Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

Бурятский институт инфокоммуникаций (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет телекоммуникаций и информатики» в г. Улан-Удэ

УТВЕРЖДАЮ _____
Зам. директора по УНР
_____/Т.Г. Батурина/
«_____» _____ 2024 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА – ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Информационная безопасность телекоммуникационных систем»

Улан-Удэ 2024

Разработчик (составитель):

1. Свешников Игорь Вадимович, кандидат физико-математических наук, доцент, заведующий кафедрой информационной безопасности БИИК СибГУТИ

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ.....

1.1 Общие положения.....

1.2 Цель освоения и характеристика новой квалификации.....

1.3 Планируемые результаты обучения.....

1.4 Учебно-тематический план.....

1.5 Календарный учебный график.....

1.6 Рабочие программы дисциплин (модулей, разделов).....

1.7 Организационно-педагогические условия.....

1.8 Формы аттестации.....

2 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ.....

2.1 Текущий контроль.....

2.2 Промежуточная аттестация.....

2.3 Итоговая аттестация.....

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Общие положения

1.1.1. Нормативные правовые основания разработки программы

Нормативные правовые основания для разработки дополнительной профессиональной программы – программы повышения квалификации «Информационная безопасность телекоммуникационных систем» (далее – программа) составляют:

– Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

– Приказ Министерства образования и науки Российской Федерации от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам» (зарегистрирован в Министерстве юстиции Российской Федерации 20 августа 2013 г., регистрационный № 29444);

– Приказ Министерства науки и высшего образования Российской Федерации от 19 октября 2020 г. №1316 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности;

Программа разработана на основе профессиональных стандартов:

– профессиональный стандарт «Специалист по технической защите информации», утвержденный приказом Минтруда России от 1 ноября 2016 г. № 599н;

– профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденный приказом Минтруда России от 3 ноября 2016 г. № 608н;

– профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей», утвержденный приказом Минтруда России от 14 сентября 2022 г.№ 533н;

– профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержденный приказом Минтруда России от 14.09.2022 № 525н.

Программа разработана на основе требований:

– федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427;

– федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.02 Информационная безопасность телекоммуникационных систем, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. № 1458.

Методических рекомендаций по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации, утвержденных ФСТЭК России 16 апреля 2018 г.;

Методических рекомендаций-разъяснений по разработке дополнительных профессиональных программ на основе профессиональных стандартов (письмо Минобрнауки России от 22 апреля 2015 г.№ ВК-1032/06).

1.1.2. Требования к слушателям

а) категория слушателей: лица, имеющие среднее профессиональное и (или) высшее образование и лица, получающие среднее профессиональное и (или) высшее образование.

б) требования к уровню профессионального образования: к освоению программ допускаются лица, имеющие среднее профессиональное и (или) высшее образование и лица, получающие среднее профессиональное и (или) высшее образование.

1.1.3. Особенности адаптации образовательной программы для лиц с ограниченными возможностями здоровья

Разработка адаптированной образовательной программы для лиц с ОВЗ и/или инвалидностью или обновление уже существующей образовательной программы определяются индивидуальной программой реабилитации инвалида (при наличии), рекомендациями заключения ПМПК (при наличии) и осуществляются по заявлению слушателя (законного представителя).

1.1.4. Форма обучения: очная

1.1.5. Трудоемкость освоения: 144 академических часа, включая все виды контактной и самостоятельной работы слушателя.

1.1.6. Период освоения: 50 календарных дней.

1.1.7. Форма документа, выдаваемого по результатам освоения программы: лицам, успешно освоившим дополнительную профессиональную программу и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации установленного образца.

1.2. Цель освоения

Целью освоения дополнительной профессиональной программы «Информационная безопасность телекоммуникационных систем» являются совершенствование компетенции(ий) в области обеспечения информационной безопасности телекоммуникационных систем как на уровне абонентских сетей доступа и корпоративных сетей передачи данных организаций, так и на уровне местных и региональных сетей. Данная программа позволит слушателем повысить квалификацию в данной области и получить соответствующее удостоверение государственного образца.

1.3 Планируемые результаты обучения

Таблица 1 – Планируемые результаты обучения

Код и наименование компетенции	Показатели освоения компетенции		
	Знания	**Умения**	**Практический опыт (при наличии)**
ПК.1 Способен оценивать уровень безопасности телекоммуникационных (далее ТК) систем	З 1.1 Угрозы ИБ З 1.2 Требования по защите информации (далее ЗИ)	У 1.1 Проводить анализ угроз ИБ в телекоммуникационных сетях У 1.2 Разрабатывать предложения по	В 1.1 Проводить контрольные проверки работоспособности применяемых программно-

Код и наименование компетенции	Показатели освоения компетенции		
	Знания	Умения	Практический опыт (при наличии)
	З 1.3. Знать отечественный и зарубежный опыт по проблемам информационной безопасности телекоммуникационных систем	вопросам комплексного обеспечения информационной безопасности У 1.3 Использовать технические средства и способы защиты информации в телекоммуникационных системах	аппаратных средств ЗИ В 1.2 Проводить предпроектное обследование объекта защиты. В 1.3 Проводить оценку рисков нарушения информационной безопасности
ПК.2. Способен разрабатывать средства защиты информации	З 2.1. Порядок разработки политики безопасности, выбор методов и средств обеспечения информационной безопасности объектов информационно-телекоммуникационных систем; З 2.2 Порядок проверки работоспособности и эффективности применяемых программно-аппаратных (в том числе криптографических) и технических средств защиты информации телекоммуникационных средств и систем	У 2.1. Осуществлять рациональный выбор элементной базы при проектировании систем и средств защиты информации; У 2.2 Разрабатывать системы управления информационной безопасностью телекоммуникационных систем, в том числе выбор методов и разработку алгоритмов принятия решений	В 2.1. Разрабатывать технические средства защиты информации и контроля их эффективности от утечки за счет побочных электромагнитных излучений и наводок; В 2.2 Проводить аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации
ПК.3.1 Способен проводить мониторинг состояния и координировать устранение неисправностей	З 3.1 Документационное обеспечение эксплуатации защищенных телекоммуникационных сетей и систем;	У 3.1 Проводить мониторинг состояния ТК систем; У 3.2 Протоколировать работу	В 3.1 Способен проводить мониторинг состояния и координировать устранение неисправностей

Код и наименование компетенции	Показатели освоения компетенции		
	Знания	Умения	Практический опыт (при наличии)
телекоммуникационных систем	З 3.2 Инструментальный мониторинг защищенности телекоммуникационных систем	телекоммуникационного оборудования	телекоммуникационных систем В 3.2 Администрировать корпоративные сети

1.4. Учебно-тематический план

Таблица 2 – Учебно-тематический план

Наименование разделов (модулей), тем, видов аттестации	Трудоемкость, ак. час				Формы аттестации
	Итого	Виды занятий, в т.ч.		СР	
		Л	ПЗ, ЛР		
Модуль 1 Организационно-правовые основы технической защиты конфиденциальной информации (далее - ТЗКИ)	**16**	**4**	**8**	**4**	**зачет**
Тема 1.1 Цели и задачи ТЗКИ	6	2	-	4	-
Тема 1.2 Основы нормативного правового обеспечения ТЗКИ	8	2	6	-	-
Промежуточная аттестация	**2**	**-**	**2**	**-**	**зачет**
Модуль 2 Основы построения защищенных телекоммуникационных (далее ТК) систем и сетей	**16**	**6**	**10**	**-**	**зачет**
Тема 2.1 Сигналы электросвязи и принципы построения систем передачи	8	2	6	-	-
Тема 2.2 Принципы построения цифровых систем передачи	2	2	-	-	-
Тема 2.3 Вычислительные сети и системы передачи информации	4	2	2	-	-
Промежуточная аттестация	**2**	**-**	**2**	**-**	**зачет**
Модуль 3 Меры и средства ТЗКИ от несанкционированного доступа (далее НСД)	**20**	**4**	**12**	**4**	**зачет**
Тема 3.1 Угрозы безопасности информации, связанные с НСД	8	2	6	-	-
Тема 3.2 Меры и средства защиты информации от НСД	10	2	4	4	-
Промежуточная аттестация	**2**	**-**	**2**		**зачет**
Модуль 4 Аттестация объектов информатизации по требованиям безопасности информации	**20**	**4**	**14**	**2**	**зачет**

Наименование разделов (модулей), тем, видов аттестации	Трудоемкость, ак. час				Формы аттестации
	Итого	Виды занятий, в т.ч.		СР	
		Л	ПЗ, ЛР		
Тема 4.1 Организация аттестации объектов информатизации на соответствие требованиям безопасности информации	8	2	6	-	-
Тема 4.2 Организация и выполнение мероприятий по аттестации объектов информатизации по требованиям безопасности информации	10	2	6	2	-
Промежуточная аттестация	**2**		**2**		**зачет**
Модуль 5 Организация защиты конфиденциальной информации в инфокоммуникационных системах и сетях связи	**24**	**8**	**14**	**2**	**зачет**
Тема 5.1 Техническая защита информации в корпоративных сетях связи	12	4	8	-	-
Тема 5.2 Проектирование защищенных инфокоммуникационных систем и сетей связи	10	4	4	2	-
Промежуточная аттестация	**2**		**2**		**зачет**
Модуль 6 Программно-аппаратные комплексы обеспечения информационной безопасности	**24**	**6**	**16**	**2**	**зачет**
Тема 6.1 Современные технологии VPN. Система защиты информации ViPNet	12	4	8	-	-
Тема 6.2 Программно-аппаратный комплекс ViPNet xFirewall	10	2	6	2	-
Промежуточная аттестация	**2**	**-**	**2**	**-**	**зачет**
Модуль 7 Сетевые технологии высокоскоростной передачи данных в мультисервисных сетях	**20**	**6**	**14**	**-**	**зачет**
Тема 7.1 Сетевые технологии высокоскоростной передачи уровня LAN	12	4	8	-	-
Тема 7.2 Сетевые технологии высокоскоростной передачи уровней MAN и WAN	6	2	4	-	-
Промежуточная аттестация	**2**	**-**	**2**	**-**	**зачет**
Итоговая аттестация	**4**		**4**		**Итоговая аттестационная работа**
Всего ак. часов	**144**	**38**	**92**	**14**	**зачет**

1.5. Календарный учебный график

Таблица 3 – Календарный учебный график

Наименование разделов (модулей), тем, видов аттестации	**Количество дней / ак. час**																								
	Д 1	**Д 2**	**Д 3**	**Д 4**	**Д 5**	**Д 6**	**Д 7**	**Д 8**	**Д 9**	**Д 10**	**Д 11**	**Д 12**	**Д 13**	**Д 14**	**Д 15**	**Д 16**	**Д 17**	**Д 18**	**Д 19**	**Д 20**	**Д 21**	**Д 22**	**Д 23**	**Д 24**	**Итого**
Модуль 1 Организационно-правовые основы ТЗКИ	**4**	**4**	**4**	**4**																					**16**
Тема 1.1 Цели и задачи ТЗКИ	4	2																							6
Тема 1.2 Основы нормативного правового обеспечения ТЗКИ		2	4	2																					8
Промежуточная аттестация				2																					2
Модуль 2 Основы построения защищенных ТК систем и сетей					**4**			**4**	**4**	**4**															**16**
Тема 2.1 Сигналы электросвязи и принципы построения систем передачи					4			4																	8
Тема 2.2 Принципы построения цифровых систем передачи									2																2
Тема 2.3 Вычислительные сети и системы передачи информации									2	2															4
Промежуточная аттестация										2															2
Модуль 3 Меры и средства ТЗКИ от НСД											**4**	**4**			**4**	**4**	**4**								**20**
Тема 3.1 Угрозы безопасности информации, связанные с НСД											4	4													8
Тема 3.2 Меры и средства защиты информации от НСД															4	4	2								10
Промежуточная аттестация																	2								2

Наименование разделов (модулей), тем, видов аттестации	Количество дней / ак. час																								
	Д 1	Д 2	Д 3	Д 4	Д 5	Д 6	Д 7	Д 8	Д 9	Д 10	Д 11	Д 12	Д 13	Д 14	Д 15	Д 16	Д 17	Д 18	Д 19	Д 20	Д 21	Д 22	Д 23	Д 24	Итого
Модуль 4 Аттестация объектов информатизации по требованиям безопасности информации																		**4**	**4**			**4**	**4**	**4**	**20**
Тема 4.1 Организация аттестации объектов информатизации на соответствие требованиям безопасности информации																		4	4						8
Тема 4.2 Организация и выполнение мероприятий по аттестации объектов информатизации по требованиям безопасности информации																						4	4	2	10
Промежуточная аттестация																								2	2
Всего ак. часов	**4**	**4**	**4**	**4**	**4**			**4**	**4**	**4**	**4**	**4**			**4**	**4**	**4**	**4**	**4**			**4**	**4**	**4**	**72**

Наименование разделов (модулей), тем, видов аттестации	Количество дней / ак. час																								
	Д 25	Д 26	Д 27	Д 28	Д 29	Д 30	Д 31	Д 32	Д 33	Д 34	Д 35	Д 36	Д 37	Д 38	Д 39	Д 40	Д 41	Д 42	Д 43	Д 44	Д 45	Д 46	Д 47	Д 48	Д 49	Д 50	Итого
Модуль 5 Организация защиты конфиденциальной информации в инфокоммуникационных системах и сетях связи	**4**	**4**			**4**	**4**	**4**	**4**																			**24**
Тема 5.1 Техническая защита информации в корпоративных сетях связи	4	4			4																						12

Наименование разделов (модулей), тем, видов аттестации	Количество дней / ак. час																									
	Д 25	**Д 26**	**Д 27**	**Д 28**	**Д 29**	**Д 30**	**Д 31**	**Д 32**	**Д 33**	**Д 34**	**Д 35**	**Д 36**	**Д 37**	**Д 38**	**Д 39**	**Д 40**	**Д 41**	**Д 42**	**Д 43**	**Д 44**	**Д 45**	**Д 46**	**Д 47**	**Д 48**	**Д 49**	**Д 50**	**Итого**
Тема 5.2 Проектирование защищенных инфокоммуникационных систем и сетей связи						4	4	2																		10
Промежуточная аттестация								2																		2
Модуль 6 Программно-аппаратные комплексы обеспечения информационной безопасности									**4**			**4**	**4**	**4**	**4**	**4**										**24**
Тема 6.1 Современные технологии VPN. Система защиты информации ViPNet									4			4	4													12
Тема 6.2 Программно-аппаратный комплекс ViPNet xFirewall														4	4	2										10
Промежуточная аттестация																2										2
Модуль 7 Сетевые технологии высокоскоростной передачи данных в мультисервисных сетях																			**4**	**4**	**4**	**4**	**4**			**20**
Тема 7.1 Сетевые технологии высокоскоростной передачи уровня LAN																			4	4	4					**12**
Тема 7.2 Сетевые технологии высокоскоростной передачи уровней MAN и WAN																						4	2			**6**
Промежуточная аттестация																							2			**2**
Итоговая аттестация																									**4**	**4**
Всего ак. часов	**4**	**4**			**4**	**4**	**4**	**4**	**4**			**4**	**4**	**4**	**4**	**4**			**4**	**4**	**4**	**4**	**4**			**4**	**72**

1.6. Рабочая программа

Наименование тем	Виды учебных занятий, ак. час		Содержание
Модуль 1 Организационно-правовые основы ТЗКИ			
Тема 1.1 Цели и задачи ТЗКИ	Лекции	2	Основные термины и определения в области ТЗИ. Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в Российской Федерации. Цели и задачи ТЗКИ. Объекты информатизации: классификация и характеристика. Защищаемые информация и информационные ресурсы. Объекты защиты конфиденциальной информации. Перечень сведений конфиденциального характера, подлежащих защите. Угрозы безопасности конфиденциальной информации. Классификация технических каналов утечки информации (далее – ТКУИ). Классификация угроз безопасности информации, связанных с НСД. Модель угроз безопасности информации в заданных условиях функционирования объекта зашиты. Методы выявления и оценки возможности реализации угроз безопасности информации Информация как объект защиты. Цели и задачи ТЗКИ. Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в Российской Федерации;
	Самостоятельная работа	4	Государственные информационные ресурсы, негосударственные информационные ресурсы, находящиеся в ведении органов государственной власти и организаций.
Тема 1.2 Основы нормативного правового обеспечения ТЗКИ	Лекции	2	Нормативные правовые акты Российской Федерации. Нормативные правовые акты ФСТЭК России. Методические документы. Технические документы (документация). Плановые документы. Информационные документы. Документы в области технического регулирования и стандартизации. Система стандартов в области защиты информации. Стандарты Единой системы конструкторской документации (ЕСКД), Единой системы технологической документации (ЕСТД) и Единой системы программной документации (ЕСПД). Основы лицензирования деятельности по ТЗКИ, аттестации объектов информатизации по требованиям безопасности информации. Система сертификации средств защиты информации. Ответственность за правонарушения в области защиты информации. Требования по защите конфиденциальной информации на объекте информатизации (от утечки по техническим каналам, от НСД и специальных воздействий).

Наименование тем	Виды учебных занятий, ак. час		Содержание
			Особенности защиты персональных данных. Требования международных и национальных стандартов по защите информации
	Практическое занятие	6	Нормативные правовые акты и методические документы ФСТЭК России в области ТЗИ Стандарты ЕСКД, ЕСТД и ЕСПД Организационно-правовые основы лицензирования деятельности по ТЗКИ, аттестации объектов информатизации по требованиям безопасности информации Требования по ТЗКИ Подготовка документов для получения лицензии на проведение работ и оказания услуг по ТЗКИ
Промежуточная аттестация	Практическое занятие	2	
Модуль 2 Основы построения защищенных ТК систем и сетей			
Тема 2.1 Сигналы электросвязи и принципы построения систем передачи	Лекции	2	Введение. Краткий обзор истории развития средств инфокоммуникаций. Основные органы по разработке международных и национальных стандартов и директивных документов в области инфокоммуникаций. Основные понятия и определения. Общие данные о структуре инфокоммуникационных систем и ее основных элементов (источники и получатели сообщений, устройства преобразования информации, линии связи). Первичные сигналы электросвязи и каналы передачи. Сообщения и сигналы в инфокоммуникационных каналах связи. Виды сигналов. Характеристики сигналов. Каналы связи инфокоммуникационных систем. Структурная схема многоканальной системы передачи (МСП). Методы разделения канальных сигналов. Взаимные помехи между каналами
	Практическое занятие	6	Виды каналов и их классификация. Характеристики каналов связи. Принципы построения многоканальных систем передачи
Тема 2.2 Принципы построения цифровых систем передачи	Лекции	2	Основные принципы построения инфокоммуникационных сетей. Назначение и состав сетей электросвязи. Методы коммутации в сетях электросвязи. Структура сетей электросвязи. Принципы построения Взаимоувязанной сети связи Российской Федерации (ВСС РФ). Особенности построения вторичных телекоммуникационных сетей. Состав и назначение сетей телефонной связи. Состав и назначение телеграфных сетей. Сети передачи данных. Сети ЭВМ. Классификация и топология инфокоммуникационных сетей. Цифровые сети интегрального обслуживания. Построение сетей сотовой связи. Основы построения систем радиосвязи.

Наименование тем	Виды учебных занятий, ак. час		Содержание
			Современные системы и сети радиосвязи. Радиорелейные системы связи. Принципы построения и классификация. Спутниковые системы. Классификация спутниковых систем связи в зависимости от орбиты ИСЗ. Службы спутниковой связи. Основы построения систем мобильной радиосвязи. Основы построения волоконно-оптических систем передачи. Особенности построения волоконно-оптических цифровых систем передачи (ВОСП). Основные активные и пассивные компоненты ВОСП. ВОСП со спектральным разделением каналов. Оптические каналы передачи информации. Современные интерфейсы инфокоммуникационных сетей. Обобщенная структурная схема оптического линейного тракта. Принципы построения многоканальных систем передачи с частотным и временным разделением каналов
Тема 2.3 Вычислительные сети и системы передачи информации	Лекции	2	Вычислительные системы и системы передачи информации. Локальные и глобальные вычислительные сети и системы передачи информации. Модель взаимодействия открытых систем (OSI). Программное обеспечение, поддерживающее работу сети. Оборудование, предназначенное для объединения локальных вычислительных сетей. Технология управления взаимодействием в сети. Обобщенная структура и функции глобальных компьютерных сетей. Технология Ethernet, основные услуги и сервисы сети. Организация и сервис виртуальных частных сетей (VPN). Сети и средства связи: передатчики, приемники, источники излучения, модуляторы, демодуляторы, усилители. Основные типы и принцип работы сетей и средств связи. Радиорелейные линии и спутниковые системы связи Волоконно-оптические системы передачи информации. Структура сети GSM. Подсистема базовой станции, регистры HLRи VLR, центр коммутации подвижной связи, центр аутентификации и регистр идентификации оборудования. Системы связи, построенные с использованием технологии 3G и 4G. Основные сетевые компоненты. Телекоммуникационные системы. Понятие о цифровых системах передачи информации. Формирование группового сигнала. Синхронизация и регенерация (восстановление) цифровых сигналов. Синхронная цифровая иерархия. Асинхронный режим передачи. Сигналы PDHи SDH. Сети интегрального обслуживания. Виртуальные каналы в глобальных сетях, сети передачи данных на основе технологий X.25, FRAMERELAY, ATM. Протокол межсетевого взаимодействия IP. Адресная схема

Наименование тем	Виды учебных занятий, ак. час		Содержание
			протокола, маршрутизация, маска подсети, расширенный сетевой префикс. Протоколы транспортного уровня TCPи UDP. Протоколы маршрутизации в стеке TCP/IP: протокол OSPF, протоколы политики маршрутизации EGPи BGP, протоколы групповой маршрутизации MBONE, DVMRP, MOSPFи P1M. Услуги телефонной сети общего пользования. Протокол SIP. Мультисервисная сеть связи. Состав оборудования. Цифровые сети интегрального обслуживания (сети ISDN). Широкополосные цифровые сети интегрального обслуживания. Перспективы развития телекоммуникационных систем в России и за рубежом
	Практическое занятие	2	Системы связи, построенные с использованием технологии 3G и 4G. Модель взаимодействия открытых систем (OSI)
Промежуточная аттестация	Практическое занятие	2	
Модуль 3 Меры и средства ТЗКИ от НСД			
Тема 3.1 Угрозы безопасности информации, связанные с НСД	Лекции	2	Понятие и общая классификация угроз безопасности информации, связанных с НСД. Источники угроз безопасности информации. Модели угроз безопасности информации, связанных с НСД. Методы оценки угроз безопасности, выявления уязвимостей в автоматизированных (информационных) системах. Банк данных угроз безопасности информации, содержащий сведения об уязвимостях программного обеспечения, используемого в автоматизированных (информационных) системах. Описание уязвимостей программного обеспечения, включенных в базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах. Международный подход к выявлению и анализу уязвимостей информационных систем, базы данных, содержащие описание уязвимостей информационных систем, в том числе CVE. Общая система оценки уязвимостей информационных систем (стандарты CVSS)
	Практическое занятие	6	Методы выявления уязвимостей информационных систем. Порядок и содержание работ по анализу уязвимостей программного обеспечения информационных систем, в том числе средств защиты информации информационных систем
Тема 3.2 Меры и средства защиты информации от НСД	Лекции	2	Общая характеристика и классификация мер и средств защиты информации от НСД. Требования к мерам защиты информации от НСД, реализуемым в автоматизированной (информационной) системе. Меры защиты информации от НСД. Средства защиты информации от НСД.

Наименование тем	Виды учебных занятий, ак. час		Содержание
			Межсетевые экраны, требования к ним и способы применения. Системы обнаружения вторжений, требования к ним и способы применения. Средства антивирусной защиты, требования к ним и способы применения. Специальные программно-аппаратные и программные комплексы доверенной загрузки и разграничения контроля доступа. Средства регистрации и учета. Средства (механизмы) обеспечения целостности информации. Криптографические средства защиты информации. Перспективные технологии биометрической аутентификации. DLP-системы, их возможности и перспективы применения. Перспективные технологии биометрической аутентификации. Системы предотвращения утечки данных, их возможности и перспективы применения Установка, настройка, эксплуатация и техническое обслуживание средств защиты информации от НСД. Мероприятия по физической защите объекта информатизации и отдельных технических средств, исключающих НСД к техническим средствам, их хищение и нарушение работоспособности
	Практическое занятие	4	Классификация мер и средств защиты информации от НСД (управление доступом; регистрация и учет; обеспечение целостности; антивирусная защита; межсетевое экранирование и сегментирование сетей; анализ защищенности и обнаружение вторжений и т.д.)
	Самостоятельная работа	4	Контроль сетевой безопасности (системы обнаружения вторжений и анализа защищенности, сетевые сканеры)
Промежуточная аттестация	Практическое занятие	2	
Модуль 4 Аттестация объектов информатизации по требованиям безопасности информации			

Наименование тем	Виды учебных занятий, ак. час		Содержание
Тема 4.1 Организация аттестации объектов информатизации на соответствие требованиям безопасности информации	Лекции	2	Организационно-правовые основы системы аттестации объектов информатизации по требованиям безопасности информации. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации (далее - система аттестации), как составной части единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации. Цели и виды аттестации объектов информатизации на соответствие требованиям безопасности информации. Участники аттестации и их полномочия (компетенции). Задачи, функции, права и обязанности органов по аттестации. Требования к органам по аттестации объектов информатизации. Деятельность аттестационных комиссий. Сводный реестр сертифицированной продукции, используемой в целях защиты информации на аттестованных объектах информатизации. Государственный контроль (надзор) за соблюдением порядка аттестации и эксплуатацией аттестованных объектов информатизации
	Практическое занятие	6	Состав и содержание документов, разрабатываемых для проведения аттестации и по результатам аттестации объекта информатизации. Программа и методики аттестационных испытаний объектов информатизации. Аттестат соответствия

Наименование тем	Виды учебных занятий, ак. час		Содержание
Тема 4.2 Организация и выполнение мероприятий по аттестации объектов информатизации по требованиям безопасности информации	Лекции	2	Основные мероприятия по проведению аттестации объектов информатизации на соответствие требованиям безопасности информации (подача и рассмотрение заявки на аттестацию объектов информатизации; предварительное ознакомление с аттестуемым объектом информатизации; разработка программ и методик аттестационных испытаний; проведение аттестационных испытаний объектов информатизации; оформление, регистрация и выдача аттестата соответствия). Требования к разработке, структуре, оформлению и утверждению программ и методик аттестационных испытаний объектов информатизации (требования к содержанию программ и методик аттестационных испытаний автоматизированных систем, защищаемых помещений). Требования обеспечения защиты конфиденциальной информации при проведении аттестации объектов информатизации. Методы проверки и испытаний, применяемые при проведении аттестационных испытаний (экспертно-документальный метод; измерение и оценка уровней ПЭМИН для отдельных технических средств автоматизированной системы и каналов утечки информации; проверка функций или комплекса функций защиты информации от НСД с помощью тестирующих средств, а также путем пробного пуска средств защиты информации от НСД и наблюдения за их выполнением; попытки «взлома систем защиты информации»). Разработка заключения и протоколов испытаний по результатам аттестации объектов информатизации. Оформление, регистрация и выдача «Аттестата соответствия». Порядок рассмотрения апелляций. Ввод в действие и эксплуатация аттестованных по требованиям безопасности информации объектов информатизации. Состав и содержание документов, разрабатываемых для проведения аттестации и по результатам аттестации объектов информатизации. Вывод из эксплуатации аттестованных по требованиям безопасности информации объектов информатизации
	Практическое занятие	6	Состав и содержание документов, разрабатываемых для проведения аттестации и по результатам аттестации объекта информатизации. Программа и методики аттестационных испытаний объектов информатизации. Аттестат соответствия
	Самостоятельная работа	2	Разработка программы аттестационных испытаний объектов информатизации
Промежуточная аттестация	Практическое занятие	2	
Модуль 5 Организация защиты конфиденциальной информации в инфокоммуникационных системах и сетях связи			
	Лекции	4	Методология обеспечения безопасности систем и сетей электросвязи. Постоянный аудит сетей связи

Наименование тем	Виды учебных занятий, ак. час		Содержание
Тема 5.1 Техническая защита информации в корпоративных сетях связи			с целью выявления уязвимостей и возможных угроз как один из обязательных элементов задачи обеспечения информационной безопасности. Мониторинг функционирования, обнаружение атак и принятие адекватных мер противодействия. Средства обеспечения и управления защищенностью средств связи сетей электросвязи (далее – СССЭ). Комплексные системы обеспечения информационной безопасности. Управление персоналом для обеспечения информационной безопасности как приоритетное направление деятельности. Подбор кадров, обучение и мотивация, контроль за соблюдением законов, должностных инструкций и правил
	Практическое занятие	8	Установка и начальная настройка беспроводного роутера MikroTik
Тема 5.2 Проектирование защищенных инфокоммуникационных систем и сетей связи	Лекции	4	Управление рисками в сфере информационной безопасности как одно из направлений бизнес-стратегии. Средства обеспечения и управления защищенностью СССЭ. Комплексные системы обеспечения информационной безопасности
	Практическое занятие	4	Организация защищенного туннельного соединения
	Самостоятельная работа	2	Стандарты информационной безопасности. Управление рисками в сфере информационной безопасности как одно из направлений бизнес-стратегии
Промежуточная аттестация	Практическое занятие	2	
Модуль 6 Программно-аппаратные комплексы обеспечения информационной безопасности			
Тема 6.1 Современные технологии VPN. Система защиты информации ViPNet	Лекции	4	Введение в технологию ViPNet VPN Компоненты управления сети ViPNet Клиентские продукты ViPNet Серверные продукты ViPNet Ключевая структура сети ViPNet. Формирование и управление ключевой системой
	Практическое занятие	8	Работа с журналами ПАК ViPNet xFirewall. Мониторинг ViPNet xFirewall
Тема 6.2 Программно-аппаратный комплекс ViPNet xFirewall	Лекции	2	Введение в технологию ViPNet xFirewall Компоненты управления сети ViPNet Особенности криптосистемы и ключевой структуры ViPNet Шлюзы безопасности ViPNet Защита АРМ пользователя с помощью ПО ViPNet Client 4U Технология ViPNet xFirewall Сценарии использования ПАК xFirewall Мониторинг состояния ViPNet xFirewall и просмотр журнала IP-пакетов

Наименование тем	Виды учебных занятий, ак. час		Содержание
	Практическое занятие	6	Настройка работы ViPNet xFirewall в качестве межсетевого экрана.
	Самостоятельная работа	2	Инсталляция и настройка (демо-версия) координатора ViPNet
Промежуточная аттестация	Практическое занятие	2	
Модуль 7 Сетевые технологии высокоскоростной передачи данных в мультисервисных сетях			
Тема 7.1 Сетевые технологии высокоскоростной передачи данных уровня LAN	Лекции	4	Вводные положения. История возникновения высокоскоростных сетевых технологий. Протоколы и стандарты. Стандартизирующие организации. Кодирование данных для высокоскоростных сервисов передачи данных. Мультиплексирование данных. Технологии мультиплексирования в современных сервисах ИС. Среды передачи для высокоскоростных сетевых технологий. Спецификации физического и канального уровня модели OSI. Модель 1EEE. Особенности реализация технологий 100 Base/1000 Base/10 Gbase Ethernet. Сервис MetroEthernet.
	Практическое занятие	8	Топологии сетевых систем и методы доступа в канал Передача голосовой и видеоинформации в сети Интернет
Тема 7.2 Сетевые технологии высокоскоростной передачи данных уровней MAN и WAN	Лекции	2	Принципы маршрутизации. Протоколы маршрутизации. Основы организации маршрутизации в операционных системах Windows, Linux. Организация маршрутизации на коммутаторах Cisco. Технологии передачи PDH, SDH, xWDM, MPLS/
	Практическое занятие	4	Проверка работоспособности сети
Промежуточная аттестация	Практическое занятие	2	

1.7. Организационно-педагогические условия

Реализация программы осуществляется в соответствии с требованиями законодательства Российской Федерации в области образования, нормативными правовыми актами, регламентирующими данное направление деятельности.

1.7.1. Требования к квалификации педагогических кадров

Реализация программы обеспечивается педагогическими работниками, а также лицами, привлекаемыми к реализации программы на иных условиях. Ква-

лификация педагогических работников должна отвечать квалификационным требованиям, указанным в квалификационных справочниках, и (или) профессиональных стандартах (при наличии).

1.7.2. Требования к материально-техническому обеспечению

Материально-техническое обеспечение (далее – МТО) необходимо для проведения всех видов учебных занятий и аттестации, предусмотренных учебным планом по программе, и соответствует действующим санитарным и гигиеническим нормам и правилам.

МТО содержит специальные помещения: учебные аудитории для проведения лекций, практических (семинарских) занятий, лабораторных работ, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы, итоговой аттестации (в соответствии с утвержденным расписанием учебных занятий). Специальные помещения укомплектованы специализированной мебелью, оборудованием, расходными материалами, программным обеспечением, техническими средствами обучения и иными средствами, служащими для представления учебной информации слушателям.

При реализации программы с использованием дистанционных образовательных технологий и (или) электронного обучения образовательная организация обеспечивает функционирование информационно-образовательной среды, включающей в себя электронные информационные ресурсы, электронные образовательные ресурсы, совокупность информационных технологий, телекоммуникационных технологий, соответствующих технологических средств и обеспечивающую освоение слушателями образовательных программ полностью или частично независимо от места нахождения слушателей: каналы связи, компьютерное оборудование, периферийное оборудование, программное обеспечение.

Код и наименование компетенции	**Материально-техническое обеспечение, необходимое для освоения ПК**
ПК.1 Способен оценивать уровень безопасности телекоммуникационных	Учебная аудитория для лекционных занятий оснащается универсальными техническими средствами обеспечения учебного процесса в составе: мультимедийного персонального компьютера (ноутбука) (с

Код и наименование компетенции	Материально-техническое обеспечение, необходимое для освоения ПК
систем	приводом лазерных дисков типа DVD-RW, звуковым сопровождением и т.п.); мультимедийного проектора с дистанционным управлением. Учебная аудитория для практических и самостоятельных занятий оснащается мультимедийным персональным компьютером (ноутбуком) преподавателя (сервером) и пользовательскими терминалами по числу обучающихся, объединенных локальной сетью («компьютерный» класс). Для проведения лабораторных работ и практических занятий используется специализированная лаборатория (№110 информационной безопасности), оборудованная средствами вычислительной техники (12 ЭВМ), локальной вычислительной сетью с подключением к сети Internet, беспроводное сетевое оборудование (маршрутизаторы MikroTik – 7 шт.), средства доверенной загрузки ОС – Соболь, криптомаршрутизатор IPC-100 – 1 шт., специализированное ПО Инфотекс.
ПК.2. Способен разрабатывать средства защиты информации	Используется специализированная лаборатория, оснащенная учебными лабораторными комплексами для обеспечения исследований специального программного обеспечения и аппаратного средства защиты конфиденциальной информации в составе: средства защиты информации от НСД; программно-аппаратный комплекс доверенной загрузки Соболь и др.; антивирусные пакеты Kaspersky; межсетевые экраны Cisco ASA-SSL-5000; контрольно-измерительное и испытательное оборудование: генераторы шумовых сигналов, вид шумового сигнала: «белый шум» (с нормальным распределением плотности вероятности мгновенных значений); хаотическая импульсная последовательность. Диапазон частот 175...5600 Гц; низкочастотные генераторы сигналов, диапазон частот 175...5600 Гц, выходное напряжение не менее 5 В; усилители мощности, диапазон частот 175...5600 Гц, выходная мощность не менее 10 Вт; акустические излучатели, диапазон воспроизводимых частот175...5600 Гц. Уровень звукового давления на расстоянии 1 м от излучателя в свободном поле не менее 95 Дб. Неравномерность АЧХ не более ±6 Дб; измерители шума и вибраций (шумомеры), диапазон частот175...5600 Гц, пределы измерения уровней сигналов 25 - 120 дБ, класс точности не ниже 2-го; селективные микровольтметры, диапазон частот 175...5600 Гц, погрешность измерения не более ±15 %; измерительные приемники (анализаторами спектра), диапазон измеряемых параметров 9 кГц - 1000 МГц, погрешность измерения не более 2 Дб; селективные нановольтметры, диапазон частот 175...5600Гц, погрешность измерения не более ±15 %; измерительные микрофоны, диапазон частот 175...5600Гц, чувствительность не хуже 10 мВ/Па, неравномерность АЧХ не более ±1 дБ;

Код и наименование компетенции	Материально-техническое обеспечение, необходимое для освоения ПК
	измерительные антенны, диапазон измеряемых частот: по магнитной составляющей 9 кГц...30 МГц; по электрической составляющей 9 кГц... 1000 МГц, погрешность измерения не более ±2 дБ; вибродатчики (акселерометры), диапазон частот175... 5600 Гц, чувствительность не хуже 1мВ/мс"', неравномерность АЧХ не более 10 %; измерительные пробники - диапазон измеряемых параметров 9кГц... 300 МГц; полосовые октавные фильтры со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц, диапазон частот 175...5600 Гц, номинальное ослабление в полосе пропускания фильтра 0 дБ, класс точности 1-й или 2-й, АЧХ в соответствии с ГОСТ 17168-82
ПК.3 Способен проводить мониторинг состояния и координировать устранение неисправностей телекоммуникационных систем	Учебная аудитория для лекционных занятий оснащается универсальными техническими средствами обеспечения учебного процесса в составе: мультимедийного персонального компьютера (ноутбука) (с приводом лазерных дисков типа DVD-RW, звуковым сопровождением и т.п.); мультимедийного проектора с дистанционным управлением. Учебная аудитория для практических и самостоятельных занятий оснащается мультимедийным персональным компьютером (ноутбуком)преподавателя (сервером) и пользовательскими терминалами по числу обучающихся, объединенных локальной сетью («компьютерный» класс) с наличием средств создания модели разграничения доступа; программа контроля полномочий доступа к информационным ресурсам; программа фиксации и контроля исходного состояния программного комплекса Windows Defender, Windows Security; программа поиска и гарантированного уничтожения информации на дисках; система обнаружения вторжений на основе искусственных нейронных сетей и анализа защищенности; сканеры безопасности

1.7.3. Требования к информационному и учебно-методическому обеспечению

Для реализации программы используются учебно-методическая документация, нормативные правовые акты, нормативная техническая документация, иная документация, учебная литература и иные издания, информационные ресурсы.

Таблица 4 – Учебно-методическая документация, нормативные правовые акты, нормативная техническая документация, иная документация, учебная литература и иные издания, информационные ресурсы

1. **Нормативные правовые акты, иная документация**

1.1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
1.2. Федеральный закон от 27 июля 2006 г. №. 152-ФЗ «О персональных данных».
1.3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
1.4. Федеральный закон от 4 мая 2011г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
1.5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
1.6. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
1.7. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
1.8. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
1.9. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
1.10. Положение о лицензировании деятельности по технической защите конфиденциальной информации. Утверждено постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 (в ред. постановления Правительства Российской Федерации от 15 июня 2016 г. № 541).
1.11. Положение о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации. Утверждено постановлением Правительства Российской Федерации от 3 марта 2012 г. 171 (в ред. постановления Правительства Российской Федерации от 15 июня 2016 г. №541).
1.12. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г.№ 608.
1.13. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.
1.14. Пособие по организации технической защиты информации, составляющей коммерческую тайну. Утверждено ФСТЭК России 25 декабря 2006 г.
1.15. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
1.16. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119
1.17. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
1.18. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 17 июля 2017 г. № 134.
1.19. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 17 июля 2017 г. № 133.

1.20. Специальные требования и рекомендации по защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

1.21. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

1.22. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

1.23. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам антивирусной защиты). Утверждены приказом ФСТЭК России от 20 марта 2012 г. №28.

1.24. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам доверенной загрузки). Утверждены приказом ФСТЭК России от 27 сентября 2013 г. № 119.

1.25. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам контроля съемных машинных носителей информации). Утверждены приказом ФСТЭК России от 28 июля 2014 г. № 87.

1.26. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

1.27. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

1.28. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден Гостехкомиссией России, 1992.

1.29. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

1.30. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утвержден Гостехкомиссией России, 1992.

1.31. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден приказом председателя Гостехкомиссии России от 4 июня 1999 г. № 114.

1.32. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода- вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

1.33. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утвержден Гостехкомиссией России, 1992.

1.34. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден Гостехкомиссией России, 1992.
1.35. Положение о системе сертификации средств защиты информации. Утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55.
1.36. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
1.37. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
1.38. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
1.39. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
1.40. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
1.41. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
1.42. ГОСТ РО 0043-003-2012 Защита информации. Аттестация объектов информатизации. Общие положения. Росстандарт, 2012.
1.43. ГОСТ РО 0043-004-2013 Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний. Госстандарт, 2013.
1.44. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.
1.45. ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России, 1998.
1.46. ГОСТ Р 51241-98 Защита информации. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. Госстандарт России, 1998.
1.47. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
1.48. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
1.49. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
1.50. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC15408-2:2008). Росстандарт, 2013.
1.51. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности (прямое применение ISO/IEC15408-3:2008). Росстандарт, 2013.
1.52. ГОСТ Р ИСО/МЭК 27000-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Госстандарт, 2021.

1.53. ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (на основе прямого применения международного стандарта ИСО/МЭК 27001:2005). Госстандарт, 2021

1.54. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Росстандарт, 2012.

1.55. ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по реализации системы менеджмента информационной безопасности. Росстандарт, 2012.

1.56. ГОСТ 34.602-2020 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. Госстандарт, 2021.

1.57. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.

1.58. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

1.59. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

1.60. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

1.61. Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи (МД по ТЗИ ВОСП-К). Утвержден приказом ФСТЭК России от 15 марта 2012 г. №27.

1.62. Временная методика оценки защищенности информации ограниченного доступа, обрабатываемой техническими средствами и системами с элементами беспроводных технологий, от утечки по каналу побочных электромагнитных излучений и наводок. Утверждена ФСТЭК России 21 декабря 2007 г.

1.63. Перечень технической и технологической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79. Утвержден ФСТЭК России 12 августа 2020 г.;

1.64. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

1.65. Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий. Утверждены приказом ФСТЭК России от 2 июня 2020 г. № 76.

1.66. Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении. Утверждена ФСТЭК России 25 декабря 2020 г.

1.67. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.

1.68. Требования по безопасности информации к средствам обеспечения безопасной дистанционной работы в информационных (автоматизированных) системах. Утверждены приказом ФСТЭК России от 16 февраля 2021 г. № 32.

1.69. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну. Утвержден приказом ФСТЭК России от 29 апреля 2021 г. № 77.

2. Основная литература

2.1. Новиков В.К. Организационное и правовое обеспечение информационной безопасности. В 2-х ч. 4.1. Правовое обеспечение информационной безопасности: учеб, пособие. - М.: МИЭТ, 2013. - 184 с.

2.2. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х ч. Ч. 2. Организационное обеспечение информационной безопасности: учеб, пособие. - М.: МИЭТ, 2013. - 172 с.

2.3. Организационно-правовое обеспечение информационной безопасности: учеб, пособие. А.А. Стрельцов, В.С. Горбатов, Т.А. Полякова и др. / под ред. А.А. Стрельцова. - М.: Академия, 2008. - 256 с.

2.4. Семкин С.Н., Семкин А.Н. Основы правового обеспечения защиты информации: учеб, пособие для вузов. - М.: Горячая линия - Телеком, 2008.

2.5. Правовой режим лицензирования и сертификации в сфере информационной безопасности: учеб, пособие / Ю.Ю. Коваленко. - М.: Горячая линия - Телеком, 2012;

2.6. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. - Минск, 2005.

2.7. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

2.8. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

2.9. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

2.10. Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи (МД по ТЗИ ВОСП-К). Утвержден приказом ФСТЭК России от 15 марта 2012 г. №27.

2.11. Временная методика оценки защищенности информации ограниченного доступа, обрабатываемой техническими средствами и системами с элементами беспроводных технологий, от утечки по каналу побочных электромагнитных излучений и наводок. Утверждена ФСТЭК России 21 декабря 2007 г.

2.12. Перечень технической и технологической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79. Утвержден ФСТЭК России 12 августа 2020 г.;

2.13. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

2.14. Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий. Утверждены приказом ФСТЭК России от 2 июня 2020 г. № 76.

2.15. Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении. Утверждена ФСТЭК России 25 декабря 2020 г.

2.16. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.
2.17. Требования по безопасности информации к средствам обеспечения безопасной дистанционной работы в информационных (автоматизированных) системах. Утверждены приказом ФСТЭК России от 16 февраля 2021 г. № 32.

2.18. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну. Утвержден приказом ФСТЭК России от 29 апреля 2021 г. № 77.
2.19. Язов Ю.К., Соловьев С.В. Защита информации в информационных системах от несанкционированного доступа: пособие. - Воронеж: Кварта, 2015.-440 с.
2.20. Программно-аппаратная защита информации: учеб, пособие / П.Б. Хорев. - М.: Форум, 2012. - 352 с.
2.21. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства: учеб, пособие / В.Ф. Шаньгин. - М: ДМК Пресс, 2008. - 544 с.

3. Дополнительная литература

3.1. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. - Минск, 2005.
3.2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
3.3. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.
3.4. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
3.5. Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи (МД по ТЗИ ВОСП-К). Утвержден приказом ФСТЭК России от 15 марта 2012 г. №27.
3.6. Временная методика оценки защищенности информации ограниченного доступа, обрабатываемой техническими средствами и системами с элементами беспроводных технологий, от утечки по каналу побочных электромагнитных излучений и наводок. Утверждена ФСТЭК России 21 декабря 2007 г.
3.7. Перечень технической и технологической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79. Утвержден ФСТЭК России 12 августа 2020 г.

4. Интернет-ресурсы

4.1. Правовые справочно-поисковые системы («Гарант», «Консультант Плюс»), www.fstec.ru, www.gost.ru/wps/portal/tk362, bdu.fstec.ru.»

5. Электронно-библиотечная система

5.1 Базы данных, информационно-справочные и поисковые системы: http://parallel.ru - Информационно-аналитический центр по параллельным вычислениям, http://gridclub.ru - Интернет-портал по грид-технологиям.

1.7.4. Общие требования к организации учебного процесса

Общие требования к организации учебного процесса определяются локальными нормативными актами образовательной организации.

1.8. Формы аттестации

Оценка качества освоения программы осуществляется в форме текущего контроля успеваемости, промежуточной аттестации (при наличии – в соответствии с учебно-тематическим планом и рабочей программой) и итоговой аттестации слушателей.

1.8.1. Текущий контроль успеваемости

В соответствии с учебно-тематическим планом и рабочей программой.

1.8.2. Промежуточная аттестация

В соответствии с учебно-тематическим планом и рабочей программой.

1.8.3. Итоговая аттестация

Освоение программы завершается итоговой аттестацией. Итоговая аттестация проводится на основе принципов объективности и независимости оценки качества подготовки слушателей. Итоговая аттестация является обязательной для слушателей.

Итоговая аттестация проводится в форме защиты итоговой аттестационной работы (ИАР).

К итоговой аттестации допускаются слушатели, не имеющие академической задолженности и в полном объеме выполнившие учебно-тематический план программы. Порядок прохождения итоговой аттестации определяется локальными нормативными образовательной организации.

2. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Оценочные материалы обеспечивают проверку достижения планируемых результатов обучения по программе и используются в процедуре текущего контроля успеваемости, промежуточной аттестации (при наличии) и итоговой аттестации.

2.1. Текущий контроль

Текущий контроль знаний проводится в формах, предусмотренных учебным планом.

Текущий контроль предназначен для проверки хода и качества формирования компетенций, стимулирования учебной работы обучаемых и совершенствования методики освоения новых знаний. Он обеспечивается проведением семинаров, оцениванием контрольных заданий, проверкой конспектов лекций, выполнением индивидуальных и творческих заданий, периодическим опросом обучающихся на занятиях.

2.2. Промежуточная аттестация

Освоение программы, в том числе отдельной ее части (модуля), может сопровождаться промежуточной аттестацией, проводимой в формах, в соответствии с учебным планом и рабочей программой.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме зачета. Принимается зачет преподавателями, читающими лекции по данному учебному модулю, в соответствии с перечнем примерных вопросов, выносимых для контроля знаний обучающихся.

Требования к результатам освоения учебного модуля. Промежуточная аттестация предназначена для определения уровня освоения всего объема учебной дисциплины. Для оценивания результатов обучения при проведении промежуточной аттестации используется шкала: «Зачтено», «Не зачтено».

Средняя оценка уровня сформированности компетенций по результатам текущего контроля	Оценка
Оценка не менее 3,0 и нет ни одной неудовлетворительной оценки по текущему контролю	«зачтено»

Оценка менее 3,0 или получена хотя бы одна неудовлетворительная оценка по текущему контролю	«не зачтено»

Проведение промежуточной аттестации в форме защиты аттестационной работы позволяет сформировать среднюю оценку по результатам текущего контроля. Так как оценочные средства, используемые при текущем контроле, позволяют оценить знания, умения и владения навыками/опытом деятельности обучающихся при освоении модуля. Для чего преподаватель находит среднюю оценку уровня сформированности компетенций у обучающегося, как сумму всех полученных оценок, деленную на число этих оценок.

Обучающийся должен:

знать:

– нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗКИ;

– возможные угрозы безопасности информации в результате специальных воздействий;

– организацию и содержание проведения работ по ТЗКИ, состав и содержание необходимых документов;

– технические каналы утечки информации, возникающие при ее обработке техническими средствами и системами;

– требования к средствам ТЗКИ и средствам контроля (мониторинга) эффективности мер защиты информации;

– средства ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации, порядок их применения, перспективы развития;

уметь:

– применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов в области ТЗКИ;

– разрабатывать необходимые документы в интересах проведения работ по ТЗКИ;

– определять возможные угрозы безопасности информации в результате специальных воздействий;

– формировать требования по ТЗКИ;

– определять требования к средствам ТЗКИ на объектах информатизации; организовывать и проводить работы по ТЗКИ;

– применять на практике штатные средства ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации;

– владеть навыками:

– работы с действующей нормативной правовой и методической базой в области ТЗКИ;

– определения угроз безопасности информации;

– определения задач, проведения организационных и технических

– мероприятий по ТЗКИ;

– определения задач, проведение организационных и технических мероприятий по контролю (мониторингу) защищенности конфиденциальной информации, подготовки материалов по результатам контроля;

– применения средств ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации.

При определении уровня достижений, обучающих на зачете, учитывается:

– знание программного материла и структуры модуля;

– знания, необходимые для решения типовых задач, умение выполнять предусмотренные программой задания;

– владение методологией модуля, умение применять теоретические знания при решении задач, обосновывать свои действия.

Если оценка уровня сформированности компетенций обучающегося не соответствует критериям получения зачета, то обучающийся сдает зачет. Зачет проводится в форме собеседования по перечню теоретических вопросов и решения

типовых контрольных заданий. Перечень теоретических вопросов и типовых контрольных заданий обучающиеся получают в начале обучения.

2.3. Итоговая аттестация

Освоение программы завершается итоговой аттестацией.

Итоговая аттестация проходит в форме защиты итоговой аттестационной работы по теме: «Проектирование защищенной корпоративной сети передачи данных компании (по предложению слушателя, желательно с привязкой к настоящему месту работы)».

Целью итоговой аттестации является установление соответствия уровня освоенности компетенций, обеспечивающих соответствующую квалификацию и уровень образования обучающихся, завершивших дополнительную профессиональную программу «Информационная безопасность телекоммуникационных систем». Итоговая аттестация призвана способствовать систематизации и закреплению знаний и умений обучающегося по специальности при решении конкретных профессиональных задач, определять уровень подготовки выпускника к самостоятельной работе.

Проведение итоговой аттестации в форме защиты итоговой аттестационной работы позволяет одновременно решить целый комплекс задач:

– ориентирует преподавателя и слушателя на конечный результат;

– позволяет в комплексе повысить качество учебного процесса, качество подготовки специалиста и объективность оценки подготовленности выпускников;

– расширяет полученные знания за счет изучения новейших практических разработок и проведения исследований в профессиональной сфере.

Целью написания итоговой аттестационной работы является выявление готовности выпускника к целостной профессиональной деятельности, способности самостоятельно применять полученные теоретические знания для решения производственных задач, умений пользоваться учебниками, учебными пособиями, современным справочным материалом, специальной технической литературой, каталогами, стандартами, нормативными документами, а также знания современной

техники и технологии. Для качественной организации по подготовке и выполнению итоговой аттестационной работы составляется график, в котором прописываются все этапы работы и сроки их выполнения:

1. Выдача заданий обучающимся
2. Разработка, выполнение и оформление разделов пояснительной записки итоговой аттестационной работы. Выполнение графической и практической части
3. Представление работы для написания отзыва
4. Представление итоговой аттестационной работы на утверждение и допуск к защите
5. Срок защиты итоговой аттестационной работы

При определении уровня достижений обучающихся при защите итоговой аттестационной работы, обращается особое внимание на следующее:

– дан полный, развернутый ответ на поставленный вопрос;

– показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные признаки, причинно-следственные связи;

– знание об объекте демонстрируются на фоне понимания его в системе данной дисциплины(модуля) и междисциплинарных связей;

– ответ формулируется в терминах дисциплины(модуля), изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию обучающегося.

При определении уровня достижений обучающихся учитывается:

– знание методов защиты корпоративных сетей предприятия;

– знания, необходимые для решения типовых задач, умение выполнять предусмотренные программой задания;

– владение методологией ИБ, умение применять теоретические знания при решении задач, обосновывать свои действия;

– определения угроз безопасности информации;

– определения задач, проведение организационных и технических мероприятий по контролю (мониторингу) защищенности конфиденциальной информации, подготовки материалов по результатам контроля;

– применения средств ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации.

– способностью оценивать технические возможности и вырабатывать рекомендации по построению телекоммуникационных систем и сетей, их элементов и устройств;

– способностью участвовать в разработке компонентов телекоммуникационных систем;

– способностью проектировать защищённые телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов;

– способностью применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду;

– способностью осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учетом предъявляемых к ним требований качества обслуживания и качества функционирования;

– способностью участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации.

Примерные вопросы на защиту итоговой аттестационной работы.

1. Как называется комплекс аппаратных и программных средств, а также персонала, предназначенный для управления различными процессами в рамках технологического процесса, производства, предприятия?

2. Как называется совокупность взаимосвязанных процессов создания и последовательного изменения состояния автоматизированной системы от формирования исходных требований к ней до окончания эксплуатации и утилизации комплекса средств автоматизации?

3. К какому типу относятся угрозы, у которых источник располагается вне системы?

4. К какому типу относятся угрозы, которые наносят ущерб объекту безопасности в целом?

5. К какому типу относятся угрозы, которые наносят ущерб отдельным частям объекта безопасности?

6. К какому типу относятся угрозы, при которых структура и содержание системы не изменяются?

7. К какому типу относятся угрозы, при которых структура и содержание системы подвергается изменениям?

8. К какому типу угроз относятся следующие угрозы: ошибки программного обеспечения, персонала, сбои в работе систем, отказы вычислительной и коммуникационной техники?

9. К какому типу угроз относятся следующие угрозы: неправомерный доступ к информации, разработка специального программного обеспечения, используемого для осуществления неправомерного доступа, разработка и распространение вирусных программ?

10. Как называется нарушитель, находящегося внутри информационной системы на момент начала реализации угрозы?

11. Как называется нарушитель, находящегося вне информационной системы на момент начала реализации угрозы?

12. Как называются внутренние нарушители, имеющие пользовательские права?

13. Какие каналы утечки информации не требуют непосредственного доступа к аппаратному обеспечению и данным информационной системы?

14. К какому типу канала утечки информации относится кража или утеря носителя информации?

15. Какие каналы утечки информации основаны на записи звука, подслушивании и прослушивании?

16. Какие каналы утечки информации основаны на перехвате сигналов, возникающих посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений?

17. Какие каналы утечки информации основаны на визуальных методах, фотографировании, видеосъёмках, наблюдении?

18. Какие каналы утечки информации основаны на получении доступа к информации на бумаге или других физических носителях информации?

19. Как называется структурированное представление всей информации, влияющей на безопасность информационной системы, которое включает в себя расчет рисков воплощения угрозы в жизнь, а также оценку предполагаемых последствий?

20. Как называются сведения, относящиеся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных), которые могут быть предоставлены другим лицам?

Критерии оценивания

Оценка «зачтено» выставляется, если слушатель в ходе защиты итоговой аттестационной работы проявил необходимый уровень сформированности компетенций, при этом знание об объекте проектирования демонстрируются на фоне понимания его в системе междисциплинарных связей, а ответ формулируется в профессиональных терминах, изложен литературным языком, логичен, доказателен и демонстрирует авторскую позицию обучающегося.

Оценка «не зачтено» ставится, если основное (базовое) содержание учебного материала не раскрыто, необходимый уровень освоения компетенций не достигнут, не даны ответы на вспомогательные вопросы, допущены грубые ошибки в определении понятий и в использовании терминологии.