Общество с ограниченной ответственностью
«Центр консалтинговых услуг ТЕУС»
(ООО «ЦКУ ТЕУС»)

УТВЕРЖДАЮ
Генеральный директор
ООО «ЦКУ ТЕУС»

Ананко В.С.

«___» _____ 2025 г.

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

Программа повышения квалификации
«Организация работы по защите персональных данных»
(72часа)

г. Севастополь
2025 г.

Оглавление

1. Общие положения

Программа направлена на совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации специалиста, участвующего в обработке и хранение персональных данных.

- Программа разработана в соответствии со следующими нормативными документами:
- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Приказ Министерства образования и науки РФ от 01.07.2013 № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;
- Профессиональный стандарт «Специалист по технической защите информации», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 09.08.2022 № 474н;
- Общероссийский классификатор занятий ОК 010-2014 (МСКЗ-08), (дата введения 01.07.2015).

Категория слушателей: специалисты предприятий и организаций, ответственные за обеспечение безопасности при работе с персональными данными.

Требования к имеющемуся уровню образования:

Лица, имеющие:

- Высшее образование (специалитет / бакалавриат / магистратура);
- Среднее профессиональное образование.
- Наличие указанного образования должно подтверждаться документом
- государственного или установленного образца.

Форма обучения: Программа повышения квалификации «Организация работы по защите персональных данных» реализуется посредством следующих форм обучения:

дистанционная форма обучения.

Обучение проводится с применением дистанционных образовательных технологий, которые содержат электронные учебно - методические материалы, нормативные документы, вебинары и реализуются с применением информационно – телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.

При реализации образовательной программы с применением дистанционных образовательных технологий местом осуществления образовательной деятельности является место нахождения организации, осуществляющей образовательную деятельность, или ее филиала независимо от места нахождения обучающихся (п.4. ст.16 Федерального закона № 273-ФЗ от 29 декабря 2012 г. «Об образовании в Российской Федерации»).

Срок обучения: 72аудиторных часа; 1 академический час – 45 минут.

2. Цель и планируемые результаты обучения

Целью данной Программы является совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации специалиста, участвующего в обработке и хранение персональных данных в следующих видах деятельности:

- проведение аттестации объектов информатизации на соответствие требованиям по защите информации;

- организация и проведение работ по защите информации в организации.

Обучающийся в ходе освоения Программы **должен знать:**

- нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации;
- порядок аттестации объектов информатизации на соответствие требованиям по защите информации;
- программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее;
- способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах;
- методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее;
- технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом высокочастотного облучения основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах;
- технические каналы утечки акустической речевой информации (прямые акустические, вибрационные, акустооптические, акустоэлектрические, акусто-электромагнитные) технические каналы утечки акустической речевой информации, создаваемые за счет возможно внедренных специальных электронных устройств перехвата информации в технические средства и (или) предметы интерьера помещения;
- способы и средства защиты информатизации от утечки за счет побочных электромагнитных излучений и наводок;
- способы и средства защиты акустической речевой информации от утечки по техническим каналам;
- нормативные правовые акты, методические документы в области защиты информации ограниченного доступа;
- организационно-распорядительную документацию по защите информации на объекте информатизации;
- эксплуатационную документацию на систему защиты информации;
- организационно-распорядительную документацию по защите информации на объекте информатизации;
- методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее;
- порядок создания автоматизированных систем в защищенном исполнении.

Обучающийся в ходе освоения программы **должен уметь:**

- определять перечень информации (сведений) ограниченного доступа, подлежащих защите в организации;
- разрабатывать техническое задание на создание системы защиты информации в организации;

- разрабатывать разрешительную систему доступа к информационным ресурсам,
- программным и техническим средствам автоматизированных (информационных) систем организации;
- разрабатывать аналитическое обоснование необходимости создания системы защиты информации в организации;
- анализировать данные о назначении, функциях, условиях функционирования основных технических средств и систем, установленных на объектах информатизации, и характере обрабатываемой на них информации;
- организовывать ввод системы защиты информации в эксплуатацию.

3. Содержание программы. Учебный план

УЧЕБНЫЙ ПЛАН

№ п/п	Наименование компонентов программы	Продолжительность, час.
1	**Законодательство РФ в области защиты персональных данных. Основные понятия в законодательстве о персональных данных. Организация работы по защите персональных данных**	**8**
2	**Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа**	**15**
3	**Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных**	**21**
4	**Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных**	**15**
5	**Меры безопасности, применяемые при обработке персональных данных в информационных системах**	**12**
	Итоговое тестирование	**1**
	ИТОГО	**72**

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Наименование дисциплин	Всего часов	Лекции
Раздел 1	**Законодательство РФ в области защиты персональных данных. Основные понятия в законодательстве о персональных данных. Организация работы по защите персональных данных**	**8**	**8**
1.1.	Правовые основы технической защиты информации ограниченного доступа	**2**	**2**
1.2.	Организационные основы технической защиты информации ограниченного	**2**	**2**

	доступа		
1.3.	Организационные основы технической защиты информации ограниченного доступа в организации	**2**	**2**
1.4.	Сертификация средств защиты и аттестация объектов информатизации	**2**	**2**
Раздел 2	**Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа**	**15**	**15**
2.1.	Выявление угроз безопасности информации на объектах информатизации	5	5
2.2.	Основные организационные меры защиты информации от несанкционированного доступа	5	5
2.3.	Основные технические и программные средства защиты информации от несанкционированного доступа	5	5
Раздел 3	**Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных**	**21**	**21**
3.1.	Угрозы безопасности информации	10	10
3.2.	Утечка информации	5	5
3.3.	Защита информации от утечки	6	6
Раздел 4	**Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных**	**15**	**15**
4.1.	Основные понятия обработки персональных данных	3	3
4.2.	Субъект персональных данных	3	3
4.3.	Оператор персональных данных	3	3
4.4.	Меры по обеспечению безопасности персональных данных	6	6
4.5.	Обработка персональных данных	3	3
4.6.	Нарушения законодательства РФ в области персональных данных	3	3
Раздел 5	Меры безопасности, применяемые при обработке персональных данных в информационных системах	**12**	**12**
5.1.	Типовые программно-технические	3	3

	средства защиты информации		
5.2.	Организация защиты персональных данных в организации	4	4
5.3.	Требования к защите, состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	4	4

Раздел 1. Законодательство РФ в области защиты персональных данных. Основные понятия в законодательстве о персональных данных. Организация работы по защите персональных данных

Тема 1.1. Правовые основы технической защиты информации ограниченного доступа

Основные понятия и определения в области защиты информации. Доктрина информационной безопасности Российской Федерации. Информационная безопасность как одно из стратегических направлений национальной безопасности Российской Федерации. Концептуальные вопросы защиты информации.

Тема 1.2. Организационные основы технической защиты информации ограниченного доступа

Силы обеспечения информационной безопасности. Задачи ФСБ России по обеспечению общей и информационной безопасности. Основные задачи ФСО России. Деятельность Минобороны России и МВД России по обеспечению информационной безопасности. Деятельность Минкомсвязи России в сфере информационной безопасности. Полномочия Роскомнадзора в сфере информационной безопасности. Полномочия ФСТЭК России. Задачи ФСТЭК России. Деятельность органов власти и местного самоуправления в сфере информационной безопасности РФ.

Тема 1.3. Организационные основы технической защиты информации ограниченного доступа в организации

Структура и функции органов и подразделений по технической защите информации в организации. Система обеспечения информационной безопасности. Лицензирование деятельности в области защиты информации.

Тема 1.4. Сертификация средств защиты и аттестация объектов информатизации

Нормативно-правовая база сертификации средств защиты и аттестации объектов информатизации. Формы подтверждения соответствия. Декларирование соответствия. Сертификат соответствия. Нормативно-правовая база сертификация средств защиты информации. Сертификация средств защиты информации (СЗИ). Электронная цифровая подпись. Аттестация объектов информатизации.

Раздел 2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа

Тема 2.1. Выявление угроз безопасности информации на объектах информатизации

Угрозы информационной безопасности. Классификация угроз информационной безопасности Классификация источников угроз. Уязвимости безопасности информации.

Тема 2.2. Основные организационные меры защиты информации от несанкционированного доступа

Аттестация объектов информатизации. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Разработка программы и методики аттестационных испытаний. Заключение договоров на аттестацию. Заключение по результатам аттестации. Рассмотрение апелляций. Аттестат соответствия. Аттестация объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну.

Тема 2.3. Основные технические и программные средства защиты информации от несанкционированного доступа

Особенности программно-математического воздействия в сетях общего пользования. Защита информации в локальных вычислительных сетях.

Раздел 3.

Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных

Тема 3.1. Угрозы безопасности информации

Угрозы безопасности информации. Случайные и преднамеренные угрозы. Традиционный шпионаж и диверсии. Системы подслушивания. Видеоразведка. Закладные устройства. Несанкционированный доступ к информации. Электромагнитные излучения и наводки. Несанкционированная модификация структур. Вредительские программы. Классификация злоумышленников.

Тема 3.2. Утечка информации

Утечка информации по техническим каналам. Физическая природа передачи информации. Каналы утечки информации. Особенности каналов утечки информации. Побочные электромагнитные излучения и наводки (ПЭМИН).

Тема 3.3. Защита информации от утечки

Защита информации от утечки по техническим каналам в общем плане. Защита информации от утечки по визуально-оптическим каналам. Средства и способы защиты информации от утечки по визуально-оптическому каналу. Защита информации от утечки по акустическим каналам. Защита информации от утечки по электромагнитным каналам. Защита от утечки за счёт электромагнитного излучения. Программно-аппаратный комплекс «Зарница». Защита от утечки за счет паразитной генерации. Защита от утечки по цепям питания. Защита от утечки за счет взаимного влияния проводов и линий связи. Взаимные влияния в линиях связи. Защита информации от утечки по материально-вещественным каналам.

Раздел 4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Тема 4.1. Основные понятия обработки персональных данных

Основные понятия, используемые в ФЗ от 27.07.2006 № 152 «О персональных данных». Принципы и условия обработки персональных данных. Условия обработки персональных данных.

Тема 4.2. Субъект персональных данных

Права субъекта персональных данных. Согласие субъекта персональных данных на обработку его персональных данных.

Тема 4.3. Оператор персональных данных

Обязанности оператора при сборе персональных данных. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных ФЗ от 27.07.2006 № 152 "О персональных данных".

Тема 4.4. Меры по обеспечению безопасности персональных данных

Меры по обеспечению безопасности персональных данных при их обработке. Состав и содержание мер по обеспечению безопасности персональных данных.

Тема 4.5. Обработка персональных данных

Уведомление об обработке персональных данных. Лица, ответственные за организацию обработки персональных данных в организациях. Обработка персональных данных без средств автоматизации. Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ.

Тема 4.6. Нарушения законодательства РФ в области персональных данных

Ответственность за нарушение законодательства Российской Федерации в области персональных данных при обработке персональных данных работника. Ответственность за нарушение законодательства Российской Федерации в области персональных данных.

Раздел 5. Меры безопасности, применяемые при обработке персональных данных в информационных системах

Тема 5.1. Типовые программно-технические средства защиты информации

Правовая база. Межсетевой экран. Брандмауэр. Криптография. Цифровая подпись.

Тема 5.2. Организация защиты персональных данных в организации

Защита персональных данных работника (общие положения). Требования к обработке персональных данных. Защита персональных данных. Организация доступа работников к персональным данным других работников.

Тема 5.3. Требования к защите, состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Требования к защите персональных данных при их обработке в информационных системах персональных данных. Состав и содержание организационных и технических мер по обеспечению безопасности персональных

данных при их обработке в информационных системах персональных данных. Организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации.

4. Организационно-педагогические условия

4.1. Материально-технические условия реализации программы

Программа повышения квалификации «Радиационный контроль металлолома» обеспечивается учебно-методической документацией и материалами по всем темам.

Для проведения дистанционных лекционных и практических занятий имеются аудитории, оснащенные современным оборудованием (компьютером, мультимедийным проектором для презентаций, экраном, доской, средствами звуковоспроизведения, NV, DVD т.п., удаленной системой видеосвязи).

Для всех видов занятий академический час устанавливается продолжительностью 45 минут.

Самостоятельная и практическая учебная работа обучающихся сопровождается методическим обеспечением и обоснованием времени, затрачиваемого на ее выполнение.

При освоении программы используются электронные образовательные технологии. На свою электронную почту обучающиеся получают ссылку для авторизации и доступа к системе электронного обучения (личный кабинет), расположенной в сети Интернет, к учебно-методическим материалам электронного курса. Это дает возможность изучать без ограничения по времени интерактивные лекции, анализировать необходимую нормативно-правовую документацию, выполнять тестовые и (или) практические задания.

Допускаетсяпроведениелекционныхзанятийпотехнологии вебинаров (интернет- конференций) в режиме реального времени в виртуальной вебинарной комнате.

Вебинар – это интернет - конференция в Интернете, которая проходит в режиме реального времени. Вовремя веб - конференции каждый из участников находится у своего компьютера и или мобильного устройства, а связь между ними поддерживается через Интернет посредством браузера. При запуске виртуального класса его материалы открываются в отдельном окне. Участники вебинара заранее получают письмо-приглашение на свою электронную почту. Для участия в вебинаре необходимо:

1. Подключить внешние колонки или активировать встроенные, чтобы слышать голос ведущего.

2. За 5 – 10 минут до начала вебинара пройти по указанной ссылке или скопировать ее в адресную строку браузера. Ссылка будет доступна только на время проведения вебинара.

Возможности виртуального класса позволяют участникам видеть и слышать лекцию преподавателя, задавать вопросы письменно (в чате), обсуждать с участниками вебинара проблемные ситуации и обмениваться практическим опытом.

Вебинары записываются, их можно просмотреть повторно в течение курса, а также шести месяцев с момента окончания обучения.

4.2. Кадровое обеспечение реализации программы

Реализация программы повышения квалификации обеспечивается научно - педагогическими кадрами, имеющими, как правило, базовое образование, соответствующее профилю преподаваемой дисциплины,и систематически занимающимися научной и научно - методической деятельностью.

К образовательному процессу привлечены преподаватели из числа

специалистов профильных организаций, предприятий и учреждений.

4.3. Учебно-методическое обеспечение программы Основные источники:

1. Конституция РФ;
2. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (КоАП РФ);
3. Федеральный закон от 28.06.2014 № 172-ФЗ «О стратегическом планировании в Российской Федерации»;
4. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»;
5. Федеральный закон от 03.04.1995 № 40-ФЗ «О федеральной службе безопасности»;
6. Федеральный закон от 27.05.1996 № 57-ФЗ «О государственной охране»;
7. Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»;
8. Федеральный закон от 26.12.2008 № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»;
9. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
10. Федеральный закон от 27.12.2002 №184-ФЗ «О техническом регулировании»;
11. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
12. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
13. Закон РФ от 21.07.1993 № 5485-I «О государственной тайне»;
14. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации»;
15. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
16. Указ Президента РФ от 07.08.2004 № 1013 «Вопросы Федеральной службы охраны Российской Федерации»;
17. Указ Президента РФ от 16.08.2004 № 1082 «Вопросы Министерства обороны Российской Федерации»;
18. Указ Президента РФ от 01.03.2011 № 248 «Вопросы Министерства внутренних дел Российской Федерации»;
19. Указ Президента РФ от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»;
20. Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационнотелекоммуникационных сетей международного информационного обмена»;
21. Указ Президента РФ от 11.03.2003 № 308 «О мерах по совершенствованию государственного управления в области безопасности Российской Федерации»;
22. Постановление Правительства РФ от 02.06.2008 № 418 «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации»;
23. Постановление Правительства РФ от 16.03.2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»;
24. Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

25. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
26. Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
27. Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»;
28. Постановление Правительства РФ от 08.08.2022 № 1393 «Об утверждении требований к автоматизированной информационной системе оформления воздушных перевозок, к базам данных, входящим в ее состав, к информационно-телекоммуникационной сети, обеспечивающей работу указанной автоматизированной информационной системы, к ее оператору, а также мер по защите информации, содержащейся в ней, и порядка ее функционирования и изменении и признании утратившими силу некоторых актов Правительства Российской Федерации»;
29. Постановление Правительства РФ от 18.05.2009 № 424 «Об особенностях подключения федеральных государственных информационных систем к информационнотелекоммуникационным сетям»;
30. Постановление Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации»;
31. Постановление Правительства РФ от 21.04.2010 № 266 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения и о внесении изменения в Положение о сертификации средств защиты информации»;
32. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
33. Постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
34. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
35. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

36. Приказ ФСБ РФ от 13.11.1999 № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия»;
37. Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с изменениями и дополнениями);
38. Приказ Федеральной службы по техническому и экспортному контролю от 03.04.2018 № 55 «Об утверждении Положения о системе сертификации средств защиты информации»
39. Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
40. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
41. Приказ Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;
42. Приказ Министерства труда и социальной защиты РФ от 09.08.2022 № 474н «Об утверждении профессионального стандарта «Специалист по технической защите информации»;
43. Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.);
44. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.);
45. Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.);
46. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.);
47. Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. решением Государственной технической комиссии при Президенте РФ от 25.07.1997 г.);
48. Руководящий документ «Защита информации. Специальные защитные знаки. Классификация и общие требования» (утв. решением Государственной технической комиссии при Президенте РФ от 25.07.1997 г.);
49. Руководящий документ «Средства защиты информации. Защита информации в контрольнокассовых машинах и автоматизированных кассовых системах.

Классификация контрольнокассовых машин автоматизированных кассовых систем и требования по защите информации»;
50. Руководящий документ. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (утв. решением Государственной технической комиссии при Президенте РФ от 04.06.1999 № 114);
51. Руководящий документ «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (введен в действие приказом Государственной технической комиссии при Президенте РФ от 19.06.2002 № 187);
52. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники;
53. Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. председателем Государственной технической комиссии при Президенте Российской Федерации 25.11.1994 г.);
54. ГОСТ Р 50752-95 «Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Методы испытаний».
55. Межгосударственный стандарт ГОСТ 30373-95/ГОСТ Р 50414-92 «Совместимость технических средств электромагнитная. Оборудование для испытаний. Камеры экранированные. Классы, основные параметры, технические требования и методы испытаний» (введен в действие постановлением Госстандарта РФ от 15.05.1996 № 308);
56. ГОСТ 29339-92 «Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники».
57. Защита интеллектуальной собственности: учебник / И. К. Ларионов, М. А. Гуреева, В. В. Овчинников [и др.] ; под ред. И. К. Ларионова, М. А. Гуреевой, В. В. Овчинникова. – 5-е изд., стер. – Москва: Дашков и К°, 2023. – 256 с. – (Учебные издания для бакалавров). – URL: https://biblioclub.ru/index.php?page=book&id=710103 – Библиогр. в кн. – ISBN 978-5-394- 05367-2.
58. Управление кадровой безопасностью организации: учебник для бакалавриата и магистратуры: / Ю. В. Долженкова, Е. В. Камнева, А. Л. Сафонов [и др.]; под ред. Ю. В. Долженковой; Финансовый университет при Правительстве Российской Федерации. – Москва: Прометей, 2022. – 286 с.: ил., табл., схем. –– URL: https://biblioclub.ru/index.php?page=book&id=700997. – Библиогр.: с. 245-256. – ISBN 978-5-00172-241-0.
59. Мансуров, Г. З. Право цифровой безопасности: учебник: / Г. З. Мансуров. – Москва: ДиректМедиа, 2022. – 148 с. – URL: https://biblioclub.ru/index.php?page=book&id=687364. – Библиогр. в кн. – ISBN 978-5-4499-3061-3. – DOI 10.23681/687364.
60. Основы информационной безопасности: учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев; Академия Следственного комитета Российской Федерации. – Москва: Юнити-Дана: Закон и право, 2018. – 287 с.: ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562348. – Библиогр. в кн. – ISBN 978-5-238-02857-6.
61. Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник / А. Г. Фабричнов, А. С. Дёмушкин, Т. В. Кондрашова, Н. Н.

Куняев. – Москва: Логос, 2011. – 452 с. – (Новая университетская библиотека). – URL: https://biblioclub.ru/index.php?page=book&id=84996. – ISBN 978-5-98704-541-1.
62. Прохорова, О. В. Информационная безопасность и защита информации: учебник: /О. В. Прохорова; Самарский государственный архитектурно-строительный университет. –Самара: Самарский государственный архитектурно-строительный университет, 2014. – 113с.: табл., схем., ил. –URL: https://biblioclub.ru/index.php?page=book&id=438331. – Библиогр.в кн. – ISBN 978-5-9585-0603-3.
63. Андруник, А. П. Кадровая безопасность: инновационные технологии управления персоналом: учебное пособие / А. П. Андруник, М. Н. Руденко, А. Е. Суглобов. – 4-е изд. – Москва: Дашков и К°, 2024. – 508 с.: табл., схем. – (Учебные издания для вузов). – URL: https://biblioclub.ru/index.php?page=book&id=709776. – Библиогр. в кн. – ISBN 978-5-394-05699-4.
64. Сидак, А. А. Информационная безопасность. Физические основы технических каналов утечки информации : учебное пособие : / А. А. Сидак, В. В. Василенко, С. В. Рыженко ;
65. Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова. – Москва: Директ-Медиа, 2022. – 128 с.: ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=694670. – Библиогр.: с. 117- 118. – ISBN 978-5-4499-3327-0. – DOI 10.23681/694670.
66. Великанова, С. С. Информационные ресурсы кадровой службы : учебное пособие : [12+] /С. С. Великанова. – Москва: Директ-Медиа, 2022. – 144 с.: ил., табл. – Режим доступа: поподписке. – URL: https://biblioclub.ru/index.php?page=book&id=683128. – Библиогр. в кн. –ISBN 978-5-4499-2892-4.
67. Аверченков, В. И. Служба защиты информации: организация и управление: учебное пособие: / В. И. Аверченков, М. Ю. Рытов. – 4-е изд., стер. – Москва: ФЛИНТА, 2021. – 186 с.: ил., схем. –URL: https://biblioclub.ru/index.php?page=book&id=93356. – Библиогр. в кн. – ISBN 978-5-9765-1271-9.
68. Корнилова, А. А. Защита персональных данных: учебное пособие: / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова; Башкирский государственный университет. – Уфа: Башкирский государственный университет, 2020. – 119 с.: ил., табл. – URL: https://biblioclub.ru/index.php?page=book&id=611314. – Библиогр. в кн.
69. Правовое регулирование информационных отношений в области государственной и коммерческой тайны, персональных данных: учебное пособие: / О. В. Ахрамеева, И. Ф. Дедюхина, О. В. Жданова [и др.]; Ставропольский государственный аграрный университет, Кафедра государственного и муниципального управления и права. – Ставрополь: Ставропольский государственный аграрный университет (СтГАУ), 2015. – 59 с. – URL: https://biblioclub.ru/index.php?page=book&id=438603.
70. Информационные технологии в юридической деятельности: учебное пособие /С. Я. Казанцев, Н. М. Дубинина, А. И. Уринцов [и др.] под ред. А. И. Уринцова. – 2-е изд.,перераб. и доп. – Москва: Юнити-Дана, 2020. – 353 с.: схем., табл, ил. – URL:https://biblioclub.ru/index.php?page=book&id=683023. – Библиогр.: с. 341. – ISBN 978-5-238-03242-9.
71. Конфиденциальное делопроизводство и защищенный электронный документооборот:учебник / А. Г. Фабричнов, А. С. Дёмушкин, Т. В. Кондрашова, Н. Н. Куняев. – Москва: Логос,2011. – 452 с. – (Новая университетская библиотека). – URL:https://biblioclub.ru/index.php?page=book&id=84996. – ISBN 978-5-98704-541-1.
72. Безопасность электронного документооборота: учебное пособие: / П. А. Тищенко,Ю. М. Казаков, Р. А. Филиппов [и др.]. – Москва; Берлин: Директ-Медиа, 2021. – 54 с. –Режим доступа: по подписке. – URL:

https://biblioclub.ru/index.php?page=book&id=602225. – Библиогр. в кн. – ISBN 978-5-4499-1928-1.

5. Контроль и оценивание результатов освоения образовательной программы

В соответствии с Законом Российской Федерации №273 «Об образовании», с учетом Приказ Минобрнауки Российской Федерации от 1 июля 2013 г. N 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам», итоговая аттестация обучающихся, завершающих обучение по дополнительной профессиональной программе профессиональной переподготовке, является обязательной.

Целью итоговой аттестации является установление уровня подготовки и освоения новых компетенций слушателя по дополнительной профессиональной программе профессиональной переподготовке.

Итоговая аттестация позволяет выявить и объективно оценить теоретическую и практическую подготовку слушателя.

Порядок проведения аттестационных испытаний определяется настоящей Программой и доводится до сведения слушателей перед началом курсов повышения квалификации.

Промежуточная аттестация проводится с целью выявления уровня освоения новых компетенций слушателя в процессе обучения по дополнительной профессиональной программе повышения квалификации.

Итоговая и промежуточная аттестация проводится в форме тестирования с использованием электронных образовательных технологий по принципу «зачет»/«не зачет».

Критерии оценки знаний слушателей:

- «Зачет»: 80% -100% -слушатель показал глубокие и всесторонние знания по выносимому на тестирование материалу в соответствии с учебной программой, владеет требованиями нормативных документов;

- «Незачет»: от 0% до 79% - слушатель показал незнание основных положений выносимого на тестирование материала; не знание требований нормативных документов; не в состоянии дать самостоятельный ответ на вопросы.

Прием итоговой и промежуточной аттестации может осуществляться одним преподавателем, имеющим соответствующую квалификацию.

После завершения промежуточной аттестации результаты вносятся в протокол аттестационной комиссии по обучению обучающихся.

После завершения итоговой тестирования результаты вносятся в протокол аттестационной комиссии по выпуску обучающихся.

Повторная сдача итоговой аттестации с целью повышения положительной оценки не допускается.

Обучающимся, не проходившим аттестационных испытаний по уважительной причине (по медицинским показаниям или в других исключительных случаях, документально подтвержденных), а также обучающимся получившим «незачет», предоставляется возможность пройти итоговую аттестацию повторно.

6. Форма документа, выдаваемого по результатам освоения программы

На основании решения аттестационной комиссии лицам, прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации

установленного образца по программе «Организация работы по защите персональных данных» объемом 72академических часа.