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 ПОЛЬЗОВАТЕЛЯ
информационной системы персональных данных
«Автоматизированное рабочее место оператора УОП»

1 Общие положения

1.1 Пользователем информационной системы персональных данных «Автоматизированное рабочее место оператора УОП» (далее - ИСПДн) является каждый сотрудник частного профессионального образовательного учреждения «Ставропольский кооперативный техникум» (далее - Учреждение), участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты информации ИСПДн.

1.2 Пользователь несет персональную ответственность за свои действия.

1.3 Пользователь в своей работе руководствуется настоящей инструкцией, нормативными документами ФСТЭК России, ФСБ России, внутренними регламентирующими документами Учреждения и другими документами.

1.4 Методическое руководство работой пользователя в части выполнения положений законодательства Российской Федерации и внутренних документов Учреждения в области защиты информации осуществляется администратором безопасности.

2 Должностные обязанности

Пользователь ИСПДн, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

2.1 Решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн, присвоенными Администратором безопасности данному пользователю. При этом для хранения файлов, содержащих конфиденциальные сведения, разрешается использовать только соответствующим образом учтенные машинные носители информации.

2.2 Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации.

2.3 Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нем

информацией посторонними лицами. Шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.4 Знать и строго выполнять правила работы со средствами защиты информации, установленными на вверенном ему автоматизированном рабочем месте (далее - АРМ).

2.5 Соблюдать требования Инструкции по организации парольной защиты.

2.6 В случае отказа системы в идентификации пользователя, либо не подтверждения личного пароля немедленно обратиться к Администратору безопасности.

2.7 Строго соблюдать установленные требования по организации антивирусной защиты. В случае обнаружения вирусов немедленно сообщить об этом Администратору безопасности.

2.8 Знать и соблюдать установленные требования по учету, хранению машинных носителей информации.

2.9 Немедленно ставить в известность Администратора безопасности и в случае подозрения, а также при обнаружении фактов совершения попыток несанкционированного доступа (далее - НСД) к ресурсам ИСПДн: 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, выхода из строя или неустойчивого функционирования узлов ИСПДн или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, непредусмотренных отводов кабелей и подключенных устройств.

2.10 Для получения консультаций по вопросам работы ПЭВМ и настройке программного обеспечения необходимо обращаться к Администратору ИСПДн, по вопросам работы средств защиты информации – к Администратору безопасности.

2.11 Принимать меры по реагированию, в случае возникновения нештатных и аварийных ситуаций, с целью ликвидации их последствий, в пределах, возложенных на него функций.

2.12 Проходить периодическую проверку знаний положений нормативной документации по вопросам защиты информации в ходе периодического контроля соблюдения режима безопасности информации в ИСПДн.

2.13 Пользователям **ЗАПРЕЩАЕТСЯ:**

- Использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях.
- Отключать (блокировать) средства защиты информации.
- Самовольно вносить какие-либо изменения в конфигурацию аппаратно- программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства.
- Осуществлять обработку защищаемой информации в присутствии посторонних (не допущенных к данной информации) лиц.
- Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.
- Записывать и хранить защищаемую информацию (содержащую сведения ограниченного распространения) на неучтенных носителях информации.

Оставлять включенной без присмотра рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры). При этом на устройстве отображения (мониторе) после блокировки сеанса не должна отображаться информация сеанса пользователя (в том числе использование «хранителя экрана», гашение экрана или иные способы).

- Оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения).
- Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок ставить в известность Ответственного за обеспечение безопасности персональных данных.
- Осуществлять какие-либо действия в ИСПДн до прохождения процедур идентификации и аутентификации.
- Подключать к рабочей станции и вычислительной сети личные внешние носители и мобильные устройства.
- Отключать (блокировать) средства защиты информации.
- Привлекать посторонних лиц для производства ремонта или настройки АРМ.
- Разглашать защищаемую информацию третьим лицам.
- Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

3 Права и ответственность пользователей

Пользователь ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с его полномочиями к ресурсам ИСПДн и вверенным ему техническим и программным средствам.

Пользователь ИСПДн, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия.

Пользователь ИСПДн несет ответственность по действующему законодательству за разглашение сведений конфиденциального характера, ставших известными ему по роду работы.