**ЧАСТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ**
**«СТАВРОПОЛЬСКИЙ КООПЕРАТИВНЫЙ ТЕХНИКУМ»**

**СОГЛАСОВАНО**
Протокол заседания
Студенческого совета
от «30» августа 2023 г. № 1
Председатель Совета
_____

**УТВЕРЖДАЮ**
Директор Частного профессионального образовательного учреждения «Ставропольский кооперативный техникум»
_____А.А. Намитоков
от «30» августа 2023 г. Приказ № 112

# ИНСТРУКЦИЯ АДМИНИСТРАТОРУ БЕЗОПАСНОСТИ
информационной системы персональных данных
«Автоматизированное рабочее место оператора УОП»

## 1 Общие положения

1.1. Настоящая инструкция определяет общие функции, права и обязанности Администратора безопасности информационной системы персональных данных «Автоматизированное рабочее место оператора УОП» (далее – ИСПДН).

1.2. Администратор безопасности назначается приказом руководителя учреждения.

1.3. Администратор безопасности в своей работе руководствуется настоящей инструкцией, требованиями законов и иных нормативно-правовых актов Российской Федерации по вопросам защиты персональных данных, руководящими и нормативными документами ФСТЭК России, ФСБ России и внутренними организационно-распорядительными документами Учреждения.

1.4. Администратор безопасности является ответственным должностным лицом Учреждения, уполномоченным на проведение работ по обеспечению устойчивого функционирования элементов ИСПДн, технической защите информации и поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов на этапах промышленной эксплуатации и модернизации.

1.5. Администратор безопасности осуществляет методическое руководство пользователей ИСПДн, в вопросах обеспечения безопасности персональных данных.

1.6. Требования Администратора безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.

1.7. Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

1.8. Рабочее место Администратора безопасности должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое).

1.9. На время отсутствия Администратора безопасности (отпуск, болезнь, пр.) его обязанности исполняет специалист, с которым предварительно проводился инструктаж по обслуживанию системы защиты информации в учреждении. Назначенный сотрудник приобретает соответствующие права и несет ответственность за надлежащее исполнение возложенных на него обязанностей.

## 2 Задачи Администратора безопасности

2.1. Основными задачами Администратора безопасности за обеспечение безопасности персональных данных являются:

- обеспечение устойчивого функционирования и работоспособности элементов ИСПДн, в т.ч. автоматизированных рабочих мест (далее - АРМ) пользователей и локальной вычислительной сети (далее - ЛВС);
- поддержание необходимого уровня защиты ИСПДн от несанкционированного доступа (далее - НСД) к информации;
- установка средств защиты информации на элементах ИСПДн и контроль выполнения правил их эксплуатации;
- сопровождение СЗИ, используемых в ИСПДн;
- периодическое обновление используемых СЗИ (при необходимости);
- проведение комплекса мероприятий по предотвращению инцидентов ИБ;
- оперативное реагирование на нарушения требований по ИБ ИСПДн и участие в их прекращении.

2.2. В рамках выполнения основных задач Администратор безопасности осуществляет:

- обеспечение установки, настройки и своевременного обновления элементов ИСПДн:

программного обеспечения автоматизированных рабочих мест (АРМ) пользователей (операционные системы, прикладное и специальное программное обеспечение (ПО); аппаратных средств; коммутационного оборудования.

- текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств СЗИ;
- принятие мер по своевременному восстановлению и выявлению причин в случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн;
- текущий контроль технологического процесса автоматизированной обработки информации;
- текущий контроль неизменности состояния СЗИ их параметров и режимов защиты;
- текущий контроль физической сохранности средств и оборудования ИСПДн;
- контроль исполнения пользователями установленных в ИСПДн правил организации парольной защиты;
- анализ журналов учета событий безопасности СЗИ, с целью выявления возможных нарушений;
- учет машинных носителей информации, используемых в ИСПДн;
- контроль действий пользователей при работе с машинными носителями информации;
- ввод полномочий пользователей в разрешительную систему доступа (матрицу доступа) и их своевременную корректировку;
- контроль за соблюдением пользователями установленных в ИСПДн правил по организации антивирусного контроля;
- участие в проведении служебных расследований фактов нарушений или угрозы нарушений безопасности информации;
- контроль соблюдения нормативных требований по защите информации, обеспечения комплексного использования технических средств, методов и организационных мероприятий по безопасности информации пользователями ИСПДн;
- методическую помощь пользователям ИСПДн по вопросам обеспечения защиты

информации и работы с используемыми СЗИ.

## 3 Обязанности Администратора безопасности информации

Администратор безопасности обязан:

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 в ЧПОУ «Кооперативный техникум» 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 в ЧПОУ «Кооперативный техникум» 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 ЧПОУ «Кооперативный техникум».

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 ЧПОУ «Кооперативный техникум».

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 в ЛВС в ЧПОУ «Кооперативный техникум».

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 ЧПОУ «Кооперативный техникум» 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 Администратор безопасности

Администратор безопасности 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 ЧПОУ «Кооперативный техникум» 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 ЧПОУ «Кооперативный техникум» информацию и документы, необходимые для выполнения своих должностных обязанностей.

## 5 Действия Администратора безопасности при обнаружении попыток НСД

5.1. К попыткам НСД относятся:

- сеансы работы с информационными ресурсами ИСПДн незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых не входят операции доступа к определенным данным или манипулирования ими;
- действия третьего лица, пытающегося получить доступ (или получившего доступ) к информационным ресурсам ИСПДн с использованием учетной записи администратора или другого пользователя ИСПДн, в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

5.2. При выявлении факта/попытки НСД Администратор безопасности обязан:

- прекратить доступ к информационным ресурсам со стороны выявленного участка НСД;

- доложить в случае необходимости руководителю Учреждения о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;

- известить начальника структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;

- проанализировать характер НСД;

- по решению руководства осуществить действия по выяснению причин, приведших к НСД;

- предпринять меры по предотвращению подобных инцидентов в дальнейшем.

## 6 Ответственность Администратора безопасности

6.1. Администраторы безопасности, виновные в несоблюдении настоящей Инструкции, расцениваются как нарушители законодательства Российской Федерации в области защиты информации и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.