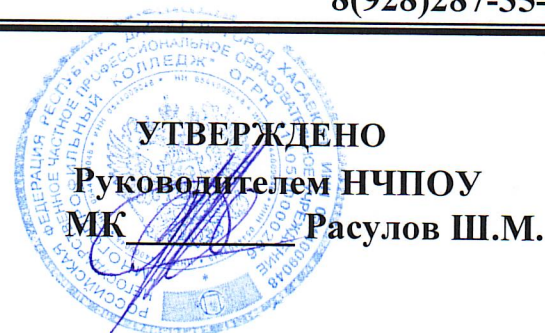


**Негосударственное частное профессиональное образовательное
учреждение
«Многопрофильный колледж»**
**Лицензия №7744 от 28 октября 2014 года серия 05Л01№0002103,
свидетельство о государственной аккредитации №6632 от 24 мая 2017
года, серия 05А01 №0001547.**
г. Хасавюрт, ул.Батырмурзаева,127

8(928)287-35-97

СОГЛАСОВАНО

**Управляющим советом
Протокол № 3 от 30.08.2024 г**



ответственного за обеспечение безопасности персональных данных
информационных систем персональных данных в НЧПОУ МК

1. Общие положения

- 1.1. Настоящая инструкция (далее – Инструкция) определяет общие функции, ответственность, права и обязанности ответственного за обеспечение безопасности персональных данных информационных систем персональных данных (ИСПДн) (далее – Ответственный) в НЧПОУ МК (далее – Колледж).
- 1.2. Настоящая инструкция разработана в соответствии с руководящими и нормативными документами регуляторов Российской Федерации в области защиты персональных данных.
- 1.3. Ответственный назначается приказом директора на основании «Положения о разграничении прав доступа к обрабатываемым персональным данным в НЧПОУ МК из числа штатных сотрудников и студентов» или сторонней организации, осуществляющей сопровождение ИСПДн по договору подряда.
- 1.4. Ответственный подчиняется непосредственно Директору колледжа.
- 1.5. На время отсутствия Ответственного (отпуск, болезнь, пр.) его обязанности исполняет лицо, назначенное в установленном порядке, которое приобретает соответствующие права и несет ответственность за надлежащее исполнение возложенных на него обязанностей.
- 1.6. Ответственный в своей работе руководствуется настоящей Инструкцией, Концепцией информационной безопасности, Политикой информационной безопасности, другими регламентирующими документами, руководящими и нормативными документами регуляторов РФ в области обеспечения безопасности персональных данных.
- 1.7. Методическое руководство работой Ответственного осуществляется ответственным за организацию обработки персональных данных в колледже.
- 1.8. Ответственный является ответственным лицом, уполномоченным на проведение работ по технической защите информации и поддержанию необходимого уровня защищенности ИСПДн колледжа и их ресурсов на этапах промышленной эксплуатации и модернизации.

2. Организация работы

2.1. Ответственный должен иметь специальное рабочее место, размещённое на территории контролируемой зоны, установленной приказом директора _ «Об определении границ контролируемой зоны и требований к ее безопасности», таким образом, чтобы исключить несанкционированный доступ к нему посторонних лиц и других сотрудников колледжа.

2.2. Рабочее место Ответственного должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое), подключением к ИСПДн, а так же средствами контроля технических средств защиты информации (далее – СЗИ).

3. Обязанности

Ответственный должен:

3.1. Соблюдать требования законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, «Правил обработки персональных данных» и других нормативных документов колледжа в области обработки и защиты персональных данных.

3.2. Поддерживать необходимый уровень защищенности (режим безопасности) персональных данных при их обработке в ИСПДн согласно «Инструкции по обеспечению безопасности персональных данных».

3.3. Наделять и изменять права доступа всех групп пользователей ИСПДн к персональным данным и защищаемым программным ресурсам и портам ввода-вывода ИСПДн.

3.4. Осуществлять установку, настройку и сопровождение программных и технических СЗИ.

3.5. Осуществлять методическое руководство всех групп пользователей колледжа в вопросах функционирования СЗИ и введенного режима защиты.

3.6. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

3.7. Участвовать в приемке новых программных и технических средств, в том числе СЗИ.

3.8. Участвовать в проведении расследований случаев несанкционированного доступа к персональным данным и других нарушений «Правил обработки персональных данных».

3.9. Обеспечить доступ к защищаемой информации всем группам пользователей ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.

3.10. Уточнять в установленном порядке обязанности всех групп пользователей ИСПДн по обеспечению безопасности персональных данных.

3.11. Вести контроль над процессом осуществления резервного копирования баз данных и настроек комплекса средств автоматизации ИСПДн согласно «Инструкции по порядку резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и СЗИ в АИС СПО».

3.12. Осуществлять контроль порядка учёта, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

3.13. Осуществлять контроль выполнения «Плана мероприятий по обеспечению защиты персональных данных в колледже ».

3.14. Анализировать состояние защиты ИСПДн и их отдельных подсистем.

3.15. Контролировать неизменность состояния СЗИ, их параметров и режимов защиты.

3.16. Контролировать физическую сохранность СЗИ и оборудования ИСПДн.

- 3.17. Контролировать исполнение всеми группами пользователей ИСПДн введённого режима защищенности, а так же правильность работы с элементами ИСПДн и СЗИ.
- 3.18. Контролировать исполнение всем группами пользователей ИСПДн парольной политики согласно «Инструкции по организации парольной защиты».
- 3.19. Организовывать антивирусную защиту всех элементов ИСПДн согласно «Инструкции по организации антивирусной защиты».
- 3.20. Контролировать работу пользователей ИСПДн колледжа.
- 3.21. Своевременно анализировать журнал учёта событий, регистрируемых СЗИ, с целью выявления возможных нарушений.
- 3.22. Не допускать установку, использование, хранение и размножение в ИСПДн ПО, не связанных с выполнением функциональных задач.
- 3.23. Не допускать к работе на элементах ИСПДн посторонних лиц.
- 3.24. Регистрировать факты выдачи внешних носителей в «Журнале учета мобильных технических средств».
- 3.25. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования СЗИ ИСПДн.
- 3.26. Периодически представлять руководству отчёт о состоянии защиты АИС СПО и о нештатных ситуациях на объектах ИСПДн и допущенных всеми группами пользователей нарушениях и установленных требований по защите информации.
- 3.27. В случае отказа работоспособности СЗИ ИСПДн, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.
- 3.28. Принимать меры по реагированию в случае возникновения нештатных или аварийных ситуаций с целью ликвидации их последствий.
- 3.29. Предлагать руководству мероприятия по совершенствованию работы по защите персональных данных.

4. Права

Ответственный имеет право

- 4.1. Требовать от всех групп пользователей ИСПДн соблюдения законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, «Правил обработки персональных данных» и других нормативных документов колледжа в области обработки и защиты персональных данных.
- 4.2. Запрещать всем группам пользователей ИСПДн доступ к персональным данным при нарушении «Правил обработки персональных данных», при неисправностях в работе СЗИ и с целью предотвращения несанкционированного доступа к охраняемой информации.
- 4.3. Участвовать в анализе ситуаций, касающихся функционирования СЗИ, и в расследованиях по случаям несанкционированного доступа к персональным данным и другим случаям нарушения режима обработки персональных данных.
- 4.4. Вносить предложения руководству по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями.
- 4.5. В пределах своей компетенции сообщать руководству о недостатках, выявленных в процессе исполнения должностных обязанностей, и вносить предложения по их устранению.
- 4.6. Требовать от руководства оказания содействия в исполнении своих должностных обязанностей и прав.
- 4.7. Привлекать с разрешения руководства сотрудников всех структурных подразделений к решению задач, возложенных на него.

4.8. Запрашивать лично или через директора колледжа информацию и документы, необходимые для выполнения своих должностных обязанностей.

5. Ответственность

Ответственный несет ответственность:

5.1. За качество проводимых работ по контролю всех групп пользователей ИСПДн в вопросах обеспечения безопасности персональных данных.

5.2. За обеспечение устойчивой работоспособности СЗИ ИСПДн.

5.3. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим трудовым законодательством Российской Федерации.

5.4. За правонарушения, совершенные в процессе осуществления своей деятельности, в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

5.5. За причинение материального ущерба – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

6. Порядок пересмотра инструкции

6.1. Настоящая Инструкция пересматривается, изменяется и дополняется по мере необходимости, но не реже одного раза в три года.

6.2. С приказом о внесении изменений (дополнений) в настоящую Инструкцию знакомятся под расписку все сотрудники, на которых распространяется действие этой инструкции.