

Министерство образования Ставропольского края
Государственное бюджетное профессиональное образовательное учреждение
«Георгиевский региональный колледж «Интеграл».

СОГЛАСОВАНО
Председатель первичной
Профсоюзной организации колледжа

А.С. Шеблыкин
« 17 » 03 2025 г.



УТВЕРЖДАЮ
Директор ГБПОУ ГРК «Интеграл»,
к.п.н. Д.А. Саховский
« 17 » 03 2025 г.
Приказ № 14
от « 17 » 03 2025 г.



ПОЛОЖЕНИЕ
о защите персональных данных
в государственном бюджетном профессиональном образовательном
учреждении «Георгиевский региональный колледж «Интеграл».

1. Общие положения

1.1. Настоящее Положение о защите персональных данных в государственном бюджетном профессиональном образовательном учреждении «Георгиевский региональный колледж «Интеграл» (далее - Положение) разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006г. № 152-ФЗ «О персональных данных», Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства Российской Федерации от 01.11.2012г. № 1119 и иными нормативно-правовыми актами, действующими на территории Российской Федерации.

1.2. Цель настоящего Положения - защита персональных данных работников государственного бюджетного профессионального образовательного учреждения «Георгиевский региональный колледж «Интеграл» (далее - Колледж, работодатель) от несанкционированного доступа и разглашения, предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

1.3. Для целей настоящего Положения используются следующие основные понятия:

- **персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (п. 1 с. 3 Федерального закона от 27.07.2006г. № 152-ФЗ);

- **угрозы безопасности персональных данных** - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных, путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом от 27.07.2006г. № 152-ФЗ (далее - персональные данные, разрешенные для распространения) (п.1.1. ст. 3 Федерального закона от 27.07.2006г. № 152-ФЗ);

- **уровень защищенности персональных данных** - комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационной системе.

1.4. Настоящее Положение и изменения к нему утверждаются директором Колледжа и вводятся приказом. Все работники должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

2. Защита персональных данных

2.1. Работодатель принимает следующие меры по защите персональных данных:

2.1.1. Назначение лица, ответственного за обработку персональных данных, которое осуществляет организацию обработки персональных данных, обучение и инструктаж, внутренний контроль за соблюдением работниками требований к защите персональных данных.

2.1.2. Разработка политики в отношении обработки персональных данных.

2.1.3. Установление правил доступа к персональным данным, обеспечение регистрации и учета всех действий, совершаемых с персональными данными.

2.1.4. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их должностными обязанностями.

2.1.5. Применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации.

2.1.6. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

2.1.7. Соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ.

2.1.8. Обнаружение фактов несанкционированного доступа к персональным данным.

2.1.9. Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.1.10. Обучение работников, непосредственно осуществляющих обработку персональных данных, положениям законодательства РФ о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику работодателя в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных.

2.1.11. Осуществление внутреннего контроля и аудита.

2.1.12. Определение типа угроз безопасности и уровней защищенности персональных данных, которые хранятся в информационных системах.

2.2. Угрозы защищенности персональных данных.

2.2.1. Угрозы первого типа. В системном программном обеспечении информационной системы есть функциональные возможности программного обеспечения, которые не указаны в описании к нему либо не отвечают характеристикам, которые заявил производитель. И это потенциально может привести к неправомерному использованию персональных данных.

2.2.2. Угрозы второго типа. Потенциальные проблемы с прикладным программным обеспечением-внешними программами, которые установлены на компьютерах работников.

2.2.3. Угрозы третьего типа. Потенциальной опасности ни от системного, ни от программного обеспечения нет.

2.3. Уровни защищенности персональных данных.

2.3.1. Первый уровень защищенности. Если работодатель отнес информационную систему к первому типу угрозы или если тип угрозы второй, но работодатель обрабатывает специальные категории персональных данных более 100 тыс. физических лиц без учета работников.

2.3.2. Второй уровень защищенности. Если тип угрозы второй и работодатель обрабатывает специальные категории персональных данных работников⁷ вне зависимости от их количества или специальные категории персональных данных менее чем 100 тыс. физических лиц, или любые другие категории персональных данных более чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает специальные категории данных более чем 100 тыс. физических лиц.

2.3.3. Третий уровень защищенности. Если при втором типе угрозы работодатель обрабатывает общие персональные данные работников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает специальные категории персональных данных работников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает биометрические персональные данные, или при третьем типе угрозы работодатель обрабатывает общие персональные данные более чем 100 тыс. физических лиц.

2.3.4. Четвертый уровень защищенности. Если при третьем типе угрозы работодатель обрабатывает только общие персональные данные работников или менее чем 100 тыс. физических лиц.

2.4. При четвертом уровне защищенности персональных данных работодатель:

- обеспечивает режим безопасности помещений, в которых размещает информационную систему;
- обеспечивает сохранность носителей информации;
- утверждает перечень работников, допущенных к персональным данным;
- использует средства защиты информации, которые прошли оценку соответствия требованиям закона в области обеспечения безопасности информации.

2.5. При третьем уровне защищенности персональных данных дополнительно к мерам, перечисленным в пункте 2.4. настоящего Положения, работодатель назначает ответственного за обеспечение безопасности персональных данных в информационной системе.

2.6. При втором уровне защищенности персональных данных дополнительно к мерам, перечисленным в пунктах 2.4., 2.5. настоящего Положения, работодатель ограничивает доступ к электронному журналу сообщений, за исключением работников, которым такие сведения необходимы для работы.

2.7. При первом уровне защищенности персональных данных дополнительно к мерам, перечисленным в пунктах 2.4.—2.6. настоящего Положения, работодатель:

- обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работников по допуску к персональным данным в системе;
- создает отдел, ответственный за безопасность персональных данных в системе, либо возлагает такую обязанность на один из существующих отделов работодателя.

2.8. В целях защиты персональных данных на бумажных носителях работодатель:

- приказом назначает ответственного за обработку персональных данных;
- ограничивает допуск в помещения, где хранятся документы, которые содержат персональные данные работников;
- хранит документы, содержащие персональных данных работников в шкафах, запирающихся на ключ;
- хранит трудовые книжки работников в сейфе в отделе кадров.

2.9. В целях обеспечения конфиденциальности документы, содержащие персональные данные работников, оформляются, ведутся и хранятся только работниками отдела правового обеспечения и охраны труда и бухгалтерии работодателя.

2.10. Работники отдела правового обеспечения и охраны труда и бухгалтерии работодателя, допущенные к персональным данным работников, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки персональных данных работники не допускаются.

2.11. Допуск к документам, содержащим персональные данные работников, внутри организации осуществляется на основании Регламента допуска работников к обработке персональных данных.

2.12. Передача персональных данных по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством РФ, допускается исключительно с согласия работника на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

2.13. Передача информации, содержащей сведения о персональных данных работников, по телефону в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

3. Гарантии конфиденциальности персональных данных

3.1. Все работники колледжа, осуществляющие обработку персональных данных, обязаны хранить тайну о сведениях, содержащих персональные данные, в соответствии с Положением, требованиями законодательства РФ.

3.2. Работник вправе требовать полную информацию о своих персональных данных, об их обработке, использовании и хранении.

3.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работников, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством.