Приложение № 10

УТВЕРЖДЕНО

Приказом ГКУ НСО ЦСПН

Ордынского района

от 03.02.2020 №13/1

**Инструкция пользователя информационных систем государственного казенного учреждения Новосибирской области «Центр социальной поддержки населения Ордынского района»**

1. **Общие положения**
   1. Инструкция пользователя информационных систем (далее ­ ИС) государственного казенного учреждения Новосибирской области «Центр социальной поддержки населения Ордынского района» (далее – учреждение) определяет функциональные обязанности, права и ответственность пользователей информационных систем учреждения, в которых обрабатывается информация ограниченного доступа (в том числе персональных данных), не содержащая сведения, составляющие государственную тайну (далее – ПДн, информация).
   2. Пользователями ИС учреждения являются уполномоченные сотрудники учреждения, включенные в Перечень лиц, осуществляющих обработку персональных данных либо имеющих доступ к персональным данным, и (или) доступ в помещения и сооружения, в которых ведется обработка персональных данных и размещены информационные системы учреждения.
   3. Настоящая Инструкция подготовлена в соответствии с требованиями нормативно-методических документов Федеральной службы по техническому и экспортному контролю (ФСТЭК России) и Федеральной службы безопасности Российской Федерации (ФСБ России) по защите информации, обрабатываемой с использованием средств автоматизации.
   4. Пользователь ИС учреждения в своей работе руководствуется настоящей Инструкцией, нормативными правовыми актами и методическими документами ФСТЭК России, ФСБ России и внутренними документами учреждения, регламентирующими вопросы обработки и защиты информации.
   5. В настоящей Инструкции используются следующие понятия и определения:
      1. Автоматизированное рабочее место (АРМ) – объект вычислительной техники, созданный на базе автономных средств вычислительной техники с необходимым для решения конкретных задач периферийным оборудованием.
      2. Компрометация пароля – утрата доверия к тому, что используемый пароль обеспечивает безопасность ПДн. К событиям, приводящим к компрометации пароля, относятся следующие события (включая, но не ограничиваясь) – несанкционированное сообщение пароля другому лицу; утеря бумажного или машинного носителя информации, на котором был записан пароль; запись пароля на бумажном, машинном, ином носителе информации, доступ к которому не контролируется.
      3. Конфиденциальность информации – обязательное для соблюдения лицом, получившим доступ к информации, требование не допускать ее распространение без наличия иного законного основания.
      4. Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.
      5. Несанкционированный доступ к информации – доступ к информации с нарушением установленных прав доступа, приводящий к нарушению конфиденциальности персональных данных, к утечке, искажению, подделке, уничтожению, блокированию доступа к информации.
      6. Средство защиты информации (СЗИ) – программные, программно-аппаратные, аппаратные средства, предназначенные и используемые для защиты информации в информационных системах.
      7. Пользователь информационной системы – лицо, участвующее в функционировании информационной системы или использующее результаты ее функционирования.
      8. Утеря пароля – события, приводящие к невозможности восстановления пароля в памяти лица, владеющего данным паролем.
      9. Электронная вычислительная машина (ЭВМ) – персональный компьютер, предназначенный для автоматизации деятельности пользователей и входящий в состав информационной системы. В состав ЭВМ входят: системный блок, монитор, клавиатура, мышь, внешние устройства (локальный принтер, сканер и т.д.), программное обеспечение.
2. **Обязанности пользователя**
   1. Пользователь ИС учреждения обязан:
      1. Знать и выполнять требования:

* настоящей Инструкции;
* положений локальных актов учреждения;
* нормативных правовых актов действующего законодательства Российской Федерации в области обработки и защиты информации.
  + 1. Хранить в тайне информацию, ставшую ему известной во время работы или иным путем, и пресекать действия других лиц, которые могут привести к разглашению информации. О таких фактах, а также о других причинах или условиях возможной утечки информации немедленно информировать ответственного за защиту информации.
    2. Выполнять при работе в ИС только те процедуры, которые необходимы для исполнения его должностных обязанностей.
    3. Использовать для выполнения должностных обязанностей только предоставленное ему автоматизированное рабочее место на базе персонального компьютера.
    4. Располагать средства отображения (монитор (экран) АРМ, принтер/многофункциональное устройство и т.п.), используемые для работы с информацией, таким образом, чтобы исключалась возможность визуального просмотра выводимой информации посторонними лицами. Осуществлять вывод на печать обрабатываемой информации исключительно в целях исполнения должностных обязанностей.
    5. Использовать для хранения и передачи защищаемой информации только зарегистрированные в установленном порядке съемные (отчуждаемые) машинные носители информации.
    6. Обеспечивать безопасное хранение вышеуказанных материальных носителей информации, исключающее несанкционированный доступ к ним.
    7. Перед началом обработки в ИС файлов, полученных из внешних источников (съемных машинных носителей информации, загруженных из сетей общего пользования и других внешних источников), осуществлять проверку файлов на наличие компьютерных вирусов.
    8. Соблюдать конфиденциальность информации, ставшей ему известной во время выполнения служебных (трудовых) обязанностей или иным путем, не предоставлять третьим лицам и не распространять информацию без согласия субъекта ПДн, если иное не предусмотрено федеральным законом; пресекать действия других лиц, которые могут привести к нарушению конфиденциальности информации.
    9. Для предотвращения несанкционированного доступа к защищаемой информации осуществлять блокировку рабочей станции, на которой производится обработка информации, по окончании сеанса работы или во время перерыва в работе (при отсутствии визуального контроля за рабочей станцией).
    10. Соблюдать правила при работе в сетях связи общего пользования, в том числе сетях международного информационного обмена (сети «Интернет») (далее – сеть):
* запрещается передавать по сети информацию без использования средств криптографической защиты информации;
* запрещается осуществлять нецелевое использование сети в корыстных и/или преступных целях.
  + 1. Знать и выполнять правила работы со средствами защиты информации, используемыми в ИС, в соответствии с технической и эксплуатационной документацией к ним.
    2. Хранить в тайне персональные пароли доступа в ИС учреждения, а также информацию о системе защиты ИС, реализованной в учреждении.
    3. Обеспечивать процессы генерации, использования и смены личного пароля с учетом следующих требований:
* длина пароля должна быть не менее восьми 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 в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения;
* при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.
  + 1. Немедленно ставить в известность ответственных лиц в пределах их компетенции (ответственного за защиту информации в учреждении) в случае:
* утраты носителя с информацией и/или при подозрении компрометации паролей доступа;
* возникновения нештатных ситуаций, фактах, попытках, причинах или условиях несанкционированного доступа к обрабатываемой информации, о блокировании, исчезновении (искажении) защищаемой информации;
* нарушения целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения попыток несанкционированного доступа к ИС учреждения;
* несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСучреждения.
  + 1. В случае выявления отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), некорректного функционирования установленных в ИС учреждения программно-аппаратных средств защиты информации ставить в известность ответственного за защиту информации в учреждении.
    2. В случае выявления инцидента информационной безопасности, при возникновении нештатных и аварийных ситуаций принимать меры по реагированию с целью ликвидации их последствий, в пределах своих полномочий, оказывать содействие при проведении работ по восстановлению работоспособности программных и программно-аппаратных средств ИС.
    3. В случае увольнения вернуть все документы и материалы на бумажных и машинных носителях информации, программные и программно-аппаратные средства (в том числе средства защиты информации), относящиеся к ИС учреждения, в том числе: отчеты, инструкции, служебную переписку, списки сотрудников, программные и программно-аппаратные средства, а также все прочие материалы и копии названных материалов, полученные в течение срока работы в учреждении.
    4. Соблюдать установленный Порядок доступа в помещения учреждения, в которых ведется обработка персональных данных и размещены информационные учреждения, контролировать действия лиц, не включенных в Перечень лиц, осуществляющих обработку персональных данных либо имеющих доступ к персональным данным, и (или) доступ в помещения и сооружения, в которых ведется обработка персональных данных и размещены информационные системы учреждения.
  1. Пользователю категорически запрещается:
* передавать кому бы то ни было, устно или письменно, информацию, а также атрибуты доступа к ресурсам ИС учреждения, открыто осуществлять ввод персонального пароля в присутствии других лиц;
* использовать защищаемую информацию при подготовке открытых публикаций, докладов, научных работ и т.д. (в случае отсутствия согласия субъекта ПДн или иных законных оснований);
* выполнять работы с документами, содержащими защищаемую информацию, за пределами служебных помещений, выносить их из служебных помещений, снимать копии с документов и других носителей информации или производить выписки из таких документов без разрешения ответственного за организацию обработки персональных данных и/или ответственного за защиту информации в учреждении, равно как использовать различные технические средства (фото-, видео- и звукозаписывающую аппаратуру) для фиксации сведений, содержащих защищаемую информацию, в целях, не относящихся к исполнению служебных обязанностей;
* оставлять без присмотра на рабочих столах, в столах и незапертых сейфах/металлических шкафах/персональных хранилищах документы, содержащие защищаемую информацию, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и иные хранилища с документами, содержащими защищаемую информацию;
* использовать компоненты программного и аппаратного обеспечения ИС учреждения в неслужебных целях;
* самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АРМ или устанавливать программные и аппаратные средства (в том числе отключать (блокировать) средства защиты информации);
* самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств (в том числе отключать (блокировать) средства защиты информации);
* осуществлять обработку информации в присутствии посторонних (не допущенных к данной информации) лиц;
* оставлять рабочее место, не активизировав средства защиты информации от НСД (временную блокировку сеанса доступа);
* подключать к АРМ и локальной вычислительной сети личные съемные носители информации и прочие мобильные технические средства;
* записывать и хранить информацию на неучтенных носителях информации;
* хранить на учтенных носителях информации данные, не относящиеся к выполнению служебных (должностных) обязанностей;
* привлекать посторонних лиц для проведения ремонта или настройки программно-аппаратных средств ИС учреждения, не уполномоченных на осуществление указанных действий в соответствии с заключенными соглашениями, договорами, контрактами;
* умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению инцидента информационной безопасности. При обнаружении такого рода ошибок – ставить в известность ответственного за защиту информации;
* выносить без согласования с ответственным за защиту информации в учреждениитехнические средства ИС учреждения, с использованием которых проводилась или проводится обработка информации, за пределы контролируемой зоны.

1. **Права пользователя**
   1. Пользователь имеет право:
      1. Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения своих функциональных обязанностей.
      2. Получать доступ к информации, материалам, техническим средствам, помещениям, необходимых для надлежащего исполнения своих обязанностей.
      3. Проходить обучение (переподготовку) по защите информации в специализированных учебных центрах.
      4. Вносить своему непосредственному руководителю предложения, касающиеся организации технологического процесса обработки и защиты информации.
      5. Для получения консультаций по вопросам обработки информации обращаться к ответственному за организацию обработки персональных данных учреждения.
      6. Для получения консультаций по вопросам информационной безопасности и использованию средств защиты информации обращаться к ответственному за защиту информации в учреждения
2. **Ответственность пользователя**
   1. Пользователь несет предусмотренную законодательством Российской Федерации в соответствии с возложенными на него обязанностями ответственность за:

* неисполнение либо ненадлежащее исполнение должностных обязанностей;
* нарушения в работе ИС учреждения, вызванные его неправомерными действиями или неправильным использованием предоставленных прав, предусмотренных настоящей Инструкцией;
* нарушение законодательства Российской Федерации, локальных актов учреждения в сфере обработки и обеспечения безопасности информации;
* превышение должностных полномочий и злоупотребление ими;
* применение к учреждению штрафных санкций по вине пользователя;
* совершение противоправных действий (уничтожение, изменение, блокирование, копирование, предоставление, распространение, а также иных неправомерных действий) в отношении информации, к которой он допущен в рамках выполнения своих должностных (функциональных) обязанностей.