Приложение № 9

УТВЕРЖДЕНО

Приказом ГКУ НСО ЦСПН

Ордынского района

от 03.02.2020 №13/1

**ИНСТРУКЦИЯ**

**ответственного за защиту информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, содержащейся в информационных системах**

**государственного казенного учреждения Новосибирской области «Центр социальной поддержки населения Ордынского района»**

1. **Общие положения**

Настоящая Инструкция определяет основные права и обязанности ответственного за защиту информации ограниченного доступа (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну (далее – информация), содержащейся в информационных системах государственного казенного учреждения Новосибирской области «Центр социальной поддержки населения Ордынского района» (далее – Учреждение).

* 1. Ответственный за защиту информации, содержащейся в информационных системах Учреждения (далее – ответственный за защиту информации), назначается приказом директора Учреждения из числа сотрудников Учреждения.
  2. Ответственный за защиту информации получает указания непосредственно от директора Учреждения или иного уполномоченного лица и подотчетно ему.
  3. Ответственный за защиту информации отвечает за организацию и обеспечение выполнения требований по защите информации, в процессе ее обработки в информационных системах Учреждения.
  4. Ответственный за защиту информации в своей работе руководствуется настоящей Инструкцией, нормативными правовыми актами Российской Федерации, нормативными правовыми актами, методическими и иными документами Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России), Федеральной службы безопасности Российской Федерации (далее – ФСБ России) и локальными актами Учреждения, регламентирующими вопросы обработки и защиты информации.

1. **Обязанности ответственного за защиту информации**
   1. Ответственный за защиту информации обязан:
      1. Знать и соблюдать требования действующих нормативных правовых актов Российской Федерации, нормативных правовых актов, методических и иных документов ФСТЭК России, ФСБ России, а также локальных актов ГКУ НСО ЦСПН Ордынского района, регламентирующих вопросы в сфере (области) обеспечения безопасности информации.
      2. Осуществлять планирование мероприятий по защите информации, обрабатываемой в информационных системах (далее – ИС) Учреждения, осуществлять пересмотр и корректировку (при необходимости) плана мероприятий по защите информации в ИС Учреждения.
      3. Обеспечивать информирование пользователей ИС о появлении актуальных угроз безопасности информации, о правилах безопасной эксплуатации ИС.
      4. Обеспечивать доведение до пользователей ИС Учреждения требований по защите информации, а также положений организационно-распорядительных документов по защите информации с учетом внесенных в них изменений.
      5. Организовывать обучение пользователей ИС Учреждения правилам безопасной эксплуатации ИС не реже 1 раза в два года.
      6. Осуществлять контроль осведомленности пользователей ИС ГКУ НСО ЦСПН Ордынского района об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации с периодичностью не реже 1 раза в два года.
      7. Осуществлять контроль выполнения пользователями ИС Учреждения требований Инструкции пользователя информационных систем Учреждения.
      8. Обеспечивать проведение контроля за обеспечением уровня защищенности информации, содержащейся в ИС Учреждения, с периодичностью не реже 1 раза в два года.
      9. Осуществлять мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа ИС.
      10. Обеспечивать контроль состава применяемых в ИС Учреждения средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков.
      11. Осуществлять контроль выполнения условий и сроков действия сертификатов соответствия на применяемые в Учреждении средства защиты информации (далее – СЗИ) и принятие мер, направленных на устранение выявленных недостатков.
      12. Обеспечивать учет и сохранность применяемых СЗИ, эксплуатационной и технической документации к ним, порядок обращения с СЗИ, направленный на исключение несанкционированного доступа к СЗИ.
      13. Обеспечивать контроль работоспособности, параметров настройки и правильности функционирования СЗИ.
      14. Обеспечивать ведение документации в области защиты информации, предусмотренной локальными актами Учреждения.
      15. Сообщать обо всех зафиксированных попытках посторонних лиц получить несанкционированный доступ к защищаемой информации и техническим средствам ИС Учреждения, и иных инцидентах информационной безопасности своему непосредственному руководителю или иному уполномоченному лицу в зависимости от характера инцидента.
      16. Обеспечивать обнаружение инцидентов информационной безопасности и реагирование на них.
      17. Принимать участие в расследовании нарушений по вопросам защиты информации (в том числе выявлении инцидентов), принимать меры по их устранению и предупреждению подобного рода нарушений.
      18. В случае возникновения нештатных и аварийных ситуаций, а также при выявлении нарушений, приводящих к снижению уровня защищенности информации, принимать меры по реагированию в пределах своих полномочий с целью предупреждения и ликвидации неблагоприятных последствий, известить своего непосредственного руководителя и ответственных лиц, исходя из характера возникшего инцидента.
      19. Участвовать в мероприятиях при проведении государственного контроля и надзора за соответствием обработки персональных данных, выполнением организационных и технических мер по обеспечению безопасности информации в Учреждении.
      20. Осуществлять в пределах своей компетенции иные функции в соответствии с целями и задачами Учреждения.
2. **Права ответственного за защиту информации**
   1. Ответственный за защиту информации имеет право:
      1. Знакомиться в установленном порядке с документами и материалами, необходимыми для выполнения возложенных на него задач.
      2. Проходить обучение (переподготовку) по защите информации в специализированных учебных центрах.
      3. Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения своих обязанностей.
      4. Получать доступ к информации, материалам, техническим средствам, помещениям, необходимый для надлежащего исполнения своих прав и обязанностей.
      5. Требовать от сотрудников Учреждения соблюдения требований действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности информации, локальных актов Учреждения по вопросам обработки информации и требований по защите информации в части их касающейся.
      6. Проводить проверки соблюдения режима обеспечения безопасности информации в Учреждении.
      7. Инициировать проведение и принимать участие в служебных расследованиях по фактам нарушения сотрудниками Учреждения установленных требований обработки и защиты информации.
      8. Требовать прекращения обработки информации в случае нарушения правил обработки и требований по защите информации.
      9. Привлекать в случае необходимости при проведении служебных расследований сотрудников Учреждения, имеющих непосредственное отношение к рассматриваемым в ходе служебного расследования вопросам.
      10. Вносить предложения об отстранении от выполнения служебных обязанностей сотрудников, систематически нарушающих требования по защите информации.
3. **Ответственность**
   1. Ответственный за защиту информации, содержащейся в Учреждении, несет предусмотренную законодательством Российской Федерации в соответствии с возложенными на него обязанностями ответственность за:

* неисполнение либо ненадлежащее исполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией;
* нарушения в работе ИС Учреждения, вызванные его неправомерными действиями или неправильным использованием предоставленных прав;
* нарушение законодательства Российской Федерации, локальных актов Учреждения в области защиты информации;
* превышение должностных полномочий и злоупотребление ими;
* применение к Учреждению штрафных санкций по вине ответственного за защиту информации;
* 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.