

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

СОГЛАСОВАНО

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

А.А. Намиток

УТВЕРЖДАЮ

Директор Частного профессионального
образовательного учреждения
«Ставропольский кооперативный техникум»

А.А. Намиток

от «30» августа 2023 г. Приказ № 112



**Правила осуществления мероприятий по обеспечению безопасности персональных данных и работой пользователей в информационной системе персональных данных
«Автоматизированное рабочее место оператора УОП»**

1 Общие положения

1.1 Настоящий документ определяет процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере защиты персональных данных (далее - ПДн); основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПДн в информационной системе персональных данных «Автоматизированное рабочее место оператора УОП» (далее - ИСПДн) требованиям к защите ПДн.

- Настоящий документ разработан в соответствии с Федеральным закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. 31.07.2023);
- Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (ред. 06.02.2023);

и другими нормативными правовыми актами в сфере защиты персональных данных.

1.2 Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдения условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ИСПДн проводятся в следующих целях:

- проверка выполнения требований организационно-распорядительной документации по защите информации в ИСПДн и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

оценка уровня осведомленности и знаний работников, допущенных к работе в ИСПДн, в области обработки и защиты персональных данных;

- оценка обоснованности и эффективности применяемых мер и средств защиты.

2 Тематика внутреннего контроля

Тематика внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн:

2.1 Проверки соответствия обработки ПДн в ИСПДн установленным требованиям разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

2.2 Регулярные контрольные мероприятия проводятся Администратором безопасности ИСПДн периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее - План, Приложение 1) и предназначены для осуществления контроля выполнения требований в области защиты ПДн.

2.3 Плановые контрольные мероприятия проводятся постоянной комиссией периодически в соответствии с утвержденным Планом (Приложение 1) и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн.

2.4 Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности (создается на период проведения мероприятий). Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

- по результатам расследования инцидента информационной безопасности;
- по результатам внешних контрольных мероприятий, проводимых регулирующими органами;
- по решению руководителя Учреждения.

3 Планирование контрольных мероприятий

3.1 Для проведения плановых внутренних контрольных мероприятий Администратор безопасности разрабатывает План внутренних контрольных мероприятий на текущий год.

3.2 План проведения внутренних контрольных мероприятий включает следующие сведения по каждому из мероприятий состав участников, привлекаемых для проведения контрольных мероприятий; сроки и этапы проведения контрольных мероприятий.

3.3 Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий.

4 Оформление результатов контрольных мероприятий

4.1 По итогам проведения плановых и внеплановых контрольных мероприятий лицо, комиссия, разрабатывает Протокол (Приложение 2), в котором указывается:

- описание проведенных мероприятий по каждому из этапов;
- перечень и описание выявленных нарушений;
- рекомендации по устранению выявленных нарушений;
- заключение по итогам проведения внутреннего контрольного мероприятия.

4.2 Протокол передается на рассмотрение руководителю Учреждения.

4.3 Общая информация о проведенном контрольном мероприятии фиксируется в «Журнале учета внутренних мероприятий по контролю за обеспечением безопасности ПДн при их обработке в ИСПДн» (Приложение 3).

5 Порядок проведения плановых и внеплановых контрольных мероприятий

5.1 Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственного за организацию обработки ПДн в Учреждении совместно с Администратором безопасности ИСПДн (далее - комиссия).

5.2 Проверки соответствия обработки ПДн установленным требованиям в ИСПДн ОИ проводятся на основании Планом проведения контрольных мероприятий (Приложение 1).

5.3 Проведение внеплановой проверки организуется в течение пяти рабочих дней с момента поступления соответствующего заявления.

5.4 При проведении проверки соответствия обработки ПДн установленным требованиям должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, исполнение которых обеспечивает установленный уровень защищенности ПДн;
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности ПДн при их обработке в ИСПДн;
- состояние учета машинных носителей ПДн;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер.

5.5 При проведении внутренней проверки комиссия имеет право:

- запрашивать у сотрудников Учреждения, допущенных к обработке ПДн в ИСПДн, сведения, необходимые для реализации полномочий;
- требовать от уполномоченных на обработку ПДн должностных лиц уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем ПДн;
- принимать меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований законодательства Российской Федерации;
- вносить руководителю Учреждения предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности ПДн предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки ПДн.

5.6 В отношении информации ограниченного доступа, ставшей известной комиссии в ходе проведения мероприятий по внутреннему контролю, должна обеспечиваться ее конфиденциальность.

5.7 Проверка должна быть завершена не позднее, чем через пять рабочих дней со дня принятия решения о её проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений составляется протокол (Приложение 2), который должен быть представлен руководителю Учреждения для ознакомления.

5.8 Все проводимые мероприятия по контролю за обеспечением безопасности персональных данных должны быть зафиксированы в Журнале (Приложение 3). Ответственность за ведение Журнала возлагается на Администратора безопасности ИСПДн.