

ИНСТРУКЦИЯ

**по организации защиты персональных данных,
содержащихся в информационных системах государственного бюджетного
профессионального образовательного учреждения Краснодарского края
«Краснодарский монтажный техникум» (ГБПОУ КК «КМТ»)**

I. Общие положения

1. Инструкция по организации защиты персональных данных, содержащихся в информационных системах государственного бюджетного профессионального образовательного учреждения Краснодарского края «Краснодарский монтажный техникум» (далее – Инструкция), разработана в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иными нормативными правовыми актами Российской Федерации, регламентирующими порядок обработки персональных данных.

2. Настоящая Инструкция определяет порядок выполнения мероприятий по защите персональных данных (далее – ПДн), содержащихся в информационных системах государственного бюджетного профессионального образовательного учреждения Краснодарского края «Краснодарский монтажный техникум», устанавливает меры по обеспечению безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн или информационная система), а также определяет обязанности должностных лиц.

В Инструкции не рассматриваются вопросы обеспечения безопасности ПДн, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также меры, связанные с применением шифровальных (криптографических) средств защиты информации.

Методы и способы защиты информации, содержащейся в государственных информационных системах, определяются в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17.

3. Государственное бюджетное профессиональное образовательное учреждение Краснодарского края «Краснодарский монтажный техникум» (далее – ГБПОУ КК «КМТ») в соответствии с Федеральным законом № 152-ФЗ является оператором, организующим и (или) осуществляющим обработку ПДн, а также определяющим цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

4. Координацию и контроль деятельности по защите ПДн, содержащихся в информационных системах ГБПОУ КК «КМТ», осуществляет подразделение,

выполняющее функции по вопросам защиты ПДн при их автоматизированной обработке (далее – уполномоченное подразделение ГБПОУ КК «КМТ»).

5. Оператор определяет подразделения ГБПОУ КК «КМТ», осуществляющие обработку ПДн в эксплуатируемых информационных системах.

В случаях когда реализация мер по организации и обработке ПДн в ИСПДн возлагается на несколько подразделений ГБПОУ КК «КМТ», вопросы разграничения полномочий между ними отражаются в инструкции по эксплуатации соответствующей информационной системы.

6. Подразделения ГБПОУ КК «КМТ», выполняют функции оператора ИСПДн при эксплуатации информационной системы, в том числе при обработке информации, содержащейся в ее базах данных

II. Организация работ по обеспечению безопасности персональных данных при их автоматизированной обработке

7. Организация работ по созданию и эксплуатации ИСПДн, а также системы защиты персональных данных (далее – СЗПДн) осуществляется в соответствии с законодательством Российской Федерации в области обеспечения безопасности информации и соответствующими государственными стандартами.

8. Работы по обеспечению безопасности ПДн включаются в планирующие документы ГБПОУ КК «КМТ».

9. В целях обеспечения безопасности ПДн создается СЗПДн, которая должна обеспечивать конфиденциальность, целостность и доступность ПДн при их обработке в ИСПДн во всех структурных элементах, на технологических участках обработки и во всех режимах функционирования информационной системы.

СЗПДн включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных определяются в соответствии с нормативными правовыми актами, принятыми Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона 152-ФЗ.

10. Выбор средств защиты информации для СЗПДн осуществляется в установленном порядке (далее – СрЗИ) подразделениями ГБПОУ КК «КМТ» - операторами ИСПДн в зависимости от уровня защищенности ПДн, определяемого в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

11. Установление класса защищенности информационной системы и уровня защищенности ПДн производится подразделением ГБПОУ КК «КМТ» -

оператором ИСПДн на этапе создания (модернизации) ИСПДн, а также при изменении масштаба информационной системы или значимости обрабатываемой в ней информации.

Подразделения ГБПОУ КК «КМТ» - операторы ИСПДн, которые осуществляли обработку ПДн, должны обеспечить СЗПДн ранее введенных и (или) модернизирующихся информационных систем в соответствии с требованиями настоящей Инструкции.

12. В целях установления класса защищенности информационной системы и уровня защищенности ПДн приказом ГБПОУ КК «КМТ» - оператором ИСПДн назначается комиссия, в состав которой включаются представители подразделения ГБПОУ КК «КМТ», эксплуатирующего ИСПДн и осуществляющего свою деятельность в области информационных технологий, связи и защиты информации.

13. Результаты установления класса защищенности информационной системы и уровня защищенности ПДн оформляются соответствующим актом ГБПОУ КК «КМТ» - оператором ИСПДн.

14. Помещения, в которых размещены объекты информатизации, содержащие ИСПДн, должны соответствовать требованиям по обеспечению их сохранности, пожарной безопасности, а также защиты от несанкционированного проникновения посторонних лиц.

15. Для каждой ИСПДн на этапе ее создания (модернизации) разрабатываются модель угроз, а также документы, отражающие вопросы резервного копирования информации, содержащей ПДн, парольной защиты, проведения антивирусного контроля, порядка удаления (изменения) персонифицированных записей из (в) ИСПДн, обезличивания ПДн, проведения технического обслуживания ИСПДн, работы с машинными носителями ПДн.

16. Обработка ПДн в ИСПДн осуществляется только после завершения работ по созданию СЗПДн и вводу в эксплуатацию ИСПДн.

17. В ИСПДн не производится обработка информации с применением аппаратно-программных средств, не предусмотренных конструкторской и эксплуатационной документацией.

18. Для обеспечения сохранности информационных ресурсов ИСПДн производится их резервное копирование на материальный носитель, обеспечивающее возможность восстановления содержащихся в информационной системе сведений.

Порядок и периодичность проведения резервного копирования информации определяются в конструкторской документации на ИСПДн, а также в инструкции по эксплуатации ИСПДн.

19. Для каждой ИСПДн предусматривается:

- учет эксплуатирующего персонала, в том числе пользователей ИСПДн, непосредственно обрабатывающих ПДн в ИСПДн и (или) имеющих доступ к ИСПДн с целью обеспечения устойчивого функционирования информационной системы при ее использовании;
- учет и выдача машинных носителей ПДн;
- проведение инструктажей по обеспечению безопасности ПДн;
- проверка исправности технических средств и технического обслуживания.

20. Взаимодействие ИСПДн с внешними информационными системами сторонних организаций осуществляется с учетом положений международных договоров Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации.

Меры, принимаемые по защите ПДн в ИСПДн при их взаимодействии с внешними информационными системами сторонних организаций, отражаются в конструкторской, эксплуатационной и организационно-распорядительной документации на соответствующую информационную систему.

III. Организация разрешительной системы доступа к ИСПДн

21. Подразделениями ГБПОУ КК «КМТ» - операторами ИСПДн организуется разрешительная система доступа к техническим и программным средствам ИСПДн, а также к информационным ресурсам ИСПДн.

22. Порядок и условия доступа к ИСПДн определяются на стадии ее создания (модернизации) в конструкторской документации на ИСПДн и в инструкции по эксплуатации ИСПДн.

23. Регистрация пользователей в ИСПДн осуществляется ответственным за обеспечение безопасности ИСПДн на основании списков должностных лиц, утвержденных приказом ГБПОУ КК «КМТ».

24. При обнаружении нарушений порядка предоставления ПДн ответственный за обеспечение безопасности ИСПДн незамедлительно информирует об этом директора ГБПОУ КК «КМТ» и приостанавливает предоставление ПДн пользователям ИСПДн до выявления причин нарушений или их устранения.

IV. Обязанности должностных лиц ГБПОУ КК «КМТ» по защите персональных данных

25. Работники подразделений ГБПОУ КК «КМТ» - операторов ИСПДн обеспечивают выполнение правовых, организационных и технических мер, предусмотренных законодательными и иными нормативными правовыми актами Российской Федерации, в части, их касающейся, в том числе:

- планирование и организацию выполнения мероприятий по обеспечению безопасности ПДн;
- конфиденциальность, целостность и доступность ПДн;
- организацию взаимодействия подразделений ГБПОУ КК «КМТ», обеспечивающих создание (модернизацию) и эксплуатацию ИСПДн;
- защиту ПДн;
- определение должностных обязанностей лиц, ответственных за организацию обработки ПДн и за эксплуатацию ИСПДн;
- организацию и осуществление контроля за выполнением установленных требований по обеспечению безопасности ПДн.

26. Ответственными за соблюдение требований по защите ПДн при их автоматизированной обработке являются работники ГБПОУ КК «КМТ», эксплуатирующие, использующие ИСПДн, непосредственно обрабатывающие

ПДн в ИСПДн, а так же, имеющие доступ к ИСПДн с целью обеспечения устойчивого функционирования информационной системы при ее использовании.

27. Лица, указанные в пункте 26 настоящей Инструкции, осуществляют обработку ПДн в соответствии с требованиями Федерального закона № 152-ФЗ и иными нормативными правовыми актами Российской Федерации в сфере защиты ПДн, а также несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты ПДн.

28. В подразделениях ГБПОУ КК «КМТ» с работниками, уполномоченными на обработку ПДн в ИСПДн, в целях повышения уровня профессиональной подготовки организуются изучение требований законодательства Российской Федерации по вопросам обеспечения безопасности ПДн, а также проверка их знаний.

V. Контроль обеспечения безопасности персональных данных

29. Целью контроля является соблюдение подразделениями ГБПОУ КК «КМТ» требований по обеспечению безопасности ПДн при их обработке в ИСПДн.

30. Задачами контроля являются:

- установление фактического положения дел в подразделении ГБПОУ КК «КМТ» по обеспечению безопасности ПДн при их обработке в ИСПДн;
- выявление проблемных вопросов в организации обеспечения безопасности ПДн;
- обеспечение соблюдения законодательства в сфере ПДн;
- выработка мер по оказанию методической и практической помощи подразделениям ГБПОУ КК «КМТ»;
- повышение ответственности работников за выполнение возложенных задач, соблюдение законности в их деятельности.

31. Контроль за выполнением требований настоящей Инструкции организуется и проводится уполномоченным подразделением ГБПОУ КК «КМТ», осуществляющим свою деятельность в области информационных технологий, связи и защиты информации, самостоятельно, не реже 1 раза в 3 года.

Юрисконсульт



О.П.Галюк

СОГЛАСОВАНО:

Техник по обслуживанию
вычислительной техники



А.А. Попов

Ведущий специалист по кадрам



Т.В. Миллер