Муниципальное бюджетное образовательное учреждение
дополнительного образования
«Усть-Ишимский Дом детского творчества»

ПРИКАЗ

14.03.2022 г Усть-Ишим № 24

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 МБОУ ДО «Усть-Ишимский ДДТ»,
ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Инструкцию пользователя информационных систем персональных данных МБОУ ДО «Усть-Ишимский ДДТ» ***(Приложение № 1).***
2. Утвердить и ввести в действие Инструкцию по парольной защите информации в МБОУ ДО «Усть-Ишимский ДДТ» ***(Приложение № 2).***
3. Утвердить и ввести в действие Инструкцию по организации антивирусной защиты информации в МБОУ ДО «Усть-Ишимский ДДТ» ***(Приложение № 3).***
4. Требования настоящего приказа довести до работников, осуществляющих обработку персональных данных в информационных системах персональных данных в МБОУ ДО «Усть-Ишимский ДДТ».
5. Контроль за исполнением настоящего Приказа оставляю за собой.

Директор: Зарипова З.А. Зарипова

Приложение № 1
к приказу
МБОУ ДО «Усть-Ишимский ДДТ»
от 14.03.2022 г № 24

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных
МБОУ ДО «Усть-Ишимский ДДТ»

1.1. Инструкция пользователя информационных систем персональных данных МБОУ ДО «Усть-Ишимский ДДТ» (далее - инструкция), разработана в соответствии с Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных»; постановлением Правительства Российской Федерации от 1 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»; постановлением Правительства Российской Федерации от 15 сентября 2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; на основании Устава и локальных нормативных актов МБОУ ДО «Усть-Ишимский ДДТ» (далее - ДДТ).

1.2. В целях реализации настоящей инструкции используются следующие термины и их определения:

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

1.2.2. 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).

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

1.2.4. 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.

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

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

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

1.2.8. 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.

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

1.3. Настоящая инструкция утверждается приказом директора.

1.4. Изменения и дополнения в настоящую инструкцию утверждаются приказом директора.

1.5. Настоящая инструкция является локальным нормативным актом, регламентирующим деятельность ДДТ.

1.6. Срок действия настоящей инструкции не ограничен и действует до принятия новой инструкции.

1.7. Настоящая инструкция подлежит пересмотру не реже одного раза в три года.

2. Общие положения

2.1. Настоящая инструкция определяет обязанности, права и ответственность работников при работе в информационных системах персональных данных (далее - информационные системы).

2.2. Требования настоящей инструкции являются обязательными для всех работников, осуществляющих обработку и защиту персональных данных в информационных системах - пользователей информационных систем (далее - пользователи).

2.3. К защищаемой информации, обрабатываемой в информационных системах ДДТ, относятся персональные данные, служебная (технологическая) информация системы защиты и другая информация ограниченного доступа.

2.4. Все пользователи информационных систем ДДТ должны быть ознакомлены с требованиями 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 персональных данных, и не исключает обязательного выполнения их требований.

3. Допуск пользователей к информационным системам персональных данных

3.1. Допуск пользователей к работе с персональными данными в информационных системах осуществляется в соответствии с «Перечнем должностей работников ДДТ», допущенных к обработке персональных данных».

3.2. К самостоятельной работе на автоматизированных рабочих местах (далее - АРМ), входящих в состав информационных систем, 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 информационных систем, 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 информационных систем.

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

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

4.1.4. Немедленно ставить в известность ответственного за обеспечение безопасности персональных данных в информационных системах или администратора:

– при подозрении компрометации личного пароля;

– несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств информационных систем;

– отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию информационных систем;

– некорректного функционирования установленных средств защиты;

-обнаружения непредусмотренных отводов кабелей и подключенных устройств;

– обнаружения фактов, попыток несанкционированного доступа и случаев нарушения установленного порядка обработки персональных данных.

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

4.2. Пользователям информационных систем запрещается:

– отключать (блокировать) средства защиты информации, предусмотренныеорганизационно-распорядительными документами в информационных системах;

– 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 информационных системах информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу;

– сообщать (или передавать) посторонним лицам личные атрибуты и пороли доступа к ресурсам иных информационных систем;

– работать в информационных системах при обнаружении каких-либо неисправностей;

– оставлять включенным без присмотра АРМ, не активизировав средства защиты от несанкционированного доступа;

– умышлено использовать недокументированные свойства и ошибки в программном обеспечении или 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 персональных данных в информационных системах;

– вскрывать корпуса технических средств АРМ и вносить изменения в схему и конструкцию устройств.

5. Организация парольной защиты

5.1. Организация парольной защиты производится в соответствии с «Инструкцией по паролной защите информации в ДДТ».

5.2. Лица, использующие пароли, обязаны:

– хранить в тайне пароль;

– четко знать и строго выполнять требования настоящей инструкции и другихруководящих документов;

– своевременно сообщать ответственному за обеспечение безопасности персональных данных в информационных системах обо всех нештатных ситуациях, нарушениях работы систем защиты от несанкционированного доступа, возникающих при работе с паролями.

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

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

5.5. Блокирование сеанса доступа пользователя в информационные системы осуществляется после 15 минут его бездействия (неактивности).

5.6. В случае утери пароля работник ставит в известность своего непосредственного руководителя и ответственного за обеспечение безопасности персональных данных в информационных системах для принятия последующих решений.

5.7. В случае компрометации пароля (просмотр посторонними, разглашение пароля и др.) необходимо известить своего непосредственного руководителя и ответственного за обеспечение безопасности персональных данных в информационных системах для принятия последующих решений.

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

6.1. Работа в сетях общего доступа и на элементах информационных систем, должна осуществляться исключительно в служебных целях.

6.2. 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.

7. Порядок установки обновлений программного обеспечения

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

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

7.3. 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.

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

системах.

8. Технология обработки персональных данных

8.1. При первичном допуске к работе в информационных системах 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 персональных данных в информационных системах.

8.2. В процессе работы пользователь производит обработку персональных данных в информационных системах.

Приложение № 2
к приказу
МБОУ ДО «Усть-Ишимский ДДТ»
от 14.03.2022 г. № 24

ИНСТРУКЦИЯ
по парольной защите информации
в МБОУ ДО «Усть-Ишимский ДДТ»

1.1. Инструкция по парольной защите информации МБОУ ДО «Усть-Ишимский ДДТ» (далее - инструкция), разработана в соответствии с Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных»; постановлением Правительства Российской Федерации от 1 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»; постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; на основании Устава и локальных нормативных актов МБОУ ДО «Усть-Ишимский ДДТ» (далее - ДДТ).

1.2. В целях реализации настоящей инструкции используются следующие термины и их определения:

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

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

1.2.3. 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.

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

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

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

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

1.3. Настоящая инструкция утверждается приказом директора.

1.4. Изменения и дополнения в настоящую инструкцию утверждаются приказом директора.

1.5. Настоящая инструкция является локальным нормативным актом, регламентирующим деятельность Центра.

1.6. Срок действия настоящей инструкции не ограничен и действует до принятия новой инструкции.

1.7. Настоящая инструкция подлежит пересмотру не реже одного раза в три года.

2.Общие положения

2.1. Настоящая инструкция устанавливает требования иответственность при организации парольной защиты информации, а также определяет порядок контроля за действиями пользователей и обслуживающего персонала информационных систем персональных данных при работе с паролями.

2.2. Требования настоящей Инструкции являются обязательными для исполнения всеми пользователями и администраторами информационных систем персональных данных, использующими в своей работе средства вычислительной техники.

2.3. Все пользователи и администраторы информационных систем персональных данных ДДТ, 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, 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 информационных систем персональных данных 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 за обеспечение безопасности персональных данных в информационных системах или администратором, 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 пароле обязательно должны присутствовать как цифры, так и буквы на верхнем и нижнем регистрах;

– 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 информационных систем персональных данных.

3.2.6. Хранение пользователями информационных систем персональных данных значений 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 информационных систем персональных данных при наличии технологической необходимости использования имен и паролей работников в их отсутствие в случае возникновения нештатных 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 течение 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 обязан представить администратору информационных систем персональных данных 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 персональных данных в информационных системах или администратору.

3.4.3. В случае выявления факта компрометации идентификаторов и паролей пользователя администратор или ответственный за обеспечение безопасности персональных данных в информационных системах 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 информационных систем персональных данных:

организация установки средств идентификации и аутентификации;

– организация парольной защиты;

– выдача первичных паролей, и электронных персональных идентификаторов и паролей к ним;

– осуществление контроля за состоянием системы парольной защиты информации.

4.2. Администратор информационных систем персональных данных имеет право:

– вносить предложения по совершенствованию системы парольной защиты информации;

– принимать участие в планировании мероприятий по парольной защите информации

и планировании оснащения средствами идентификации и аутентификации;

– осуществлять контроль состояния средств идентификации и аутентификации;

– 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 информационных систем персональных данных.

4.4. Пользователям информационных систем персональных данных 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 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 персональных данных в информационных системах или администратора.

5. Ответственность должностных лиц в рамках системы парольной защиты информации

5.1. Пользователи, ответственный за обеспечение безопасности персональных данных в информационных системах и администратор 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 персональных данных в информационных системах и администратор несут ответственность по действующему законодательству Российской Федерации за разглашение сведений конфиденциального характера, ставших известными при выполнении служебных обязанностей, в том числе предусмотренных настоящей инструкцией.

Приложение № 3
к приказу
МБОУ ДО «Усть-Ишимский ДДТ»
от 14.03.2022 г № 24

ИНСТРУКЦИЯ
по антивирусной защитеМБОУ ДО «Усть-Ишимский ДДТ»

1.1. Инструкция по антивирусной защите МБОУДО «Усть-Ишимский ДДТ» (далее - инструкция), разработана в соответствии с Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных»; постановлением Правительства Российской Федерации от 1 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»; постановлением Правительства Российской Федерации от 15 сентября 2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; на основании Устава и локальных нормативных актов МБОУ ДО «Усть-Ишимский ДДТ» (далее - ДДТ).

1.2. В целях реализации настоящей инструкции используются следующие термины и их определения:

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

1.2.2. 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).

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

1.2.4. 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.

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

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

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

1.2.8. 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.

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

1.3. Настоящая инструкция утверждается приказом директора.

1.4. Изменения и дополнения в настоящую инструкцию утверждаются приказом директора.

1.5. Настоящая инструкция является локальным нормативным актом, регламентирующим деятельность ДДТ.

1.6. Срок действия настоящей инструкции не ограничен и действует до принятия новой инструкции.

1.7. Настоящая инструкция подлежит пересмотру не реже одного раза в три года.

2.Общие положения

2.1. Настоящая Инструкция по антивирусной защите ДДТ 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 ДДТ, использующими в своей работе средства вычислительной техники.

2.4. Все работники ДДТ, использующие антивирусные средства, должны быть ознакомлены с требованиями 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 персональных данных, и не исключает обязательного выполнения их требований.

3.Требования к антивирусным средствам

3.1. В ДДТ 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.

4. Права и обязанности

4.1. Антивирусной защите подлежит вся, обрабатываемая в ДДТ 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 информационных системах персональных данных 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 персональных данных в информационной системе.

4.6. Основные задачи ответственного за обеспечение безопасности персональных данных в информационных системах:

– организация процесса установки антивирусных средств;

– сопровождение антивирусных средств (обновление, антивирусный контроль, сопровождение действий пользователей в случаях обнаружения вирусов, обеспечение работоспособности антивирусных средств);

– контроль состояния системы антивирусной защиты информации в ДДТ.

4.7. Ответственный за обеспечение безопасности персональных данных в информационных системах 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 персональных данных в информационных системах 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 ДДТ;

– инициировать служебные проверки и участвовать в проведении расследований по фактам заражения вирусами 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 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 информационных систем персональных данных 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 информационных систем персональных данных на отсутствие негативных воздействий указанного программного обеспечения.

5.4. Периодичность обновления антивирусных баз:

– - обновление антивирусных баз для всех информационных систем персональных данных, 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 информационных систем персональных данных, не имеющих подключение 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 информационных систем персональных данных;

– 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 вовремя, 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	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 информационные системы персональных данных 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 о факте обнаружения вируса;

– принять согласованные с ответственным за обеспечение безопасности меры по локализации и удалению вируса с использованием антивирусных средств.

7.3. При невозможности ликвидации последствий вирусного заражения ответственному за обеспечение безопасности 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 персональных данных в информационных системах.

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 ДДТ. В состав комиссии в обязательном порядке включается администратор, ответственный за обеспечение безопасности, непосредственный руководитель работника, допустившего факт компрометации. При необходимости в состав комиссии могут включаться другие работники.

7.7. Результаты работы комиссии оформляются актом. Акт подлежит утверждению директором ДДТ.

7.8. В процессе работы комиссии обязательными для установления являются:

– дата и время заражения (обнаружения заражения);

– ФИО, должность работника, 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 персональных данных в информационных системах 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.