инструкцию по организации антивирусной защиты информации в МБУ ДО «ДДТ» согласно Приложению 3 к настоящему приказу.
4. Утвердить и ввести в действие Порядок обращения со съемными машинными носителями персональных данных в МБУ ДО «ДДТ» согласно Приложению 4 к настоящему приказу.
5. Требования настоящего приказа довести до работников, осуществляющх обработку персональных данных в информационных системах персональных данных в МБУ ДО «ДДТ».
6. Контроль исполнения настоящего Приказа оставляю за собой.

Директор МБУ ДО «ДДТ» И.Н. Лаврентьева

Приложение 1
к приказу МБУ ДО «ДДТ»
от «09» февраля 2021 г. № 06

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных МБУ ДО «ДДТ»

1. Термины и определения

Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

Антивирусная защита – защита информации и компонентов информационной системы от вредоносных компьютерных программ (вирусов) (обнаружение вредоносных компьютерных программ (вирусов), блокирование, изолирование "зараженных" объектов, удаление вредоносных компьютерных программ (вирусов) из "зараженных" объектов).

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

Пользователь информационной системы персональных данных – работник, осуществляющий обработку персональных данных в информационной системе персональных данных;

Средство антивирусной защиты – программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации;

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция пользователя информационных систем персональных данных МБУ ДО «ДДТ» (далее – Инструкция) определяет обязанности, права и ответственность работников при работе в информационных системах персональных данных (далее – ИСПДн).

2.2. Требования настоящей Инструкции являются обязательными для всех работников, осуществляющих обработку и защиту персональных данных (далее – ПДн) в ИСПДн – пользователей ИСПДн (далее – Пользователи).

2.3. К защищаемой информации, обрабатываемой в ИСПДн МБУ ДО «ДДТ» (далее – Учреждение), относятся ПДн, служебная (технологическая) информация системы защиты и другая информация ограниченного доступа.

2.4. Все пользователи ИСПДн Учреждения должны быть ознакомлены с требования настоящей Инструкции под подпись.

2.5. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и ПДн, и не исключает обязательного выполнения их требований.

3. Допуск пользователей к информационным системам персональных данных

3.1. Допуск пользователей к работе с ПДн в ИСПДн осуществляется в соответствии с Матрицей доступа к информационным ресурсам.

3.2. К самостоятельной работе на автоматизированных рабочих местах (далее – АРМ), входящих в состав ИСПДн, допускаются лица, изучившие требования настоящей Инструкции и локальных нормативных актов по защите информации, освоившие правила эксплуатации АРМ и технических средств защиты.

3.3. Допуск производится после проверки знания настоящей Инструкции и практических навыков в работе.

4. Обязанности пользователя

4.1. Каждый Пользователь имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

4.1.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн.

4.1.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными в ИСПДн.

4.1.3. Выполнять требования по антивирусной защите в части, касающейся действий Пользователей.

4.1.4. Немедленно ставить в известность ответственного за обеспечение безопасности ПДн в ИСПДн или администратора ИСПДн:

- при подозрении компрометации личного пароля;
- 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 ИСПДн;
- некорректного функционирования установленных средств защиты;
- обнаружения непредусмотренных отводов кабелей и подключенных устройств;
- обнаружения фактов, попыток несанкционированного доступа и случаев нарушения установленного порядка обработки ПДн.

4.1.5. Экран видеомонитора в помещении располагать во время работы так, чтобы исключалась возможность ознакомления с отображаемой на них информацией посторонними лицами.

4.2. Пользователям ИСПДн запрещается:

- отключать (блокировать) средства защиты информации, предусмотренные организационно-распорядительными документами на ИСПДн;
- производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;
- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- обрабатывать в ИСПДн информацию и выполнять другие работы, не предусмотренные перечнем прав Пользователя по доступу к ИСПДн;
- сообщать (или передавать) посторонним лицам личные атрибуты и пароли доступа к ресурсам ИСПДн;
- работать в ИСПДн при обнаружении каких-либо неисправностей;
- оставлять включенным без присмотра АРМ, не активизировав средства защиты от несанкционированного доступа;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к ознакомлению с защищаемой информацией посторонних лиц;
- производить перемещения технических средств АРМ без согласования с ответственным за обеспечение безопасности ПДн в ИСПДн;
- вскрывать корпуса технических средств АРМ и вносить изменения в схему и конструкцию устройств.

5. Организация работы со съемными машинными носителями информации

5.1. Организация работы со съемными машинными носителями информации (далее – СМНИ), содержащие ПДн и иную информацию конфиденциального характера, осуществляется в соответствии с «Порядком обращения со съемными машинными носителями информации в МБУ ДО «ДДТ».

5.2. Пользователи обязаны знать и соблюдать установленные требования по учету и хранению СМНИ.

5.3. СМНИ должен быть зарегистрирован в «Журнале учета съемных машинных носителей информации».

5.4. СМНИ закрепляется за определенным лицом, несущим ответственность за сохранность и местонахождение данного СМНИ.

5.5. При необходимости передачи информации на СМНИ, лицо ответственное за хранение уведомляет ответственного за обеспечение безопасности ПДн в ИСПДн о необходимости передачи информации с помощью СМНИ, доставляет СМНИ по месту назначения, передает информацию с него и возвращает его на место хранения.

5.6. Хранение СМНИ осуществляется:

- для флеш-карт, смарт-карт, компакт дисков и др.) в защищенных сейфах;
- для СМНИ, входящих в состав ИСПДн, производится опечатывание корпуса АРМ.

5.7. Пользователям запрещается:

- записывать и хранить ПДн и иную информацию конфиденциального характера на неучтенных СМНИ;
- оставлять СМНИ без присмотра, передавать их другим лицам и выносить за пределы контролируемой зоны, за исключением случаев, в которых разрешена передача СМНИ;
- хранить СМНИ вблизи сильных источников электромагнитных излучений и прямых солнечных лучей;
- хранить на учтенных СМНИ программы и данные, не относящиеся к рабочей информации.

6. Организация парольной защиты

6.1. Организация парольной защиты производится в соответствии с «Инструкцией по парольной защите информации в МБУ ДО «ДДТ».

6.2. Лица, использующие пароли, обязаны:

- хранить в тайне свой пароль
- четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов;
- своевременно сообщать ответственному за обеспечение безопасности ПДн в ИСПДн обо всех нештатных ситуациях, нарушениях работы систем защиты от несанкционированного доступа, возникающих при работе с паролями.

6.3. Во время ввода паролей необходимо исключить возможность его просмотра посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или отражённом свете) или техническими средствами (видеокамеры, фотоаппараты и др.)

6.4. Для предотвращения доступа к персональным данным, пользователь во время перерыва в работе обязан осуществить блокирование системы нажатием комбинации Ctrl+Alt+Delete и кнопки «Блокировать» или нажатием комбинации Win+L.

6.5. Блокирование сеанса доступа пользователя в ИСПДн осуществляется после 15 минут его бездействия (неактивности).

6.6. В случае утери пароля сотрудник ставит в известность своего непосредственного руководителя и ответственного за обеспечение безопасности ПДн в ИСПДн для принятия последующих решений.

6.7. В случае компрометации пароля (просмотр посторонними, разглашение пароля и др.) необходимо известить своего непосредственного руководителя и ответственного за обеспечение безопасности ПДн в ИСПДн для принятия последующих решений.

7. Правила работы в сетях общего доступа и (или) международного обмена

7.1. Работа в сетях общего доступа и на элементах ИСПДн, должна осуществляться исключительно в служебных целях.

7.2. При работе в сетях общего доступа запрещается:

- осуществлять работу при отключенных средствах защиты;
- передавать по сетям общего доступа защищаемую информацию без использования средств шифрования;

- запрещается скачивать из сети Интернет программное обеспечение и другие файлы, если это не определено его должностными обязанностями;
- запрещается посещение и использование сети Интернет в личных целях.

8. Порядок установки обновлений программного обеспечения

8.1. Установке крупных обновлений программного обеспечения должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий от устанавливаемых обновлений.

8.2. В случае обнаружения негативного воздействия устанавливаемого обновления на штатное функционирование информационной инфраструктуры, данное обновление устанавливаться не должно по согласованию с администратором ИСПДн.

8.3. Установке новых версий программного обеспечения или внесению серьезных изменений и дополнений в действующее программное обеспечение должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий указанного программного обеспечения.

8.4. Установка протестированных обновлений, новых версий программного обеспечения или внесение изменений и дополнений в действующее программное обеспечение может быть произведено только по согласованию с администратором ИСПДн и ответственным за обеспечение безопасности ПДн в ИСПДн.

9. Технология обработки персональных данных

9.1. При первичном допуске к работе в ИСПДн Пользователь знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных документов по вопросам автоматизированной обработки информации, изучает Инструкцию, получает персональный идентификатор или личный пароль у ответственного за обеспечение безопасности ПДн в ИСПДн.

9.2. В процессе работы Пользователь производит обработку ПДн в ИСПДн.

9.3. При необходимости вывод ПДн из ИСПДн осуществляется следующим образом:

- копированием ПДн на учтенные СМНИ;
- передача ПДн по каналам связи с обязательным применением средств криптографической защиты.

10. Срок действия и порядок внесения изменений

10.1. Настоящая Инструкция вступает в силу с момента его утверждения и действует бессрочно.

10.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

10.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом директора Учреждения.

Приложение 2
к приказу МБУ ДО «ДДТ»
от «09» февраля 2021 г. № 06

ИНСТРУКЦИЯ
по парольной защите информации в МБУ ДО «ДДТ»

1. Термины и определения

Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователь информационной системы персональных данных – работник, осуществляющий обработку персональных данных в информационной системе персональных данных.

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция по парольной защите информации в МБУ ДО «ДДТ» (далее – Инструкция) устанавливает требования и ответственность при организации парольной защиты информации, а также определяет порядок контроля над действиями пользователей и обслуживающего персонала информационных систем персональных данных (далее – ИСПДн) при работе с паролями.

2.2. Требования настоящей Инструкции являются обязательными для исполнения всеми пользователями и администраторами ИСПДн МБУ ДО «ДДТ» (далее – Учреждение), использующими в своей работе средства вычислительной техники.

2.3. Все пользователи и администраторы ИСПДн Учреждения, использующие в своей работе средства вычислительной техники, должны быть ознакомлены с требованиями настоящей Инструкции под подпись.

2.4. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и персональных данных (далее – ПДн), и не исключает обязательного выполнения их требований.

3. Требования, предъявляемые к идентификаторам (кодам) и паролям (порядок формирования и обращения с ними)

3.1. Авторизация пользователей ИСПДн осуществляется путем ввода идентификатора и/или пароля.

3.2. Требования к формированию паролей и обращению с ними.

3.2.1. Пароль формируется при создании учетной записи ответственным обеспечение безопасности ПДн в ИСПДн или администратором ИСПДн, при первичном входе в учетную запись пароль должен быть изменен владельцем.

3.2.2. Владельцы личных паролей обязаны обеспечить их тайну.

3.2.3. Пароли генерируются с учетом следующих требований:

- пароль должен знать только его владелец;
- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать смысловую нагрузку (имена, фамилии, наименования организаций, улиц, городов и т.д.), общепринятые сокращения (userOl, password02 и т.п.) и последовательные сочетания клавиш клавиатуры (qwertyOl, Ицукен12);
- максимальный срок действия пароля составляет 120 дней;
- минимальный срок действия пароля составляет 2 дня;
- количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя должно быть не более 6.

3.2.4. Требования к формированию паролей обеспечиваются техническими возможностями используемых операционных систем, средств защиты информации и информационных ресурсов.

3.2.5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в полгода. Внеплановая смена пароля производится в случае его компрометации, а также по просьбе пользователя ИСПДн.

3.2.6. Хранение пользователями ИСПДн своих паролей на бумажном носителе ЗАПРЕЩЕНО.

3.2.7. Пользователь не имеет права сообщить личный пароль другим лицам (разрешается только с согласования ответственного за обеспечение безопасности или администратора ИСПДн при наличии технологической необходимости использования имен и паролей работников в их отсутствие в случае возникновения нештатбных ситуаций, форс-мажорных обстоятельств и т.п. По возращению работники обязаны сразу же сменить свои пароли на новые значения согласно данной Инструкции).

3.3. Порядок смены паролей и идентификаторов при изменениях в организационно-штатной структуре (кадровые перестановки, увольнение работников):

3.3.1. При прекращении действия трудового договора с работником все созданные для этого работника учетные записи (пользовательское имя) подлежат блокированию не позднее, чем в день увольнения работника. Полное удаление учетных записей производится в течении 5 рабочих дней со дня увольнения работника. Основанием для блокирования и последующего удаления учетных записей работника является заявка,

представленная непосредственным руководителем увольняемого не позднее, чем за 3 рабочих дня до дня его увольнения.

3.3.2. При проведении организационно-штатных мероприятий (кадровые перестановки) непосредственный руководитель структурного подразделения обязан представить администратору ИСПДн заявку на изменение в правах доступа.

3.4. Порядок действий при компрометации идентификаторов и паролей.

3.4.1. Под компрометацией понимается: утрата пароля учетной записи и (или) пароля идентификатора, разглашение учетной записи пароля или пароля идентификатора (явная компрометация), или иная ситуация, которая дает основание для предположения о нарушении конфиденциальности паролей и идентификаторов (неявная компрометация).

3.4.2. При выявлении факта утраты пароля, разглашения пароля, пароля идентификатора, самого идентификатора пользователь обязан незамедлительно сообщить о данных фактах своему непосредственному руководителю и ответственному за обеспечение безопасности ПДн в ИСПДн или администратору ИСПДн.

3.4.3. В случае выявления факта компрометации идентификаторов и паролей пользователя администратор ИСПДн или ответственный за обеспечение безопасности ПДн в ИСПДн обязан немедленно заблокировать учетную запись данного пользователя и незамедлительно произвести внеплановую смену пароля для этого пользователя.

4. Права и обязанности

4.1. Основные задачи администратора ИСПДн:

- организация установки средств идентификации и аутентификации;
- организация парольной защиты во всех ИСПДн;
- выдача первичных паролей, и электронных персональных идентификаторов и паролей к ним;
- осуществление контроля за состоянием системы парольной защиты информации в ИСПДн.

4.2. Администратор ИСПДн имеет право:

- вносить предложения по совершенствованию системы парольной защиты информации в ИСПДн;
- принимать участие в планировании мероприятий по парольной защите информации в ИСПДн и планировании оснащения средствами идентификации и аутентификации;
- осуществлять контроль состояния средств идентификации и аутентификации в ИСПДн;
- инициировать служебные проверки и участвовать в проведении расследований по фактам компрометации;
- оказывать помощь в решении проблем, возникающих при эксплуатации средств идентификации и аутентификации.

4.3. Обязанности в части парольной защиты информации отражены в инструкции администратора ИСПДн.

4.4. Пользователям ИСПДн в своей работе запрещается:

- сообщать кому-либо свой личный пароль и/или пароль к электронному персональному идентификатору;
- передавать кому-либо выданный электронный персональный идентификатор;

- осуществлять вход в операционные системы ИСПДн и в информационные ресурсы под чужими идентификаторами и паролями;
- отключать средства идентификации и аутентификации.

4.5. В случае появления подозрений на факт компрометации пароля, а также в случае выявления инцидентов (фактов и т.п.), связанных со сбоями в работе средств идентификации и аутентификации, пользователи обязаны немедленно проинформировать об этом ответственного за обеспечение безопасности ПДн в ИСПДн или администратора ИСПДн.

5. Ответственность должностных лиц в рамках системы парольной защиты информации

5.1. Пользователи, ответственный за обеспечение безопасности ПДн в ИСПДн и администратор ИСПДн несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.

5.2. Пользователи, ответственный за обеспечение безопасности ПДн в ИСПДн и администратор ИСПДн несут ответственность по действующему законодательству Российской Федерации за разглашение сведений конфиденциального характера, ставших известными при выполнении служебных обязанностей, в том числе предусмотренных настоящей Инструкцией.

6. Срок действия и порядок внесения изменений

6.1. Настоящая Инструкция вступает в силу с момента его утверждения и действует бессрочно.

6.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

6.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом директора Учреждения.

Приложение 3
к приказу МБУ ДО «ДДТ»
от «09» февраля 2021 г. № 06

ИНСТРУКЦИЯ
по антивирусной защите
МБУ ДО «ДДТ»

1. Термины и определения

Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

Антивирусная защита – защита информации и компонентов информационной системы от вредоносных компьютерных программ (вирусов) (обнаружение вредоносных компьютерных программ (вирусов), блокирование, изолирование "зараженных" объектов, удаление вредоносных компьютерных программ (вирусов) из "зараженных" объектов).

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Пользователь информационной системы персональных данных – работник, осуществляющий обработку персональных данных в информационной системе персональных данных.

Средство антивирусной защиты – программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации.

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция по антивирусной защите МБУ ДО «ДДТ» (далее – Инструкция) регулирует вопросы организации антивирусной защиты и требования к порядку проведения антивирусного контроля.

2.2. Инструкция устанавливает требования и ответственность при организации защиты информации от разрушающего воздействия вредоносных программ – компьютерных вирусов.

2.3. Требования настоящей Инструкции являются обязательными для исполнения всеми работниками МБУ ДО «ДДТ» (далее – Учреждения), использующими в своей работе средства вычислительной техники.

2.4. Все работники Учреждения, использующие антивирусные средства, должны быть ознакомлены с требованиями настоящей Инструкцией под подпись.

2.5. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и персональных данных (далее – ПДн), и не исключает обязательного выполнения их требований.

3. Требования к антивирусным средствам

3.1. В Учреждении к применению допускаются только лицензионные антивирусные программные и (или) программно-аппаратные средства (антивирусные средства), закупленные у разработчика указанных средств или его официальных дилеров.

3.2. Антивирусные средства должны функционировать в течение всего времени работы средств вычислительной техники (от момента загрузки операционной системы до момента ее выгрузки).

3.3. Антивирусное средство не должно существенно затруднять работоспособность средств вычислительной техники информационных систем персональных данных (далее – ИСПДн).

4. Права и обязанности

4.1. Антивирусной защите подлежит вся, обрабатываемая в Учреждении при помощи средств вычислительной техники, информация, независимо от ограничений доступа к ней.

4.2. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль.

4.3. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

4.4. В ИСПДн запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

4.5. Сопровождение (регулярное обновление, антивирусный контроль, выявление фактов заражения и проведение служебных расследований) правил антивирусной защиты возлагаются на ответственного за обеспечение безопасности ПДн в ИСПДн.

4.6. Основные задачи ответственного за обеспечение безопасности ПДн в ИСПДн:

- организация процесса установки антивирусных средств в ИСПДн;
- сопровождение антивирусных средств (обновление, антивирусный контроль, сопровождение действий пользователей в случаях обнаружения вирусов, обеспечение работоспособности антивирусных средств);
- контроль состояния системы антивирусной защиты информации в Учреждении.

4.7. Ответственный за обеспечение безопасности ПДн в ИСПДн несет ответственность за:

- за своевременную установку антивирусных средств;
- за эксплуатацию (антивирусный контроль, работоспособность антивирусных средств, сопровождение действий пользователей в случаях обнаружения вирусов) системы антивирусной защиты информации;
- за своевременное обновление лицензий на антивирусные средства;
- за своевременное обновление антивирусных баз.

4.8. Ответственный за обеспечение безопасности ПДн в ИСПДн имеет право:

- вносить предложения по совершенствованию системы антивирусной защиты информации;
- принимать участие в планировании мероприятий по антивирусной защите информации и планировании оснащения антивирусными средствами;
- осуществлять контроль состояния средств антивирусной защиты информации в Учреждении;
- инициировать служебные проверки и участвовать в проведении расследований по фактам заражения вирусами ИСПДн и средств вычислительной техники;
- оказывать помощь в решении проблем, возникающих при эксплуатации средств антивирусной защиты.

4.9. Пользователь антивирусного средства – лицо, на рабочем месте которого применяется антивирусное средство.

4.10. Пользователям антивирусных средств запрещается:

- менять настройки или отключать средства антивирусной защиты во время работы;
- использовать средства антивирусной защиты, отличные от установленных средств;
- без разрешения ответственного за обеспечение безопасности ПДн в ИСПДн копировать любые файлы на съемные носители информации, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

5. Порядок и периодичность обновления антивирусных баз

5.1. Своевременное обновление баз данных средств антивирусной защиты информации является неотъемлемой частью обеспечения эффективной политики антивирусной защиты информации.

5.2. Установке обновлений должно предшествовать тестирование ИСПДн на отсутствие негативных воздействий от вновь устанавливаемых обновлений.

5.3. Установке новых версий программного обеспечения или внесению изменений и дополнений в действующее программное обеспечение должно предшествовать тестирование ИСПДн на отсутствие негативных воздействий указанного программного обеспечения.

5.4. Периодичность обновления антивирусных баз:

- обновление антивирусных баз для всех ИСПДн, имеющих подключение к сетям общего пользования и сетям международного информационного обмена, должно быть ежедневным. Источник обновления – сервер разработчика

антивирусного средства, либо собственный централизованный сетевой источник обновлений, получающий обновления с сервера разработчика антивирусного средства.

– обновление антивирусных баз для ИСПДн, не имеющих подключения к сетям общего пользования и сетям международного информационного обмена, обновление должно быть не менее 1 раза в неделю. Источником обновления в данном случае являются антивирусные базы, записанные на предварительно учтенный в установленном порядке съемный машинный носитель информации.

6. Порядок и периодичность проведения антивирусного контроля

6.1. Объектами антивирусного контроля являются:

– жесткие магнитные диски рабочих станций и серверов ИСПДн;
– сетевые хранилища (системы хранения данных);
– оперативная и системная память средств вычислительной техники;
– съемные машинные носители информации;
– входящий и исходящий контент (веб-трафик);
– файлы, получаемые и передаваемые через сети общего пользования и международного информационного обмена;
– почтовые сообщения электронной почты.

6.2. Антивирусный контроль входящей информации со съемных машинных носителей информации необходимо проводить до переноса информации на жёсткий магнитный диск рабочей станции или сетевой диск. Информация, получаемая по телекоммуникационным каналам, должна проверятся во время, или сразу после получения. Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель).

6.3. Виды и периодичность антивирусных проверок представлены в таблице 1.

Таблица 1

№ п/п	Объект контроля	Вид проверки	Периодичность проверки
1	Жесткие магнитные диски рабочих станций и серверов ИСПДн	Полная проверка	1 раз в месяц
		Быстрое сканирование	1 раз в неделю
2	Сетевые хранилища (системы хранения данных)	Полная проверка	1 раз в месяц
3	Оперативная и системная память средств вычислительной техники	Полная проверка	1 раз в месяц
		Быстрое сканирование	1 раз в неделю
4	Съемные машинные носители информации	Полная проверка	При каждом подключении
5	Веб-трафик	Минимально необходимое требование - настройка антивирусного средства по умолчанию	Постоянно
6	Файлы, получаемые и передаваемые через сети общего пользования и международного информационного обмена	Полная проверка	При каждом получении и отправке
7	Почтовые сообщения электронной почты	Минимально необходимое требование - настройка антивирусного средства по умолчанию	При каждом получении и отправке

7. Порядок действий при обнаружении вирусов

7.1. Основными путями проникновения вирусов в ИСПДн являются: любые съемные машинные носители информации, электронные почтовые сообщения, трафик,

получаемый из сетей общего пользования и сетей международного информационного обмена, ранее зараженные рабочие станции и сервера.

7.2. В случае обнаружения вирусов при входном контроле съемных машинных носителей информации, файлов или электронных почтовых сообщений, пользователь должен:

- немедленно приостановить все работы на своей рабочей станции;
- сообщить ответственному за обеспечение безопасности ПДн в ИСПДн о факте обнаружения вируса;
- принять согласованные с ответственным за обеспечение безопасности ПДн в ИСПДн меры по локализации и удалению вируса с использованием антивирусных средств.

7.3. При невозможности ликвидации последствий вирусного заражения ответственному за обеспечение безопасности ПДн в ИСПДн необходимо:

- сообщить о факте обнаружения программных вирусов в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации;
- заархивировать зараженные файлы и направить с приложением соответствующего сопроводительного документа в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации.

7.4. При получении информации о возможном нарушении либо выявлении факта нарушения требований настоящей Инструкции работа на рабочей станции данного пользователя незамедлительно блокируется по решению ответственного за обеспечение безопасности ПДн в ИСПДн.

7.5. Факты модификации и разрушения данных на серверах или рабочих станциях, заражение их вирусами, а также обнаружение других вредоносных программ – все это относится к значимым нарушениям безопасности информации и должны быть проанализированы посредством проведения служебного расследования.

7.6. Служебное расследование проводится комиссией, назначаемой приказом Директора Учреждения. В состав комиссии в обязательном порядке включается администратор ИСПДн, ответственный за обеспечение безопасности ПДн в ИСПДн, непосредственный руководитель работника, допустившего факт компрометации. При необходимости в состав комиссии могут включаться другие сотрудники.

7.7. Результаты работы комиссии оформляются актом. Акт подлежит утверждению Директора Учреждения.

7.8. В процессе работы комиссии обязательными для установления являются:

- дата и время заражения (обнаружения заражения);
- ФИО, должность и подразделение сотрудника, техническое средство которого заражено вирусной программой;
- уровень критичности заражения;
- обстоятельства, способствовавшие заражению;
- информационные ресурсы, затронутые заражением;
- характер и размер реального и потенциального ущерба.

7.9. В ходе своей работы комиссия может запрашивать объяснительные записки от работников, подозреваемых в виновности заражения (путем письменного запроса их

непосредственным руководителям). Объяснительная записка должна быть представлена комиссии в течение 3 (трех) рабочих дней с момента поступления запроса. В случае отказа предоставить объяснительную записку, данный факт отражается в акте.

7.10. Уничтожение материалов расследования фактов заражения осуществляется в соответствии с установленными требованиями по делопроизводству и номенклатурой дел.

8. Ответственность

8.1. Пользователи и Ответственный за обеспечение безопасности ПДн в ИСПДн несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.

9. Срок действия и порядок внесения изменений

9.1. Настоящая Инструкция вступает в силу с момента его утверждения и действует бессрочно.

9.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

9.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом Директора Учреждения.

Приложение 4
к приказу МБУ ДО «ДДТ»
от «09» февраля 2021г. № 06

ПОРЯДОК
обращения со съемными машинными носителями персональных данных в МБУ ДО «ДДТ»

Термины и определения

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Съемный машинный носитель персональных данных – сменный носитель персональных данных, предназначенный для записи и считывания персональных данных, представленных в стандартных кодах.

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.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

1. Общие положения

2.1. Настоящий Порядок обращения со съемными машинными носителями персональных данных в МБУ ДО «ДДТ» (далее – Порядок), разработан в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

2.2. Настоящий Порядок определяет:

- правила обращения со съемными машинными носителями информации, в том числе и ПДн (далее – СМНИ);
- порядок организации учета СМНИ;
- порядок уничтожения СМНИ.

2.3. Под СМНИ в настоящем Порядке понимаются следующие носители информации:

- оптические диски (CD, DVD) однократной и многократной записи;
- электронные накопители информации (флэш-память, съемные жесткие диски);
- иные носители информации.

2.4. Требования настоящего Порядка являются обязательными для исполнения всеми работниками МБУ ДО «ДДТ» (далее – Учреждение), использующими в своей работе СМНИ.

2.5. Все работники Учреждения, использующие СМНИ, должны быть ознакомлены с требованиями настоящим Порядком под подпись.

2.6. Настоящий Порядок является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и ПДн, и не исключает обязательного выполнения их требований.

2. Правила обращения со съемными машинными носителями персональных данных

3.1. Обращение со СМНИ должно осуществляется таким образом, чтобы исключались их утрата, порча и несанкционированный доступ к ним посторонних лиц.

3.2. При обращении со СМНИ, выполняются следующие основные правила:

- СМНИ учитываются и выдаются под подпись;
- СМНИ, срок эксплуатации которых истек, уничтожаются в установленном порядке;
- для выноса СМНИ за пределы контролируемой зоны, запрашивается специальное разрешение у ответственного за обеспечение безопасности ПДн в ИСПДн (далее – Ответственный), а факт выноса фиксируется;
- право на перемещение СМНИ за пределы контролируемой зоны, имеют только те лица, которым оно необходимо для выполнения своих должностных обязанностей (функции);
- все СМНИ должны храниться в сейфах (металлических шкафах), оборудованных приспособленными для опечатывания замочных скважин замками;
- допускается хранение СМНИ вне сейфов (металлических шкафов) при условиях уничтожения (стирания) ПДн и остаточной информации (информации, которую можно восстановить после удаления с помощью нештатных средств и методов) с использованием средств стирания данных и остаточной информации, либо если на съемном машинном носителе ПДн хранятся только ПДн в зашифрованном виде с использованием средств криптографической защиты информации.

3.3. СМНИ должен использоваться не более срока эксплуатации, установленного изготовителем материального носителя.

3. Порядок хранения и учета съемных машинных носителей персональных данных

4.1. СМНИ, должны иметь специальную маркировку. Тип маркировки выбирается Ответственным.

4.2. Все находящиеся на хранении и в обращении СМНИ учитываются Ответственным в «Журнале учета съемных машинных носителей персональных данных в МБУ ДО «ДДТ», форма которого установлена в Приложении 1 к настоящему Порядку.

4.3. В нерабочее время и время отсутствия необходимости использования ПДн СМНИ должны храниться в хранилищах СМНИ.

4.4. Перечень хранилищ определяется в Журнале учета хранилищ носителей персональных данных в МБУ ДО «ДДТ».

4.5. Пользователи для выполнения работ получают СМНИ у Ответственного. При получении делаются соответствующие записи в Журнале учета съемных машинных носителей персональных данных в МБУ ДО «ДДТ».

4. Порядок уничтожения съемных машинных носителей персональных данных

5.1. Уничтожение ПДн производится только в следующих случаях:

- обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным Законом;
- ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
- в случае выявления неправомерной обработки ПДн, если обеспечить правомерность обработки ПДн невозможно;
- в случае достижения цели обработки ПДн;
- в случае отзыва субъектом ПДн согласия на обработку его ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн.

5.2. СМНИ, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению.

5.3. Уничтожение СМНИ осуществляется комиссией по уничтожению, назначенной приказом Директора Учреждения.

5.4. При уничтожении СМНИ необходимо:

- убедиться в необходимости уничтожения СМНИ;
- убедиться в том, что уничтожаются только та информация, которая предназначена для уничтожения;
- уничтожить СМНИ подходящим способом, в соответствии с настоящим Порядком или способом, указанным в соответствующем требовании или распорядительном документе.

5.5. При уничтожении СМНИ применяются следующие способы:

- тщательное измельчение – для документов, исполненных на бумаге;
- тщательное вымарывание (с проверкой тщательности вымарывания) информации, подлежащей уничтожению – для сохранения возможности обработки иных данных, зафиксированных в документе;
- физическое уничтожение (разрушение) носителей информации – для СМНИ на оптических дисках;
- физическое уничтожение частей СМНИ – разрушение или сильная деформация – для носителей информации на жестком магнитном диске (уничтожению подлежат внутренние диски и микросхемы); SSD-дисках, USB- и Flash-носителях (уничтожению подлежат модули и микросхемы долговременной памяти);
- стирание с помощью сертифицированных средств уничтожения информации – для записей в базах данных и отдельных документов на машинном носителе.

5.6. По результатам уничтожения СМНИ комиссией составляется «Акт уничтожения съемных машинных носителей персональных данных», форма которого установлена в Приложении 2 к настоящему Порядку.

5. Ответственность

6.1. Ответственным за хранение, учет и выдачу СМНИ, является Ответственный.

6.2. Все работники Учреждения, использующие СМНИ и Ответственный, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Порядком, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.

6. Срок действия и порядок внесения изменений

7.1. Настоящий Порядок вступает в силу с момента его утверждения и действует бессрочно.

7.2. Настоящий Порядок подлежит пересмотру не реже одного раза в три года.

7.3. Изменения и дополнения в настоящий Порядок вносятся приказом директора Учреждения.

Приложение 1
к порядку обращения со съемными
машинными носителями персональных
данных в МБУ ДО «ДДТ»

ФОРМА

Журнал учета съемных машинных носителей персональных данных
МБУ ДО «ДДТ»

№ п/п	Тип носителя	Номер (серийный/ инвентарный)	Расписка в получении			Подпись ответственного лица	Место хранения	Примечание	Дата и номер акта уничтожения
			ФИО	Дата	Подпись				
1	2	3	4	5	6	7	8	9	10

Приложение 2
к порядку обращения со съемными
машинными носителями персональных
данных в МБУ ДО «ДДТ»

ФОРМА

АКТ

«___» _____ 20__ г. № _____

Об уничтожении съемных машинных носителей персональных данных

Комиссия в составе:
Председатель:
Лаврентьева И.Н., директор МБУ ДО «ДДТ» _____

Члены комиссии:

1. Тимонина М.М., методист МБУ ДО «ДДТ» _____

составила настоящий акт о том, что в результате проведенной экспертной оценки подлежат уничтожению следующие съемные машинные носители персональных данных:

№ п/п	Дата окончания срока обработки зафиксированных на носителе персональных данных	Учетный номер съемного носителя или наименование технического средства, на котором уничтожаются файлы	Примечание
1	2	3	4

Всего съемных носителей_____
(цифрами и прописью)
Перечисленные съемные носители уничтожены путем _____
_____.
(механического уничтожения, сжигания, разрезания, деформирования и т.п.)

Председатель:
_____ _____ _____
Члены комиссии:
_____ _____ _____
_____ _____ _____
_____ _____ _____

ЛИСТ ОЗНАКОМЛЕНИЯ
с приказом МБУ ДО «ДДТ» от «09» февраля 2021 г. № 06
«Об утверждении инструкций по защите персональных данных»

№ п/п	Фамилия имя отчество	Должность	Дата ознакомления	Подпись
1	Лаврентьева И.Н.	директор	«09» 02. 2021 г.	
2	Тимонина М.М.	методист	«09» 02. 2021 г.	
3	Воротникова В.В.	педагог ДО	«09» 02. 2021 г.	
4	Туманова Н.В.	педагог ДО	«09» 02. 2021 г.	