Автономная некоммерческая организация
дополнительного профессионального образования
«Межрегиональная академия строительного и промышленного комплекса»

УТВЕРЖДАЮ
Ректор АНО ДПО «МАСПК»
_____М.В. Маковский
«___» _____2020 г.

Дополнительная профессиональная программа
(повышение квалификации)

Информационная безопасность
(наименование программы)

РАССМОТРЕНО И ПРИНЯТО
учебно-методическим советом
протокол от 13.01.2020 г. № 1

Москва - 2020

Раздел 1. ХАРАКТЕРИСТИКА ПРОГРАММЫ

Цель программы: дополнительная профессиональная программа повышения квалификации направлена на совершенствование профессиональных компетенций слушателей в области информационной безопасности.

Категория слушателей: к освоению дополнительной профессиональной программы допускаются: лица, имеющие среднее профессиональное и (или) высшее образование

Трудоемкость программы: 72 академических часа (продолжительность академического часа не менее 40 минут)

Сроки освоения программы: 9 рабочих дней.

Форма обучения: заочная (с применением дистанционных образовательных технологий).

Режим занятий – определяется совместно с Заказчиком (не более 8 часов в день).

Планируемые результаты обучения

В результате изучения дисциплины слушатель должен:

Знать:

- средства и методы предотвращения и обнаружения вторжений;
- технические каналы утечки информации;
- возможности технических средств перехвата информации;
- способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;
- организацию защиты информации от утечки по техническим каналам на объектах информатизации

Уметь:

- пользоваться нормативными документами по противодействию технической разведке;
- оценивать качество готового программного обеспечения

Владеть:

- методами и средствами технической защиты информации;
- методами расчета и инструментального контроля показателей технической защиты информации

Совершенствуемые компетенции

№	Компетенция	Код компетенции
1	способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно управленческой и технической реализуемости и экономической целесообразности	ПК-4
2	способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов	ПК-6
3	способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия	ПК-9
4	способностью администрировать подсистемы информационной безопасности объекта	ПК-10
5	способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью	ПК-25
6	способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью	ПК-26

Раздел 2. СТРУКТУРА И СОДЕРЖАНИЕ КУРСА

Всего часов	Лекции	Практическая и самостоятельная работа	Форма контроля
72	**70**	**-**	**2**

2.1. Учебно-тематический план

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Форма контроля
			Лекции	Практика	
1	2	3	4	5	6
1.	**МОДУЛЬ 1. Теоретические и методологические вопросы организационно-правового обеспечения информационной безопасности**	**6**	**6**		
	1.1. Понятие информационной безопасности и ее место в системе национальной безопасности Российской Федерации 1.2. Особенности информационных правоотношений при построении информационного общества 1.3. Правовое регулирование информационной безопасности в системе российского информационного права 1.4. Проблемы методологии правового				

	обеспечения информационной безопасности				
2.	**МОДУЛЬ 2. Формирование правовых основ обеспечения информационной безопасности — реализация принципа верховенства права в глобальном информационном обществе**	**8**	**8**		
	2.1 Международные правовые акты в области обеспечения информационной безопасности 2.2. Зарубежный опыт правового обеспечения информационной безопасности 2.3. Продвижение российских инициатив в области обеспечения международной информационной безопасности				
3.	**МОДУЛЬ 3. Государственная политика Российской Федерации и национальные интересы в области обеспечения информационной безопасности**	**8**	**8**		
	3.1. Государственная политика Российской Федерации в области организационно-правового обеспечения информационной безопасности в условиях новых вызовов и угроз 3.2. Стратегические задачи и приоритетные направления правового регулирования в области обеспечения информационной безопасности в России 3.3 Организационное обеспечение информационной безопасности как составляющая реализации государственной политики в этой сфере				
4.	**МОДУЛЬ 4. Информационное противодействие**	**10**	**10**		
	4.1. Особенности современной информационной борьбы и обеспечение информационной безопасности 4.2. Конфликты и противоречия, связанные с правовым регулированием отношений в сети Интернет 4.3 Преступность в информационной сфере как угроза информационной безопасности в условиях глобализации				
5.	**МОДУЛЬ 5. Основные проблемы и пути совершенствования организационно-правового обеспечения информационной безопасности**	**12**	**12**		
	5.1 Правовые проблемы обеспечения национальной безопасности при построении информационного общества в России 5.2. Организационно-правовое обеспечение информационной безопасности субъектов Российской Федерации				

	5.3. Международное сотрудничество в области информационной безопасности в условиях глобализации 5.4. Приоритетные направления научных исследований в области организационно-правового обеспечения информационной безопасности				
6.	**МОДУЛЬ 6. Стандарты информационной безопасности**	**8**	**8**		
	6.1. Стандартизация информационной безопасности 6.2. Международные стандарты 6.3. Национальные стандарты российской федерации в области информационной безопасности 6.4. Руководящие документы ФСТЭК России 6.5. Защита и обработка конфиденциальных документов				
7.	**МОДУЛЬ 7. Уровни обеспечения информационной безопасности**	**10**	**10**		
	Раздел 1 Спецификации в области информационной безопасности 1.1 Оценочные стандарты и технические спецификации 1.2 Информационная безопасность распределенных систем **Раздел 2** Административный уровень информационной безопасности 2.1 Основные понятия административного уровня информационной безопасности 2.2 Политика безопасности 2.3 Программа безопасности 2.4 Синхронизация программы безопасности с жизненным циклом систем 2.5 Понятие об управлении рисками **Раздел 3** Процедурный уровень информационной безопасности 3.1. Основные классы мер процедурного уровня 3.2 Управление персоналом 3.3 Физическая защита 3.4 Поддержание работоспособности 3.5 Реагирование на нарушения режима безопасности 3.6 Планирование восстановительных работ **Раздел 4** Основные программно-технические меры обеспечения информационной безопасности 4.1 Основные понятия программно-технического уровня информационной безопасности 4.2 Особенности современных				

	информационных систем, существенные при обеспечении информационной безопасности 4.3 Архитектура системы безопасности				
8.	**МОДУЛЬ 8. Аудит информационной безопасности**	**8**	**8**		
	1.1 Особенности аудита информационной безопасности организаций, использующих аутсорсинг 1.2 Особенности аудита информационной безопасности в банковской системе Российской Федерации 1.3 Комплексное обследование информационной безопасности и оценивание результатов аудита				
ИТОГОВАЯ АТТЕСТАЦИЯ ПО КУРСУ		**2**		**2**	**Итоговое тестирование**
Всего часов:		**72**	**70**	**2**	

2.2. Сетевая форма обучения

Не предусмотрена.

Раздел 3. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Учебные дни	День 1	День 2	День 3	День 4	День 5
Кол-во часов	**8**	**8**	**8**	**8**	**8**
Вид занятий	Теоретическое обучение				
Учебные дни	День 6	День 7	День 8	День 9	День 9
Кол-во часов	**8**	**8**	**8**	**6**	**2**
Вид занятий	Теоретическое обучение				ИА (Тест)

Раздел 4. РАБОЧАЯ ПРОГРАММА

МОДУЛЬ 1. Теоретические и методологические вопросы организационно-правового обеспечения информационной безопасности

Понятие информационной безопасности и ее место в системе национальной безопасности Российской Федерации. Особенности информационных правоотношений при построении информационного общества. Правовое регулирование информационной безопасности в системе российского информационного права. Проблемы методологии правового обеспечения информационной безопасности

МОДУЛЬ 2. Формирование правовых основ обеспечения информационной безопасности — реализация принципа верховенства права в глобальном информационном обществе

Международные правовые акты в области обеспечения информационной безопасности. Зарубежный опыт правового обеспечения информационной безопасности. Продвижение российских инициатив в области обеспечения международной информационной безопасности

МОДУЛЬ 3. Государственная политика Российской Федерации и национальные интересы в области обеспечения информационной безопасности

Государственная политика Российской Федерации в области организационно-правового обеспечения информационной безопасности в условиях новых вызовов и угроз. Стратегические задачи и приоритетные направления правового регулирования в области обеспечения информационной безопасности в России. Организационное обеспечение информационной безопасности как составляющая реализации государственной политики в этой сфере

МОДУЛЬ 4. Информационное противодействие

Особенности современной информационной борьбы и обеспечение информационной безопасности. Конфликты и противоречия, связанные с правовым регулированием отношений в сети Интернет. Преступность в информационной сфере как угроза информационной безопасности в условиях глобализации

МОДУЛЬ 5. Основные проблемы и пути совершенствования организационно-правового обеспечения информационной безопасности

Правовые проблемы обеспечения национальной безопасности при построении информационного общества в России. Организационно-правовое обеспечение информационной безопасности субъектов Российской Федерации. Международное сотрудничество в области информационной безопасности в условиях глобализации. Приоритетные направления научных исследований в области организационно-правового обеспечения информационной безопасности

МОДУЛЬ 6. Стандарты информационной безопасности

Стандартизация информационной безопасности. Международные стандарты. Национальные стандарты российской федерации в области информационной безопасности. Руководящие документы ФСТЭК России. Защита и обработка конфиденциальных документов

МОДУЛЬ 7. Уровни обеспечения информационной безопасности

Раздел 1 Спецификации в области информационной безопасности

Оценочные стандарты и технические спецификации. Основные понятия. Механизмы безопасности. Классы безопасности. Информационная безопасность распределенных систем. Сетевые сервисы безопасности. Сетевые механизмы безопасности. Администрирование средств безопасности. Основные понятия. Функциональные требования. Требования доверия безопасности

Раздел 2 Административный уровень информационной безопасности

Основные понятия административного уровня информационной безопасности. Политика безопасности. Программа безопасности. Синхронизация программы безопасности с жизненным циклом систем. Понятие об управлении рисками

Раздел 3 Процедурный уровень информационной безопасности

Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ

Раздел 4 Основные программно-технические меры обеспечения информационной безопасности
Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные при обеспечении информационной безопасности. Архитектура системы безопасности

МОДУЛЬ 8. Аудит информационной безопасности
Особенности аудита информационной безопасности организаций, использующих аутсорсинг. Особенности аудита информационной безопасности в банковской системе Российской Федерации. Комплексное обследование информационной безопасности и оценивание результатов аудита

Раздел 5. ФОРМЫ АТТЕСТАЦИИ И ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Формы контроля, реализуемые в ходе освоения слушателем ДППК, направлены на установление соответствия результатов освоения дополнительной профессиональной программы.

Промежуточная аттестация программой не предусмотрена.

Итоговая аттестация: формой итоговой оценки результатов освоения дополнительной профессиональной программы повышения квалификации является тестирование.

Перечень вопросов, выносимых на тестирование, размещается в системе дистанционного обучения. Учет результатов освоения образовательной программы слушателем ведется в системе дистанционного обучения.

Критерии оценивания итоговой аттестации:

Критерии оценки (% правильных ответов по итоговому тесту)	**Оценка**
50% и выше	Зачтено
>49%	Не зачтено

Оценочные материалы по дополнительной профессиональной программе (итоговое тестирование):

1. Информационная безопасность, это:
а) сбор, обработка, хранение, поиск и распространение информации, а также образование организационного ресурса и формирование свободного доступа
б) теория, воспринимаемая человеком или специальными устройствами как отражение фактов материального или духовного мира в процессе коммуникации
в) практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации
г) процесс передачи части функций руководителя другим управляющим или сотрудникам для достижения конкретных целей организации

2. Основная задача информационной безопасности, это:

а) сбалансированная защита конфиденциальности, целостности и доступности данных, с учётом целесообразности применения и без какого-либо ущерба производительности организации
б) описание широкомасштабных намерений, которые должны быть реализованы в короткий срок и которые направлены на приведение в порядок в области защиты данных
в) последовательность шагов, ведущих к выполнению определенного программного обеспечения
г) программные объекты, имеющие способы реагировать на события сбалансированных интерпретаторов

3. Уровень гарантированности, это:

а) набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию
б) мера доверия, которая может быть оказана архитектуре и реализации информационной системы
в) активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия
г) допустимость выполнения субъектами

4. Аутентификация служит для:

а) повтора следующего сеанса связи
б) проверки подлинности
в) автоматизации информационного процесса
г) предоставления всех полномочий

5**. Конфиденциальность данных обеспечивает:**

а) защиту от аутентификации
б) защиту от несанкционированного получения информации
в) защиту с подтверждением подлинности источника данных
г) гарантию целостности данных

6. Электронная цифровая подпись, это:

а) текстовая или бинарная подпись разработчика конкретных данных
б) дополнительное симметричное шифрование данных
в) пароль для данных
г) результат преобразования хеш-функции от конкретных данных

7. Социальная защита, это:

а) программные комплексы и средства системы информации в информационных системах различного назначения и в основных средствах обработки данных
б) скремблирование телефонных переговоров, кодирование цифровой информации криптографическими методами, программные методы модификации информации
в) измерительные приборы и устройства, программно-аппаратные комплексы, предназначенные для выявления каналов утечки информации
г) роли, которые персонифицированы и за исполнение которых установлена ответственность существующих в организации ролей

8. Пассивное скрытие, это:

а) постоянная и эффективная техническая защита информационных ресурсов
б) оптимизация денежных расходов на организацию защиты информации
в) защита носителей информации от полного уничтожения

г) исключение или значительное затруднение обнаружение объектов

9. Маршрутизатор, это:

а) детектор, обеспечивающий распространение маршрутизации световых излучений в глобальной сети
б) устройство, обеспечивающее распределение маршрутов для пакетов данных обмена в глобальной сети
в) удаленное информационное разрушающее воздействие, осуществляемое по каналам связи
г) сетевая рабочая станция

10. Подсеть, это:

а) логическое объединение хостов маршрутизатором
б) физическое объединение хостов
в) сетевой компьютер
г) атакующая программа

11. Основная причина уязвимости хостов сети, это:

а) свободный доступ к информации по организации сетевого взаимодействия, протоколам и механизмам защит
б) совокупность хостов, являющихся частью глобальной сети, для которых маршрутизатором выделен одинаковый номер подсети
в) распределенные информационные систем, рабочих станций и вычислительных узлов, объединённых каналами связи
г) сложность организации защиты межсетевого взаимодействия

12. Возможность искажения информации может привести к:

а) выходу операционной системы из строя
б) контролю над информационным потоком между объектами системы
в) восстановлению данных системы
г) отказу сетевого оборудования

13. Удаленная атака по сети может классифицироваться как:

а) однонаправленная и четырех-направленная
б) двунаправленная и трех-направленная
в) с обратной связью и без обратной связи
г) только однонаправленная атака

14. Чтобы определить уязвимость расчетно-вычислительной сети необходимо:

а) перехватить пакет данных РВС
б) изучить логику работы РВС
в) установить базовые методы маршрутизации
г) реагировать на какие-либо изменения, происходящие на атакуемом объекте

15. Признак недостаточной идентификация или аутентификация объектов и субъектов системы, это:

а) внедрение в систему ложного объекта, выдающего себя за доверенный объект системы
б) возможность предоставления удаленного доступа
в) получение запроса на соединение сервера
г) способность сетевой ОС отвечать лишь на ограниченное число запросов

Раздел 6. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

6.1 Учебно-методическое обеспечение и информационное обеспечение программы

Основная литература

1) Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности, – СПб: СПбНИУИТМО, 2014. – 173с.

2) Макаренко С. И. Информационная безопасность: учебное пособие. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.: ил.

3) Морозов, А. В. Организационно-правовое обеспечение информационной безопасности: монография / А. В. Морозов, Т. А. Полякова; РПА Минюста России. — М.: РПА Минюста России, 2013. — 276 с. — 1 000 экз. — ISBN 978-5-89172-544-7

4) Нестеров С. А. Информационная безопасность и защита информации: Учеб. пособие. – СПб.: Изд-во Политехн. ун-та, 2009. – 126 с.

5) Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учебное пособие / Ю. Н. Сычев. - Москва: ФГБОУ ВО «РЭУ им. Г. В. Плеханова», 2017. - 207 с.

6) Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – СПб.: Питер, 2012 – 960 с.: ил. – ISBN 978-5459-000342-0

Дополнительная литература

1) Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.

2) Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.

3) Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография. / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ, 2015. - 239 с.

4) Конотопов, М.В. Информационная безопасность. Лабораторный практикум / М.В. Конотопов. - М.: КноРус, 2013. - 136 с.

5) Мельников, Д.А. Информационная безопасность открытых систем: учебник / Д.А. Мельников. - М.: Флинта, 2013. - 448 с.

6) Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 416 с.

7) Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на С. Вильямс. 2016. – 1024 с.

Нормативно-правовое обеспечение программы

1) Уголовный кодекс Российской Федерации

2) Федеральный закон N 63-ФЗ 2011 года “Об электронной подписи”

3) Федеральный закон N 65-ФЗ 2011 года “О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "Об электронной подписи"”

4) Федеральный закон N 149-ФЗ 2006 года “Об информации, информационных технологиях и о защите информации”

5) Федеральный закон N 184-ФЗ 2002 года “О техническом регулировании”

6) Федеральный закон N 5-ФЗ 1994 года “О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания”

7) Министерство юстиции Российской Федерации. Федеральная служба судебных приставов. от 1 июня 2015 года N 315 “Об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных в Федеральной службе судебных приставов и ее территориальных органах требованиям к защите

персональных данных, установленным Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора”

8) Распоряжение правительства Российской Федерации от 12 июля 2011 года N 1214-р «Об утверждении плана подготовки правовых актов в целях реализации федеральных законов "Об электронной подписи" и "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "Об электронной подписи"»

9) Указ президента Российской Федерации “О мерах по противодействию терроризму”

10) Указ президента Российской Федерации “О Национальном плане противодействия коррупции на 2012-2013 годы и внесении изменений в некоторые акты Президента Российской Федерации по вопросам противодействия коррупции”

11) Указ президента Российской Федерации N 260 2015 года “О некоторых вопросах информационной безопасности Российской Федерации”

12) Указ президента Российской Федерации N 31с 2013 года “О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации”

13) Указ президента Российской Федерации N 590 2011 года “Вопросы Совета Безопасности Российской Федерации”

14) Указ президента Российской Федерации N 849 2000 года “О полномочном представителе Президента Российской Федерации в федеральном округе” (с изменениями на 19 июля 2017 года)

15) Р 1323565.1.012-2017 Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

16) СТО БР ИББС-1.0-2014 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения

17) ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения

18) ГОСТ Р 1.0-2012 Стандартизация в Российской Федерации. Основные положения (с Изменением N 1)

19) ГОСТ Р 34.10-2012 Информационная технология (ИТ). Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

20) ГОСТ Р 34.11-2012 Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования

21) ГОСТ Р 50922-2006 Защита информации. Основные термины и определения

22) ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

23) ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

24) ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство

25) ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

26) ГОСТ 6.10.4-84 Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения

Нормативные документы ФСТЭК

1) Федеральная служба по техническому и экспортному контролю. приказ от «14» марта 2014 г. Москва № 31. «Об утверждении требований к обеспечению защиты

информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды .

2) Приказ ФСТЭК России №27 от 15.02.2017 "О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17".

3) Приказ ФСТЭК России № 21 от 18 февраля 2013 г. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Зарегистрирован в Министерстве Юстиции Российской Федерации 14 мая 2013 г. Регистрационный номер - 28375. Отменяет приказ ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных».

4) ПРИКАЗ 11 февраля 2013 г. N 17 "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"

5) Государственная Техническая Комиссия при Президенте Российской Федерации является основным государственным органом в России, курирующем вопросы защиты информации от НСД. Руководящие документы, Положения и Постановления Гостехкомиссии России формируют большую часть отечественной нормативной базы в области защиты информации.

6) Положение о государственном лицензировании деятельности в области защиты информации. Решение Гостехкомиссии России и ФАПСИ от 27 апреля 1994 года № 10 (с дополнениями от 24 июня 1997 года № 60)

7) Положение о лицензировании деятельности по технической защите конфиденциальной информации. Утверждено постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79

8) Положение о лицензировании деятельности по международному информационному обмену. Утверждено постановлением Правительства Российской Федерации от 3 июня 1998 г. № 564

9) Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608

10) Положение о сертификации средств защиты информации по требованиям безопасности информации. Утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995 г. № 199

11) Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.

12) Руководящий документ Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утвержденао решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

13) Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г.

14) Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

15) Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Классификация автоматизированных систем и требования по защите информации. Решение председателя Гостехкомиссии России от 30 марта 1992 года

16) Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники.Решение председателя Гостехкомиссии России от 30 марта 1992 года

17) Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 25 июля 1997 года

18) Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования. Решение председателя Гостехкомиссии России от 25 июля 1997 года

19) РД. СЗИ. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации. Сборник руководящих документов по ЗИ. Гостехкомиссия России, 1998 год

20) Руководящий документ. Средства защиты информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам. Гостехкомиссия России, 1998 год

21) Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Приказ председателя Гостехкомиссии России от 4 июня 1999 года № 114

22) Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности. Гостехкомиссия России, 2003 год

23) Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Приказ председателя Гостехкомиссии России от 19 июня 2002 года № 187

24) Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты. Гостехкомиссия России, 2003 год

25) Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты. Гостехкомиссия России, 2003 год

26) Руководство по разработке профилей защиты и заданий по безопасности. Гостехкомиссия России, 2003 год.

27) Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

28) Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г. Пометка «для служебного пользования» снята Решением ФСТЭК России от 16 ноября 2009 г

29) Приказ Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю от 31 августа 2010 г. N 416/489 г. Москва "Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования".

30) Кодекс этики и служебного поведения государственных гражданских служащих Федеральной службы по техническому и экспортному контролю (Утвержден приказом ФСТЭК России от «17 марта» марта 2011 г. № 138)

31) Информационное сообщение о работах в области 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

32) Информационное сообщение по вопросу необходимости получения лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации.

33) Методический документ ФСТЭК "Меры защиты информации в государственных информационных системах"

34) Проект методического документа ФСТЭК России "Меры защиты информации в государственных информационных системах". Версия 1.3.

35) Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00

36) Информационное сообщение ФСТЭК России от 7 апреля 2014 г. № 240/24/1208 “О применении сертифицированной по требованиям безопасности информации операционной системы Windows XP в условиях прекращения ее поддержки разработчиком”

37) Информационное сообщение Федеральной службы по техническому и экспортному контролю от 7 апреля 2014 г. № 240/24/1208 “О применении сертифицированной по требованиям безопасности информации операционной системы Windows XP в условиях прекращения ее поддержки разработчиком”.

38) Информационное сообщение ФСТЭК России от 24 декабря 2014 г. N 240/24/4918 «Об утверждении Требований к средствам контроля съемных машинных носителей информации»

39) В соответствии с подпунктом 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085, приказом ФСТЭК России от 28 июля 2014 г. N 87 (зарегистрирован Минюстом России 5 сентября 2014 г., регистрационный N 33994) утверждены Требования к средствам контроля съемных машинных носителей информации (далее – Требования), которые вступили в силу с 1 декабря 2014 г.

40) Методические документы ФСТЭК России "Профили защиты"

41) Профиль защиты (protection profile) - Независимая от реализации совокупность требований безопасности для некоторой категории изделий ИТ, отвечающая специфическим запросам потребителя (ГОСТ Р ИСО/МЭК 15408). Профиль защиты - это специальный нормативный документ представляющий собой совокупность задач защиты, функциональных требований, требований адекватности и их обоснование.

42) Информационное письмо ФСТЭК России "Об утверждении требований к системам обнаружения вторжений"

43) В соответствии с подпунктом 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085, приказом ФСТЭК России от 6 декабря 2011 г. N 638 (зарегистрирован Минюстом России 1 февраля 2012 г., рег. N 23088) утверждены Требования к системам обнаружения вторжений (далее - Требования), которые вступили в действие с 15 марта 2012 г.

44) Методические рекомендации по формированию аналитического прогноза по укомплектованию подразделений по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию иностранным техническим разведкам ...

45) Методические рекомендации по формированию аналитического прогноза по укомплектованию подразделений по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию иностранным техническим разведкам и технической защите информации подготовленными кадрами на заданный период. УТВЕРЖДЕНЫ первым заместителем директора ФСТЭК России 23 апреля 2011 г.

46) Информационное сообщение ФСТЭК России от 6 марта 2015 г. N 240/22/879 "О банке данных угроз безопасности информации"
47) Приказ ФСТЭК России от 18 февраля 2013 г. n 21 "об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

6.2. Материально-технические условия реализации программы.

Организация располагает материально-технической базой, обеспечивающей проведение всех видов подготовки, практической работы обучающихся, которые предусмотрены учебным планом, и соответствующей действующим санитарным и противопожарным правилам и нормам. Перечень материально-технического обеспечения включает в себя систему дистанционного обучения, в которой каждый слушатель имеет доступ к учебным курсам, а также – тестовым испытаниям и дополнительным материалам (видеотеке).

Обеспеченность слушателей учебной и учебно-методической литературой осуществляется путем доступа к ресурсам электронных библиотечных систем.

Реализация ДППК обеспечивается научно-педагогическими кадрами, имеющими высшее образование, соответствующее профилю преподаваемой дисциплины (модуля).