Приложение 1
к приказу
от «28» 12.2023 г. № 64

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных МБУ ДО «ДЮСШ» МО Черноморский район РК

7. Термины и определения

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

1.2. 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).

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

1.4. 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.

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

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

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

1.8. 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.

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

8. Общие положения

4.1.1. Настоящая Инструкция пользователя информационных систем персональных

данных МБОУ «ЧСШ №1 им. Н.Кудри», (далее – Инструкция) определяет обязанности, права и ответственность работников при работе в информационных системах персональных данных (далее – ИСПДн).

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

4.1.3. К защищаемой информации, обрабатываемой в ИСПДн МБОУ «ЧСШ №1 им. Н.Кудри», (далее – Учреждение), относятся ПДн, служебная (технологическая) информация системы защиты и другая информация ограниченного доступа.

4.1.4. Все пользователи ИСПДн Учреждения должны быть ознакомлены с требованиями настоящей Инструкции под подпись.

4.1.5. 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.

9. Допуск пользователей к информационным системам персональных данных

5.1. Допуск пользователей к работе с ПДн в ИСПДн осуществляется в соответствии с «Перечнем должностей работников **МБУ ДО «ДЮСШ» МО Черноморский район РК** ,допущенных к обработке персональных данных».

5.2. 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.

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

10. Обязанности пользователя

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

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

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

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

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

8.1. при подозрении компрометации личного пароля;

8.2. несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;

8.3. отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ИСПДн;

8.4. некорректного функционирования установленных средств защиты;

8.5. обнаружения непредусмотренных отводов кабелей и подключенных устройств;

8.6. обнаружения фактов, попыток несанкционированного доступа и случаев нарушения установленного порядка обработки ПДн.

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

6.2. Пользователям ИСПДн запрещается:

8.7. отключать (блокировать) средства защиты информации, предусмотренные организационно-распорядительными документами на ИСПДн;

8.8. производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;

8.9. самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

8.10. обрабатывать в ИСПДн информацию и выполнять другие работы, не предусмотренные перечнем прав Пользователя по доступу к ИСПДн;

8.11. сообщать (или передавать) посторонним лицам личные атрибуты и пароли доступа к ресурсам ИСПДн;

8.12. работать в ИСПДн при обнаружении каких-либо неисправностей;

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

8.14. умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к ознакомлению с защищаемой информацией посторонних лиц;

8.15. производить перемещения технических средств АРМ без согласования с ответственным за обеспечение безопасности ПДн в ИСПДн;

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

11. Организация работы со съемными машинными носителями информации

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 МБОУ «ЧСШ №1 им. Н.Кудри»,».

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

3. СМНИ должны быть зарегистрированы в «Журнале учета съемных машинных носителей информации».

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

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.

6. Хранение СМНИ осуществляется:

8.17. для флеш-карт, смарт-карт, компакт дисков и др.) в защищенных сейфах;

8.18. для СМНИ, входящих в состав ИСПДн, производится опечатывание корпуса АРМ.

7. Пользователям запрещается:

8.19. записывать и хранить ПДн и иную информацию конфиденциального характера на неучтенных СМНИ;

8.20. оставлять СМНИ без присмотра, передавать их другим лицам и выносить за пределы контролируемой зоны, за исключением случаев, в которых разрешена передача СМНИ;

8.21. хранить СМНИ вблизи сильных источников электромагнитных излучений и прямых солнечных лучей;

8.22. хранить на учтенных СМНИ программы и данные, не относящиеся к рабочей информации.

12. Организация парольной защиты

7.1. Организация парольной защиты производится в соответствии с «Инструкцией по парольной защите информации в **МБУ ДО «ДЮСШ» МО Черноморский район РК** .

7.2. Лица, использующие пароли, обязаны:

8.23. хранить в тайне свой пароль

8.24. четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов;

8.25. 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.

7.3. 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.)

7.4. 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.

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

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

7.7. 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.

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

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

– При работе в сетях общего доступа запрещается:

8.26. осуществлять работу при отключенных средствах защиты;

8.27. передавать по сетям общего доступа защищаемую информацию без использования средств шифрования;

8.28. запрещается скачивать из сети Интернет программное обеспечение и другие файлы. если это не определено его должностными обязанностями;

8.29. запрещается посещение и использование сети Интернет в личных целях.

14. Порядок установки обновлений программного обеспечения

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

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

3.3. 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.

3.4. 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.

15. Технология обработки персональных данных

– 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.

– В процессе работы Пользователь производит обработку ПДн в ИСПДн.

– При необходимости вывод ПДн из ИСПДн осуществляется следующим образом:

8.30. копированием ПДн на учтенные СМНИ;

8.31. передача ПДн по каналам связи с обязательным применением криптографической защиты.

16. Срок действия и порядок внесения изменений

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

1.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в

три года.

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