

## **ИНСТРУКЦИЯ** **пользователя информационных систем персональных данных** **МБУ ДО «ЦДОД»**

### **1. 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.

### **2. Общие положения**

- 2.1. Настоящая Инструкция пользователя информационных систем персональных данных МБУ ДО «ЦДОД» (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 «ЦДОД» (далее – Учреждение), относятся ПДн, служебная (технологическая) информация системы защиты и другая информация ограниченного доступа.
- 2.4. Все пользователи ИСПДн Учреждения 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 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 «Перечнем должностей работников МБУ ДО «ЦДОД», допущенных к обработке персональных данных».
- 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 «ЦДОД»».
- 5.2. Пользователи обязаны знать и соблюдать установленные требования по учету и хранению СМНИ.
- 5.3. СМНИ должны быть зарегистрированы 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 «ЦДОД»».
- 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 отраженном 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 работник 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.

