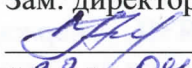


МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю

Зам. директора по УР

 Н.А. Андреева
«28» 04 2026 г.

Теория и практика комплексной безопасности Б1.В.01
рабочая программа дисциплины

Кафедра: Инфокоммуникационные технологии и системы связи

Направление подготовки: **11.03.02 Инфокоммуникационные технологии и системы связи**

Профиль: **Защищенные инфокоммуникационные системы.**

Формы обучения: **очная, заочная**

**Распределение часов дисциплины по семестрам (для очной формы обучения),
курсам (для заочной формы обучения)**

Вид учебной работы	ОФ		ЗФ	
	4 года		5 лет	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	2	72/8	2	72/5
Контактная работа, в том числе (по семестрам, курсам):		30/8		12/5
Лекции		10/8		4/5
Лабораторных работ				
Практических занятий		20/8		8/5
Семинаров				
Самостоятельная работа		42/8		60/5
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с разбивкой по семестрам		1/8		1/5
Число экзаменов с разбивкой по семестрам				

Программу составил:

Профессор кафедры ИТСС, д.пол.н., к.т.н. доц. Жуковский А.Г.

Рабочая программа дисциплины

«Теория и практика комплексной безопасности»

разработана в соответствии с ФГОС ВО:

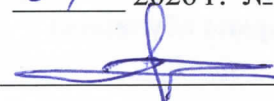
направления подготовки 11.03.02 ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ СВЯЗИ, утвержденным приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. N 930.

Составлена на основании учебного плана

направления 11.03.02 Инфокоммуникационные технологии и системы связи
профиля «Защищенные инфокоммуникационные системы», одобренных Учёным советом СКФ МТУСИ, протокол № 8 от 31.03 2026 г., и утвержденных директором СКФ МТУСИ 31.03 2026 г.

Рассмотрена и одобрена на заседании кафедры
«Информационная безопасность»

Протокол от «28» 04 2026 г. № 9

И.О. Зав. кафедрой  А.Г. Жуковский

1. Цели изучения дисциплины

Целью преподавания дисциплины «Теория и практика комплексной безопасности» является теоретическая и практическая подготовка специалистов к деятельности, связанной с комплексным анализом возможных угроз и созданием адекватной модели нарушителя, постановкой конкретных задач заданной степени сложности в рамках модели для обеспечения информационной безопасности компьютерных систем, а также содействие фундаментализации образования и развитию системного мышления.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способности решать профессиональные задачи в соответствии с *технологическим* видом деятельности:

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ПК-1: Способен обеспечить защиту от несанкционированного доступа сооружений и средств связи сетей электросвязи
Знать (Необходимые знания):
– методы контроля функционирования СССЭ, их защищенности от НСД; – принципы построения современных сетей электросвязи, математические модели каналов связи, виды модуляции сигналов; – функциональное назначение и основные характеристики средств контроля функционирования СССЭ, их защищенности от НСД; – организация и содержание мониторинга функционирования СССЭ, их защищенности от НСД; – возможные источники и технические каналы утечки информации; – нормативные правовые акты в области связи и защиты информации.
Уметь (Необходимые умения):
– использовать средства мониторинга работоспособности и эффективности применяемых программных, программно-аппаратных (в том числе криптографических) и технических средств защиты СССЭ от НСД; – проводить контроль функционирования СССЭ, их защищенности от НСД; – определять технические характеристики СССЭ, их защищенности от НСД; – оценивать помехоустойчивость и эффективность сетей электросвязи при передаче трафика, оптимизировать их параметры; – осуществлять проверки СССЭ, программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД на соответствие заданным требованиям; – проводить документационное обеспечение функционирования СССЭ, их защищенности от НСД.
Владеть (Трудовые действия):
– средствами анализа функциональности СССЭ, защищенности от НСД сооружений и СССЭ; – умением контролировать целостности сооружений и СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем

защиты СССР от НСД;

– составлением отчетов по результатам проверок, в том числе выявление инцидентов, которые могут привести к сбоям или нарушению функционирования или возникновению угроз безопасности информации, циркулирующей в СССР.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Дисциплина «Теория и практика комплексной безопасности» является логическим продолжением дисциплин Б1.О.24 «Основы информационной безопасности», Б1.В.07 Линии радиосвязи и методы их защиты, Б1.В.10 Сети и системы радиосвязи и средства их информационной защиты.
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
2	Дисциплина является базовой для успешного освоения дисциплин: Б1.В.08 Сети электросвязи и методы их защиты, Б1.В.15 Сетевая безопасность, Б1.В.ДВ.04.01 Технические средства и методы защиты информации.

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 72 часа, 30 аудиторных часов)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 4, Семестр 8					
Модуль 1.					
4 часа лекций, 8 часов практики, 20 часов самостоятельной работы					
1.1	Лекция 1. Направления обеспечения информационной безопасности 1. Правовое направление информационной безопасности 2. Организационное направление информационной безопасности 3. Инженерно-техническое направление информационной безопасности	Лек	2	ПК-1	Л1.1 Л1.2 Л1.3
1.2	Практическое занятие 1. информационная безопасность государства 1. Основные положения государственной политики информационной безопасности 2. Ключевые проблемы информационной безопасности государства 3. Основные направления деятельности государства в области информационной безопасности	ПЗ	2	ПК-1	Л2.1 Л2.2
1.3	Лекция 2. Обеспечение сохранения коммерческой тайны предприятия 1. Общие положения 2. Порядок определения информации, содержащей коммерческую тайну, и сроков ее действия 3. Система допуска сотрудников, командированных и частных лиц к сведениям, составляющим коммерческую тайну 4. Порядок работы с документами с грифом КТ 5. Обеспечение сохранности документов, дел и изданий. 6. Обязанности лиц, допущенных к сведениям, составляющим коммерческую тайну 7. Принципы организации и проведения контроля за обеспечением режима при работе со сведениями, содержащими коммерческую	Лек	2	ПК-1	Л1.1 Л1.2 Л1.3

	тайну 8. Ответственность за разглашение, утрату документов, содержащих коммерческую тайну				
1.4	Практическое занятие 2. Выявление потенциальных угроз и каналов утечки информации 1. Угрозы информационной безопасности в сферах деятельности государства 2. Угрозы безопасности информации, ИС и субъектов информационных отношений 3. Угрозы для процессов, процедур и программ обработки информации 4. Угрозы информации, возникающие при побочных электромагнитных излучениях и наводках	ПЗ	2	ПК-1	Л2.1 Л2.2
1.5	Практическое занятие 3. Принципы функционирования охранных систем 1. Емкостные средства обнаружения нарушителей; 2. Допплеровские радиолучевые средства обнаружения; 3. Тепловизоры 4. Инфракрасные средства обнаружения нарушителей 5. Пьезоэлектрические датчики 6. Датчики, работающие на «эффекте Холла» 7. Ультразвуковые датчики 8. Системы электрического наведенного поля	ПЗ	2	ПК-1	Л2.1 Л2.2
1.6	Практическое занятие 4. Защита каналов связи 1. Криптографические методы и средства защиты информации 2. Защита данных при передаче по каналам связи ИС 3. Выбор и совместимость средств защиты сообщений 4. Брандмауэры - основа СЗИ 5. Технологии виртуальной частной сети для корпоративных пользователей	ПЗ	2	ПК-1	Л2.1 Л2.2
1.7	Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 №149-ФЗ. Федеральный закон "О связи" от 07.07.2003 №126-ФЗ. Федеральный закон "О безопасности" от 28.12.2010 №390-ФЗ Федеральный закон "Об электронной подписи" от 06.04.2011 №63-ФЗ. Федеральный закон "О персональных данных" от 27.07.2006 №152-ФЗ. Закон РФ "О государственной тайне" от 21.07.1993 №5485-1. Федеральный закон "О коммерческой тайне" от 29.07.2004 №98-ФЗ. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 №187-ФЗ. Федеральный закон "О федеральной службе безопасности" от 03.04.1995 №40-ФЗ	СРС	20	ПК-1	Л3.1 Л3.2
Модуль 2. 6 часов лекций, 12 часов практики, 22 часа самостоят работы					
2.1	Лекция 3. Требования к защите компьютерной информации 1.Классификация требований к системам защиты информации. 2. Формализованные требования к защите информации от НСД. 3. Общие подходы к построению систем защиты компьютерной информации	Лек	2	ПК-1	Л1.1 Л1.2 Л1.3
2.2	Практическое занятие 5. Программно-технические методы и средства защиты информации 1. Службы и механизмы защиты информации программно-техническими методами	ПЗ	4	ПК-1	Л2.1 Л2.2

	2. Методы идентификации и аутентификации пользователей 3. Общие определения и классификация схем цифровых подписей 4. Инструментальные средства тестирования системы защиты 5. Межсетевые экраны 6. Виртуальные частные сети и их информационная защита				
2.3	Лекция 4. Сертификация информационных систем 1. Основные понятия 2. Перечень продукции, процессов и услуг, подлежащих сертификации 3. Процесс сертификации 4. Порядок подготовки и проведения сертификации 5. Типовой алгоритм испытаний ПО на соответствие требованиям безопасности	Лек	2	ПК-1	Л1.1 Л1.2 Л1.3
2.4	Практическое занятие 6 Организационные мероприятия по защите информации 1. Организация документооборота на предприятии 2. Организация службы безопасности на предприятии. 3. Состав службы безопасности на предприятии. 4. Организация охранного видеонаблюдения 5. Организация защиты информации в ИС от утечки по каналам ПЭМИН	Лек	4	ПК-1	Л2.1 Л2.2
2.5	Лекция 5. Оценка уязвимости и рисков 1. Процесс анализа рисков 2. Элементы управления рисками 3. Этапы процесса управления рисками 4. Методики оценки потенциально возможных угроз ИС	Лек.	2	ПК-1	Л1.1 Л1.2 Л1.3
2.6	Практическое занятие 7. Оценка эффективности систем защиты информации. 1. Вероятностный подход: структуризация предметной области оценки, анализ. 2. Подход на основе формирования требований к объекту: классы защищенности и их характеристики, контрольные процедуры, определение соответствия защиты установленным требованиям 3. Содержание и особенности экспертной оценки эффективности защиты. 4. Классификационная структура методов и моделей оценки 5. Системы показателей защищенности (эффективности). 6. Области применения и анализ приемлемости различных методов и моделей для оценки эффективности	ПЗ	4	ПК-1	Л2.1 Л2.2
2.7	Закон РФ "О частной детективной и охранной деятельности в Российской Федерации" от 11.03.1992 №2487-1 Федеральный закон "О лицензировании отдельных видов деятельности" от 04.05.2011 №99-ФЗ. Федеральный закон "Об экспортном контроле" от 18.07.1999 г. №183-ФЗ . Федеральный закон "О техническом регулировании" от 27.12.2002 №184-ФЗ. Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ. Гражданский кодекс Российской Федерации часть 4 (ГК РФ ч.4) 18.12.2006 №230-ФЗ. "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 №195-ФЗ. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности	СРС	22	ПК-1	Л3.1 Л3.2
3	Зачет				
Итого – 72 часа					

4.2 Заочная форма обучения (всего 72 часа, 12 аудиторных часов, 60 часов самост раб)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 4, 5					
Модуль 1.					
2 часа лекций, 4 часа практики, 30 часов самостоятельной работы					
1.1	Лекция 1. Направления обеспечения информационной безопасности 1. Правовое направление информационной безопасности 2. Организационное направление информационной безопасности 3. Инженерно-техническое направление информационной безопасности	Лек	2	ПК-1	Л1.1 Л1.2 Л1.3
1.2	Практическое занятие 1. информационная безопасность государства 1. Основные положения государственной политики информационной безопасности 2. Ключевые проблемы информационной безопасности государства 3. Основные направления деятельности государства в области информационной безопасности	ПЗ	2	ПК-1	Л2.1 Л2.2
1.3	Лекция 2. Обеспечение сохранения коммерческой тайны предприятия 1. Общие положения 2. Порядок определения информации, содержащей коммерческую тайну, и сроков ее действия 3. Система допуска сотрудников, командированных и частных лиц к сведениям, составляющим коммерческую тайну 4. Порядок работы с документами с грифом КТ 5. Обеспечение сохранности документов, дел и изданий. 6. Обязанности лиц, допущенных к сведениям, составляющим коммерческую тайну 7. Принципы организации и проведения контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну 8. Ответственность за разглашение, утрату документов, содержащих коммерческую тайну	СРС	2	ПК-1	Л1.1 Л1.2 Л1.3
1.4	Практическое занятие 2. Выявление потенциальных угроз и каналов утечки информации 1. Угрозы информационной безопасности в сферах деятельности государства 2. Угрозы безопасности информации, ИС и субъектов информационных отношений 3. Угрозы для процессов, процедур и программ обработки информации 4. Угрозы информации, возникающие при побочных электромагнитных излучениях и наводках	СРС	2	ПК-1	Л2.1 Л2.2
1.5	Практическое занятие 3. Принципы функционирования охранных систем 1. Емкостные средства обнаружения нарушителей; 2. Допплеровские радиолучевые средства обнаружения; 3. Тепловизоры 4. Инфракрасные средства обнаружения нарушителей 5. Пьезоэлектрические датчики 6. Датчики, работающие на «эффекте Холла» 7. Ультразвуковые датчики 8. Системы электрического наведенного поля	ПЗ	2	ПК-1	Л2.1 Л2.2
1.6	Практическое занятие 4.	СРС	2	ПК-1	Л2.1

	Защита каналов связи 1. Криптографические методы и средства защиты информации 2. Защита данных при передаче по каналам связи ИС 3. Выбор и совместимость средств защиты сообщений 4. Брандмауэры - основа СЗИ 5. Технологии виртуальной частной сети для корпоративных пользователей				Л2.2
1.7	Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 №149-ФЗ. Федеральный закон "О связи" от 07.07.2003 №126-ФЗ. Федеральный закон "О безопасности" от 28.12.2010 №390-ФЗ Федеральный закон "Об электронной подписи" от 06.04.2011 №63-ФЗ. Федеральный закон "О персональных данных" от 27.07.2006 №152-ФЗ. Закон РФ "О государственной тайне" от 21.07.1993 №5485-1. Федеральный закон "О коммерческой тайне" от 29.07.2004 №98-ФЗ. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 №187-ФЗ. Федеральный закон "О федеральной службе безопасности" от 03.04.1995 №40-ФЗ	СРС	24	ПК-1	Л3.1 Л3.2
Модуль 2. 2 часа лекций, 4 часа практики, 30 часов самостоят работы					
2.1	Лекция 3. Требования к защите компьютерной информации 1.Классификация требований к системам защиты информации. 2. Формализованные требования к защите информации от НСД. 3. Общие подходы к построению систем защиты компьютерной информации	СРС	2	ПК-1	Л1.1 Л1.2 Л1.3
2.2	Практическое занятие 5. Программно-технические методы и средства защиты информации 1. Службы и механизмы защиты информации программно-техническими методами 2. Методы идентификации и аутентификации пользователей 3. Общие определения и классификация схем цифровых подписей 4. Инструментальные средства тестирования системы защиты 5. Межсетевые экраны 6. Виртуальные частные сети и их информационная защита	СРС	4	ПК-1	Л2.1 Л2.2
2.3	Лекция 4. Сертификация информационных систем 1. Основные понятия 2. Перечень продукции, процессов и услуг, подлежащих сертификации 3. Процесс сертификации 4. Порядок подготовки и проведения сертификации 5. Типовой алгоритм испытаний ПО на соответствие требованиям безопасности	СРС	2	ПК-1	Л1.1 Л1.2 Л1.3
2.4	Практическое занятие 6 Организационные мероприятия по защите информации 1. Организация документооборота на предприятии 2. Организация службы безопасности на предприятии. 3. Состав службы безопасности на предприятии. 4. Организация охранного видеонаблюдения 5. Организация защиты информации в ИС от утечки по каналам ПЭМИН	СРС	4	ПК-1	Л2.1 Л2.2
2.5	Лекция 5. Оценка уязвимости и рисков 1. Процесс анализа рисков 2. Элементы управления рисками 3. Этапы процесса управления рисками 4. Методики оценки потенциально возможных угроз ИС	Лек.	2	ПК-1	Л1.1 Л1.2 Л1.3
2.6	Практическое занятие 7. Оценка эффективности систем защиты	ПЗ	4	ПК-1	Л2.1

	информации. 1. Вероятностный подход: структуризация предметной области оценки, анализ. 2. Подход на основе формирования требований к объекту: классы защищенности и их характеристики, контрольные процедуры, определение соответствия защиты установленным требованиям 3. Содержание и особенности экспертной оценки эффективности защиты. 4. Классификационная структура методов и моделей оценки 5. Системы показателей защищенности (эффективности). 6. Области применения и анализ приемлемости различных методов и моделей для оценки эффективности				Л2.2
2.7	Закон РФ "О частной детективной и охранной деятельности в Российской Федерации" от 11.03.1992 №2487-1 Федеральный закон "О лицензировании отдельных видов деятельности" от 04.05.2011 №99-ФЗ. Федеральный закон "Об экспортном контроле" от 18.07.1999 г. №183-ФЗ . Федеральный закон "О техническом регулировании" от 27.12.2002 №184-ФЗ. Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ. Гражданский кодекс Российской Федерации часть 4 (ГК РФ ч.4) 18.12.2006 №230-ФЗ. "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 №195-ФЗ. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности	СРС	18	ПК-1	Л3.1 Л3.2
3	Зачет				
Итого – 72 часа					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л1.1	Э. В. Запонов, А. П. Мартынов, И. Г. Машин	Методы и средства комплексной защиты информации в технических системах : учебное пособие	Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2019	Э1
Л1.2	Герасимова, О. Ю.	Информационная безопасность и защита информации в образовательной среде : учебное пособие	Казань : Бук, 2024.	Э2
Л1.3	Штеренберг, С. И.	Защита информации в компьютерных системах : учебное пособие	Санкт-Петербург: Санкт-Петербургский государственный университет промышленных технологий и дизайна, 2022.	Э3

5.1.2. Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	В. А. Гриднев, Ю. А. Губсков, А. С. Дерябин, А. В. Яковлев.	Программно-аппаратные средства защиты информации. В 3 частях. Ч.3 : учебное пособие /— Тамбов :	Тамбовский государственный технический университет, ЭБС АСВ, 2024	Э4
Л2.2	Э. В. Запонов, А. П. Мартынов, И. Г. Машин [и др.].	Методы и средства комплексной защиты информации в технических системах : учебное пособие	Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2019	Э5
5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Компания «Конфидент»	Защита информации. Dallas Lock : практикум / видеоуроки	База знаний Dallas Lock	Э6
Л3.2	ФСТЭК	Официальный сайт ФСТЭК РФ. Раздел «Документы»	Федеральная служба по техническому и экспортному контролю	Э7
5.2. Электронные образовательные ресурсы				
Э1	https://www.iprbookshop.ru/101925.html			
Э2	https://www.iprbookshop.ru/books/160834/details			
Э3	https://www.iprbookshop.ru/140114.html			
Э4	https://www.iprbookshop.ru/books/145338/details			
Э5	https://www.iprbookshop.ru/books/101925/details			
Э6	https://dallaslock.ru/products/faq/			
Э7	https://fstec.ru/dokumenty-filter			
5.3. Программное обеспечение				
П.1	MS Word	лицензионное		
П.2	Power Point	лицензионное		

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оснащенная проектором, ПК (ноутбуком), экраном
6.2 МТО лабораторных работ и практических занятий	
1	Учебные аудитории, оборудованные компьютерной техникой, с возможностью подключения к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ
6.3 МТО рубежных контролей, экзамена	
1	Учебные аудитории, оборудованные компьютерной техникой, с возможностью подключения к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ

7. Оценочные материалы

Оценочные материалы и перечень видов оценочных средств текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

8. Методические рекомендации по освоению дисциплины
--

Методические рекомендации по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.
--

9. Особенности реализации дисциплины (модуля) при обучении инвалидов и лиц с ограниченными возможностями здоровья

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков.

Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания.

Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.).

Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь.

Текущий контроль успеваемости осуществляется в устной форме.

При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины «Теория и практика комплексной безопасности Б1.В.01» для использования в 20___/20___ учебном году

Утверждаю

Зам. директора по УР _____
«___» _____ 20___ г.

Направление: 11.03.02 Инфокоммуникационные технологии и системы связи

Профиль: Защищенные инфокоммуникационные системы

Форма обучения: очная, заочная

(Возможны следующие варианты):

а) Рабочая программа действует без изменений.

б) В рабочую программу вносятся следующие изменения:

1);

2);

3)

Разработчик (и): _____
(ФИО, ученая степень, ученое звание)

«___» _____ 20___ г.

Рабочая программа пересмотрена и одобрена на заседании кафедры _____

Протокол № _____ от «___» _____ 20___ г.

Заведующий кафедрой _____

Оценочные материалы для проведения текущего контроля и промежуточной аттестации по дисциплине

1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

1.1 Шкала оценивания компетенций

Шкала оценивания компетенций		
Оценка	Уровень освоения компетенции	Критерии оценивания
«Отлично»	Высокий уровень	Обучающийся показывает всестороннее, систематическое и глубокое знание основного и дополнительного учебного материала, умеет свободно выполнять задания, предусмотренные программой; усвоил основную и знаком с дополнительной рекомендованной литературой; может объяснить взаимосвязь основных понятий дисциплины в их значении для последующей профессиональной деятельности; проявляет творческие способности в понимании, изложении и использовании учебного материала.
«Хорошо»	Повышенный уровень	Обучающийся показывает достаточный уровень знаний в пределах основного учебного материала, без существенных ошибок выполняет предусмотренные в программе задания; усвоил основную литературу, рекомендованную в программе; способен объяснить взаимосвязь основных понятий дисциплины при дополнительных вопросах преподавателя. Допускает не существенные погрешности в ответах, устраняет их без помощи преподавателя.
«Удовлетворительно»	Пороговый уровень	Обучающийся показывает знания основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы; справляется с выполнением заданий, предусмотренных программой, допуская при этом большое количество не принципиальных ошибок; знаком с основной литературой, рекомендованной программой. Допускает существенные погрешности в ответах, но обладает необходимыми знаниями для их устранения под руководством преподавателя.
«Неудовлетворительно»	Минимальный уровень не достигнут	Обучающийся обнаруживает пробелы в знаниях основного учебного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не знаком с рекомендованной литературой, не может исправить допущенные ошибки. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

1.2 Показатели, критерии и шкалы оценивания компетенций

Показатели компетенции	Оценочные средства	Шкала оценивания (баллов)
ПК-1		
Знать:		
– методы контроля функционирования СССЭ, их защищенности от НСД; – принципы построения современных сетей электросвязи, математические модели каналов связи, виды модуляции сигналов; – функциональное назначение и основные характеристики средств контроля функционирования СССЭ, их защищенности от НСД; – организация и содержание мониторинга функционирования СССЭ, их защищенности от НСД; – возможные источники и технические каналы утечки информации; нормативные правовые акты в области связи и защиты информации.	Контрольная работа	Модуль 1 0÷10 «Удовлетворительно» - 4-6 «Хорошо» - 7-8 «Отлично» - 9-10
	Контрольная работа	Модуль 2 0÷10 «Удовлетворительно» - 5-6 «Хорошо» - 7-8 «Отлично» - 9-10
Уметь		
– использовать средства мониторинга работоспособности и эффективности применяемых программных, программно-аппаратных (в том числе криптографических) и технических средств защиты СССЭ от НСД; – проводить контроль функционирования СССЭ, их защищенности от НСД; – определять технические характеристики СССЭ, их защищенности от НСД; – оценивать помехоустойчивость и эффективность сетей электросвязи при передаче трафика, оптимизировать их параметры; – осуществлять проверки СССЭ, программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от	Практическое занятие 1-4	Модуль 1 0÷20 «Удовлетворительно» - 8-12 «Хорошо» - 13-16 «Отлично» - 17-20
	Практическое занятие 5-6	Модуль 2 0÷20 «Удовлетворительно» - 8-12 «Хорошо» - 13-16 «Отлично» - 17-20

НСД на соответствие заданным требованиям; проводить документационное обеспечение функционирования СССЭ, их защищенности от НСД.		
Владеть		
– средствами анализа функциональности СССЭ, защищенности от НСД сооружений и СССЭ; – умением контролировать целостности сооружений и СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД; составлением отчетов по результатам проверок, в том числе выявление инцидентов, которые могут привести к сбоям или нарушению функционирования или возникновению угроз безопасности информации, циркулирующей в СССЭ.	Практическое занятие 1-4	Модуль 1 0÷20 «Удовлетворительно» - 8-12 «Хорошо» - 13-16 «Отлично» - 17-20
	Практическое занятие 5-6	Модуль 2 0÷20 «Удовлетворительно» - 8-12 «Хорошо» - 13-16 «Отлично» - 17-20
Зачет		41-100 баллов менее 41 - незачет

1.3 Оценочные материалы: типовые контрольные задания, иные материалы

1.3.1 Оценочные средства для очной формы обучения

Модуль 1 (50 баллов):

Модуль содержит 3 лекционных занятия и 4 практических занятия. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За выполненные практические работы студент получает максимум 40 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы (ПК-1):

1. Основные концептуальные положения системы защиты информации
2. Концептуальная модель информационной безопасности
3. Угрозы конфиденциальной информации
4. Действия, приводящие к неправомерному овладению конфиденциальной информацией
5. Правовая защита

6. Организационная защита
7. Инженерно-техническая защита
8. Общие положения
9. Защита информации от утечки по визуально оптическим каналам
10. Защита информации от утечки по акустическим каналам
11. Защита информации от утечки по электромагнитным каналам
12. Защита информации от утечки по материально - вещественным каналам
13. Классификация методов криптографического преобразования информации
14. Шифрование. Основные понятия
15. Методы шифрования с симметричным ключом
16. Системы шифрования с открытым ключом
17. Стандарты шифрования
18. Перспективы использования криптозащиты информации в КС.

Практическое занятие 1. Исследование характеристик и возможностей программ по защите и сокрытию файлов, папок

Контрольные вопросы ПЗ №1 (ПК-1):

1. Укажите назначение, достоинства и недостатки программы Wise Folder Hider.
2. Укажите назначение, достоинства и недостатки программы Secure Folders
3. Укажите назначение, достоинства и недостатки программы Anvide Lock Folder
4. Укажите назначение, достоинства и недостатки программы Folder Lock
5. Укажите назначение, достоинства и недостатки программы Easy File Locker
6. Укажите назначение, достоинства и недостатки программы Folder Guard
7. Укажите назначение, достоинства и недостатки программы DEKSI USB Security
8. Укажите назначение, достоинства и недостатки программы Locker
9. Укажите назначение, достоинства и недостатки программы Advanced Hider
10. Укажите назначение, достоинства и недостатки программы Hide Folders XP
11. Укажите назначение, достоинства и недостатки программы Hide Files

Практическое занятие 2. Исследование характеристик и возможностей программ по шифрованию, безвозвратному удалению, стеганографии

Контрольные вопросы ПЗ №2 (ПК-1):

1. Укажите назначение, достоинства и недостатки программы TrustPort Tools
2. Укажите назначение, достоинства и недостатки программы Cryptic Disk
3. Укажите назначение, достоинства и недостатки программы Locker (скрытие файлов)
4. Укажите назначение, достоинства и недостатки программы Max File Encryption
5. Укажите назначение, достоинства и недостатки программы Secure Disk

6. Укажите назначение, достоинства и недостатки программы Masker 7.1
7. Укажите назначение, достоинства и недостатки программы Fox Secret
8. Укажите назначение, достоинства и недостатки программы HideInPicture 1.0
9. Укажите назначение, достоинства и недостатки программы Шифровальщик
10. Укажите назначение, достоинства и недостатки программы Advanced Encryption Package
11. Укажите назначение, достоинства и недостатки программы Gpg4win
12. Укажите назначение, достоинства и недостатки программы Cryptic Disk Professional
13. Укажите назначение, достоинства и недостатки программы CyberSafe Files Encryption
14. Укажите назначение, достоинства и недостатки программы Steganos Privacy Suite
15. Укажите назначение, достоинства и недостатки программы Lavasoft Privacy Toolbox
16. Укажите назначение, достоинства и недостатки программы pkiImage Free Edition

Практическое занятие 3. Основные этапы доступа к ресурсам вычислительной системы; использование простого пароля; использование динамически изменяющегося пароля; взаимная проверка подлинности и другие случаи опознавания; способы разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам

Контрольные вопросы ПЗ№3 (ПК-1):

1. Политика информационной безопасности предприятия и организации.
2. Правовые (организационно-технические, экономические) методы обеспечения информационной безопасности.
3. Обеспечение информационной безопасности компьютерных систем.
4. Анализ современных подходов к построению систем защиты информации.
5. Критерии оценки защищенности компьютерных систем, методы и средства обеспечения их информационной безопасности.
6. Особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну.
7. Обеспечение безопасности технических систем и человека в условиях использования информационного оружия.
8. Анализ факторов, определяющих безопасность технических систем.
9. Классификация и возможности технических разведок.
10. Показатели защищенности средств вычислительной техники от НСД к информации.
11. Пароль как средство защиты от НСД.
12. Требования по защите информации в автоматизированных системах от НСД.
13. Оценка безопасности информационных технологий по Общим критериям.

ПЗ №4. Исследование характеристик и возможностей антивирусного ПО

Контрольные вопросы ПЗ№4 (ПК-1):

1. Укажите назначение, достоинства и недостатки программы AVAST Free Antivirus
2. Укажите назначение, достоинства и недостатки программы AVG AntiVirus Free
3. Укажите назначение, достоинства и недостатки программы Dr.Web Antivirus
4. Укажите назначение, достоинства и недостатки программы Антивирус Касперского
5. Укажите назначение, достоинства и недостатки программы ESET NOD32 Антивирус
6. Укажите назначение, достоинства и недостатки программы AVZ Antivirus
7. Укажите назначение, достоинства и недостатки программы Avira Free Antivirus
8. Укажите назначение, достоинства и недостатки программы Norton AntiVirus
9. Укажите назначение, достоинства и недостатки программы McAfee Antivirus
10. Укажите назначение, достоинства и недостатки программы Emsisoft Anti-Malware
11. Укажите назначение, достоинства и недостатки программы BullGuard Antivirus
12. Укажите назначение, достоинства и недостатки программы Protector Plus Antivirus
13. Укажите назначение, достоинства и недостатки программы Panda Antivirus
14. Укажите назначение, достоинства и недостатки программы Ashampoo Anti-Virus
14. Укажите назначение, достоинства и недостатки программы G Data AntiVirus
16. Укажите назначение, достоинства и недостатки программы K7 AntiVirus
17. Укажите назначение, достоинства и недостатки программы VIRUSfighter
18. Укажите назначение, достоинства и недостатки программы Twister Antivirus

Модуль 2: (50 баллов):

Модуль содержит 3 лекционных занятия и 2 практических занятия. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За выполненные и защищенные практические работы студент получает максимум 40 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы (ПК-1):

1. Проблемы обеспечения безопасности обработки информации.
2. Проблемы обеспечения безопасности хранения информации в вычислительных системах.
3. Базовые этапы построения системы комплексной защиты вычислительных систем.
4. Анализ моделей нарушителя
5. Угрозы информационно-программному обеспечению
6. Классификация компьютерных вирусов
7. Файловые вирусы

8. Загрузочные вирусы
9. Вирусы и операционные системы
10. Методы и средства борьбы с вирусами
11. Профилактика заражения вирусами компьютерных
12. Порядок действий пользователя при обнаружении заражения ЭВМ вирусами
13. Внесение функциональной и информационной избыточности.
14. Понятие надежности
15. Способы резервирования информации
16. Правила обновления резервных данных
17. Методы сжатия информации
18. Архивация файловых данных
19. Резервирование системных данных

ПЗ №5. Исследование характеристик и возможностей программ по восстановлению потерянных данных

Контрольные вопросы ПЗ №5 (ПК-1):

1. Укажите назначение, достоинства и недостатки программы Hetman Partition Recovery
2. Укажите назначение, достоинства и недостатки программы Active File Recovery
3. Укажите назначение, достоинства и недостатки программы R-Studio 7.6
4. Укажите назначение, достоинства и недостатки программы Auslogics File Recovery
5. Укажите назначение, достоинства и недостатки программы Active UNDELETE
6. Укажите назначение, достоинства и недостатки программы Paragon Rescue Kit
7. Укажите назначение, достоинства и недостатки программы Wise Data Recovery
8. Укажите назначение, достоинства и недостатки программы Puran File Recovery
9. Укажите назначение, достоинства и недостатки программы O&O DiskRecovery
10. Укажите назначение, достоинства и недостатки программы Tenorshare Any Data Recovery
11. Укажите назначение, достоинства и недостатки программы Power Data Recovery
12. Укажите назначение, достоинства и недостатки программы GetDataBack
13. Укажите назначение, достоинства и недостатки программы Recover My Files
14. Укажите назначение, достоинства и недостатки программы R-Undelete
15. Укажите назначение, достоинства и недостатки программы Handy Recovery
16. Укажите назначение, достоинства и недостатки программы Ashampoo Undeleter

ПЗ №6. Исследование характеристик и возможностей программ по организации резервного копирования

Контрольные вопросы ПЗ №6 (ПК-1):

1. Укажите назначение, достоинства и недостатки программы Iperius Backup
2. Укажите назначение, достоинства и недостатки программы FBackup
3. Укажите назначение, достоинства и недостатки программы Backup4all
4. Укажите назначение, достоинства и недостатки программы Uranium Backup Free
5. Укажите назначение, достоинства и недостатки программы Simple Data Backup
6. Укажите назначение, достоинства и недостатки программы Personal Backup
7. Укажите назначение, достоинства и недостатки программы Back4Sure
8. Укажите назначение, достоинства и недостатки программы SyncBackFree
9. Укажите назначение, достоинства и недостатки программы Handy Backup
10. Укажите назначение, достоинства и недостатки программы EASEUS Todo Backup 8.0 Free Edition
11. Укажите назначение, достоинства и недостатки программы Exiland Backup Free 4.0
12. Укажите назначение, достоинства и недостатки программы Nero BackItUp
13. Укажите назначение, достоинства и недостатки программы Paragon Rescue Kit 14.0 Free
14. Укажите назначение, достоинства и недостатки программы Action Backup
15. Укажите назначение, достоинства и недостатки программы LimBackup
16. Укажите назначение, достоинства и недостатки программы AVSbackup
17. Укажите назначение, достоинства и недостатки программы ExtraBackup
18. Укажите назначение, достоинства и недостатки программы Cobian Backup
19. Укажите назначение, достоинства и недостатки программы Backup & Recovery 10 Build 9169 Free Edition
20. Укажите назначение, достоинства и недостатки программы Information Backup System

Вопросы, выносимые на зачет по дисциплине «Теория и практика комплексной безопасности» (ПК-1)

1. Понятие и сущность ЗИ. Назначение ЗИ. Задачи ЗИ.
2. Методологические основы организации ЗИ.
3. Принципы организации ЗИ. Основные требования, предъявляемые к ЗИ.
4. Правовое регулирование в области безопасности информации.
5. Общая характеристика организационных методов защиты информации.
6. Основные факторы, влияющие на организацию ЗИ.
7. Функции руководства предприятия и подразделений предприятия, экспертной комиссии, службы защиты информации.
8. Классификация информации по видам тайны и степеням конфиденциальности. Нормативное закрепление состава защищаемой информации; структура перечней

сведений, относимых к различным видам тайны.

9. Значение носителей защищаемой информации как объектов защиты. Факторы, определяющие состав носителей информации.
10. Методика выявления состава носителей защищаемой информации. Хранилища носителей информации как объект защиты.
11. Особенности помещений для работы с защищаемой информацией как объектов защиты.
12. Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами защиты.
13. Определение возможных методов несанкционированного доступа к защищаемой информации.
14. Методика выявления нарушителей (незаконных пользователей) и состава интересующей их информации.
15. Факторы, влияющие на выбор компонентов ЗИ. Объекты защиты как основной фактор, определяющий состав компонентов ЗИ.
16. Обеспечение полноты составляющих защиты. Учет всех факторов и обстоятельств, оказывающих влияние на качество защиты.
17. Обеспечение безопасности всей совокупности подлежащей защите информации во всех компонентах ее сбора, хранения, передачи и использования, а также во все время и при всех режимах функционирования систем обработки информации.
18. Понятие модели объекта, основные виды моделей и их характеристика.
19. Распределение функций по защите информации между руководством предприятия, службой защиты информации, обеспечение взаимодействия между ними.
20. Разработка нормативных документов, регламентирующих деятельность персонала по защите информации. Подбор и обучение персонала.
21. Состав нормативно-методических документов по обеспечению функционирования системы ЗИ.
22. Содержание и особенности экспертной оценки эффективности защиты.
23. Сведения, составляющие коммерческую тайну предприятия
24. Угрозы безопасности информации в компьютерных системах.
25. Угрозы для протоколов и служб Internet
26. Виртуальные частные сети и их информационная защита
27. Методы идентификации и аутентификации пользователей
28. Межсетевые экраны
29. Оценка защищенности информации от утечки по каналам ПЭМИН
30. Основные концептуальные положения системы защиты информации
31. Действия, приводящие к неправомерному овладению конфиденциальной информацией
32. Направления обеспечения безопасности
33. Правовые документы по защите информации и их характеристика
34. Задачи по обеспечению организационных мероприятий по защите информации.

35. Классификация мер инженерно-технической защиты информации.
36. Классификация инженерно-технической защиты информации по техническим средствам.
37. Классификация программных средств защиты информации
38. Каналы разглашения конфиденциальной информации.
39. Способы пресечения разглашения информации.
40. Каналы утечки конфиденциальной информации. Их классификация.
41. Защита информации от утечки по визуально-оптическим каналам
42. Защита информации от утечки по акустическим каналам
43. Защита информации от утечки по электромагнитным каналам
44. Способы несанкционированного доступа
45. Защита от наблюдения и фотографирования
46. Способы прослушивания посредством радиозакладок.
47. Обеспечение безопасности телефонных переговоров
48. Назначение и характеристики нелинейных локаторов
49. Назначение и характеристики средств постановки активных помех
50. Назначение и принцип работы скремблеров (дескремблеров)
51. Противодействие незаконному подключению к линиям связи
52. Меры защиты от радиоперехвата
53. Основные встроенные механизмы защиты ОС и их недостатки
54. Анализ существующих угроз для современных универсальных ОС
55. Задачи и методы резервирования.
56. Криптографические методы защиты информации.
57. Компьютерные вирусы и механизмы борьбы с ними.
58. Профилактика заражения вирусами компьютерных систем.

2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

2.1 Порядок и методика проведения текущего контроля и промежуточной аттестации

Предусмотрены следующие виды контроля:

- текущий контроль по каждому модулю – в форме написания контрольной работы для оценки теоретических знаний;
- текущий контроль по каждому модулю – в форме отчетов по лабораторным работам и практическим занятиям для оценки практических навыков;
- промежуточная аттестация по дисциплине – в форме зачета с оценкой

Текущий контроль успеваемости в форме защиты лабораторных и практических проводится в два этапа:

- 1-й этап: допуск к выполнению лабораторной работы – проводится в форме письменной «летучки» (5-10 мин) с целью контроля знаний студентов теоретической части лабораторной работы и готовности к выполнению практических исследований;

- 2-й этап выполняется по окончании каждой лабораторной работы (практического занятия) в форме индивидуального собеседования по выполненным исследованиям или расчетам. Проводится с целью контроля закрепления теоретической части материала и степени отработки студентом практических навыков исследования на аппаратуре.

Контрольные работы выполняются в виде короткого письменного ответа на один вопрос, изученный на предыдущей лекции в начале каждой последующей лекции. Ответ на вопрос дается в течение 5-10 минут. Таким образом, после лекционного курса каждого модуля формируется общая оценка за теоретические знания.

С целью повышения качества обучения за счет побуждения студентов к активной текущей учебной работе, четкого и оперативного контроля всего хода учебного процесса, снижения роли случайных и субъективных факторов при оценивании учебной деятельности студентов в образовательном процессе реализована модульно-рейтинговая система.

Правила ее использования прописаны в «Положении об МРС».

Набранные обучающимся баллы могут быть переведены в оценку:

- «неудовлетворительно» - от 0% до 40% от максимального количества баллов;
- «удовлетворительно» - от 41% до 60% максимального количества баллов;
- «хорошо» - от 61% до 80% максимального количества баллов;
- «отлично» - от 81% до 100% максимального количества баллов.

Для получения зачета студенту достаточно набрать от 41 и более баллов.

Соотношения максимального количества баллов, полученных студентом по блокам модулей, показаны в Таблице.

Таблиц - Распределение баллов по блокам модулей дисциплины «Теория и практика комплексной безопасности»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок (Распределение баллов по занятиям)
Модуль 1	50	20	30
Модуль 2	50	20	30
Зачет с оценкой	100	100	

Результаты текущего контроля доводятся до сведения обучающихся на последнем занятии в рамках аудиторной работы до проведения промежуточной аттестации.

На зачете с оценкой производится оценка тех компетенций, которые должны быть в той или иной форме освоены в процессе изучения. Рекомендуется формировать вопросы в экзаменационных билетах таким образом, чтобы преподаватель смог оценить все компетенции данной дисциплины.

2.2 Методика проведения зачета в группах заочной формы обучения

Зачет по дисциплине у студентов заочной формы обучения проводится письменно по классической методике. Вопросы сгруппированы в билетах. В каждом билете содержится по 2 вопроса. Количество билетов должно быть не менее числа студентов в группе. Студенты готовят устные ответы на вопросы.

3 Промежуточная аттестация

Промежуточная аттестация проводится в форме зачета с оценкой.

Зачет с оценкой проводится по расписанию в устном виде. Количество вопросов в экзаменационном билете – 2. Оценка ответов и объявление результатов производится в день экзамена. Результаты аттестации заносятся в экзаменационную ведомость и зачетную книжку обучающегося.

Обучающиеся, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Один комплект отпечатанных билетов, подписанных преподавателем кафедры и утвержденных заведующим кафедрой хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину

	МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»	Утверждаю Зав. кафедрой «ИТСС» _____ Юхнов В.И. «___» _____ 20__ г.
Направление подготовки: Инфокоммуникационные технологии и системы связи Курсы: 4 Дисциплина: Теория и практика комплексной безопасности		
Билет №1 1. Преимущества цифровых методов передачи телевизионных сигналов. 2. Анализ транспортного потока. Ошибки транспортного потока различных приоритетов. Профессор каф. «ИТСС» _____ Жуковский А.Г. «___» _____ 20__ г.		

4 Тестовые задания для проведения оценки сформированности компетенции ПК-1

Тестовые задания позволяют оценить уровень сформированности компетенции ПК-1.

Задания распределены по блокам в соответствии с уровнем сложности. Каждый блок содержит номер задания, и текст задания.

Базовый уровень (Блок А) содержит примерно 50 % заданий.

Он формируется из заданий с выбором одного или нескольких верных ответов из предложенных или воспроизведения фактического материала (терминология, факты, классификация, параметры и др.);

Повышенный уровень (Блок Б) в среднем составляет 35 % заданий.

В нем используются задания на сопоставление, сравнение, установление последовательности;

Высокий уровень (Блок В) в среднем составляют – 15 % заданий.

В задании используются: решения нетиповых задач, алгоритмы, доказательства, задания с развернутым ответом – определения, перечисление, изображение схемы, структуры и др.

Количество заданий по компетенции ПК-1 равно 20.

Один комплект тестовых вопросов с указанием правильных ответов хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину.

ПК-1: Способен обеспечить защиту от несанкционированного доступа сооружений и средств связи сетей электросвязи.

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№ задания	Дисциплина	Тексты заданий
1	Б1.В.01 Теория и практика комплексной безопасности	Организационная структура службы информационной безопасности определяется: 1. Требованиями законодательства 2. Требованиями государственных и международных стандартов 3. Потребностями в защите информационных ресурсах и возможностями в соответствии с оценками руководителей предприятия
2	Б1.В.01 Теория и практика комплексной безопасности	Аудит информационной безопасности - это: 1. Экспертное обследование различных аспектов защищенности информационных ресурсов 2. Проверка правильности оформления и учета расходов на средства защиты информации 3. Проверка уровня защищенности информационных ресурсов
3	Б1.В.01 Теория и практика комплексной безопасности	Передача функций по обеспечению информационной безопасности на аутсорсинг обуславливается: 1. Требованиями законодательства 2. Экономической целесообразностью 3. Имиджевыми соображениями
4	Б1.В.01 Теория и практика комплексной безопасности	Аудит информационной безопасности подразделяется на: 1. Текущий и итоговый 2. Внешний и внутренний 3. Объективный и субъективный
5	Б1.В.01 Теория и практика комплексной безопасности	Страхование информационных рисков: 1. Обеспечивает защиту целостности и конфиденциальности информационных ресурсов 2. Позволяет компенсировать потери в случае нанесения ущерба информационным ресурсам 3. Является инструментом управления рисками
6	Б1.В.01 Теория и практика комплексной безопасности	Риски в сфере информационной безопасности включают в себя: 1. Нарушение конфиденциальности 2. Необратимую утрату информации 3. Недоступность информационных ресурсов
7	Б1.В.01 Теория и практика комплексной безопасности	Лицензированием деятельности по разработке средств защиты информации в РФ занимается: 1. ФСО 2. СВР 3. ФСТЭК 4. МВД
8	Б1.В.01 Теория и практика комплексной безопасности	Цели аудита информационной безопасности могут включать в себя: 1. Выявление лиц, нарушающих требования информационной безопасности 2. Сертификацию на соответствие общепризнанным требованиям и стандартам 3. Установление степени защищенности информационных ресурсов
9	Б1.В.01 Теория и практика комплексной безопасности	Основой внутриобъектового режима является: 1. Режим сигнализации 2. Режим видеонаблюдения

№ задания	Дисциплина	Тексты заданий
		3. Пропускной режим
10	Б1.В.01 Теория и практика комплексной безопасности	Комплексность решения задач информационной безопасности предполагает: 1. Исключение "узких мест" в системе защиты информации 2. Анализ всех возможных сценариев нарушения безопасности и способов защиты 3. Обеспечение круглосуточной ежедневной работы службы информационной безопасности

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия
Инструкция: Прочитайте текст и установите соответствие

№ задания	Дисциплина	Тексты заданий
11	Б1.В.01 Теория и практика комплексной безопасности	Сертификат безопасности свидетельствует о качествах защищенной информационной техники. Они таковы: 1. Достоверность эффективности защиты. 2. Надежность. 3. Корректность применения. Достигаются следующими действиями: А. Точным описанием порядка и области применения продукта. Б. Тестированием всех аспектов безопасности при разработке, производстве, поставке и применении продукта. В. Точным описанием защитных функций продукта в связи с характерными угрозами и наличием оценки степени устойчивости механизмов защиты.
12	Б1.В.01 Теория и практика комплексной безопасности	Для информационной техники характерны следующие риски 1. Потеря конфиденциальности; 2. Потеря целостности; 3. Потеря функциональности, Это приводит к А. Манипуляции с данными; Б. Несанкционированное получение информации; В. Потеря или разрушение данных.
13	Б1.В.01 Теория и практика комплексной безопасности	При определении уровня качества защиты учитываются многие факторы: 1. Корректность разработки продукта к которой относятся ...; 2. Эффективность конструкции продукта которой относятся ...; 3. Безопасность среды разработки которой относятся ...; 4. Рабочая документация которой относятся ...; 5. Область использования которой относятся А. Пригодность, совместное проявление функций, оценка уязвимых мест, стойкость механизмов защиты; Б. Требования к защищенности, архитектурный проект, подробный проект, реализация; В. Контроль конфигурации, язык программирования, компилятор, безопасность при разработке; Г. Документация пользователя, администратора системы; Д. Поставка и конфигурирование, начало использования, техническое обслуживание.
14	Б1.В.01 Теория и практика комплексной безопасности	Для повышения надежности системы защиты информации используются три режима резервирования системы защиты дополнительными механизмами защиты: 1. Горячий резерв; 2. Активный холодный резерв; 3. Пассивный холодный резерв; Поставьте в соответствие определения данных режимов А. Только одно из средств защиты (основное или дополнительное) настроено и включено. Б. Основной и дополнительный механизмы защиты настроены, но включен только один из них. В. Основные и дополнительные механизмы защиты настроены и включены.

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности
Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Дисциплина	Тексты заданий
15	Б1.В.01 Теория и практика комплексной безопасности	Условно качество защищенности можно охарактеризовать по четырем уровням: низкое, удовлетворительное, хорошее, отличное. Расставьте описание уровней в порядке их повышения 1. Максимальные требования к подтверждению корректности, практически не преодолимая защита от манипуляций 2. Грубо протестированная корректность, слабая защита от манипуляций или отсутствие таковой; 3. Обстоятельно протестированная корректность, удовлетворительное действие защиты против манипуляций; 4. Тщательно протестированная корректность, хорошая или очень хорошая защита от манипуляций;
16	Б1.В.01 Теория и практика комплексной безопасности	Расставьте в порядке повышения надежности: 1.Последовательно соединенные системы, 2.Параллельно соединенные системы или 3. Системы, имеющие смешанный вид соединения
17	Б1.В.01 Теория и практика комплексной безопасности	Расставьте в порядке повышения эффективности поисковые устройства для обнаружения скрытых электронных устройств – 1. Нелинейные локаторы, 2. Индикаторы поля, 3. Досмотровые зеркала, 4. Анализаторы спектра.

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом
Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Дисциплина	Тексты заданий
18	Б1.В.01 Теория и практика комплексной безопасности	Под сертификацией продукции по требованиям безопасности информации понимается: _____
19	Б1.В.01 Теория и практика комплексной безопасности	К техническим средствам ИС относятся: _____
20	Б1.В.01 Теория и практика комплексной безопасности	Надежность системы защиты информации это _____

Методические рекомендации по освоению дисциплины «Теория и практика комплексной безопасности»

1. Методические рекомендации преподавателю

Дисциплина «Теоретические основы электротехники» включает в себя:

- лекционные занятия – 10 часов;
- практические занятия – 20 часов;
- промежуточную аттестацию – зачет.

Перед началом изучения дисциплины преподаватель должен ознакомить студентов с рабочей программой и оценочными материалами по дисциплине, с видами учебной и самостоятельной работы, перечнем литературы и интернет-ресурсов, с формами текущей и промежуточной аттестации, с критериями оценки качества знаний для итоговой оценки по дисциплине.

При проведении лекций, преподаватель:

- 1) формулирует тему и цель занятия, объявляет учебные вопросы;
- 2) излагает основные теоретические положения;
- 3) с помощью технических средств обучения и/или под запись дает определения основных понятий, расчетных формул;
- 4) проводит примеры из отечественного и зарубежного опыта, дает текущие статистические данные для наглядного и образного представления изучаемого материала;
- 5) в конце занятия выдает вопросы для самостоятельного изучения.

Во время выполнения заданий в учебной аудитории студент может консультироваться с преподавателем, определять наиболее эффективные методы решения поставленных задач. Если какая-то часть задания остается не выполненной, студент может продолжить её выполнение во время внеаудиторной самостоятельной работы.

Для оценки полученных знаний и освоения учебного материала по каждому разделу и в целом по дисциплине преподаватель использует формы текущего контроля и контроля знаний обучающихся при проведении промежуточной аттестации.

2. Методические рекомендации студентам

Приступая к изучению новой учебной дисциплины, студенты должны ознакомиться с рабочей программой, оценочными материалами, учебной, научной и методической литературой, имеющейся в ЭИОС СКФ МТУСИ,

Глубина усвоения дисциплины зависит от активной и систематической работы студента на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

2.1 Методические указания для обучающихся по подготовке к лекционным занятиям

Важно сосредоточить внимание на содержании лекции. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине.

Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти, необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы.

Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности студентов.

2.2 Методические указания для обучающихся по подготовке к практическим занятиям

Целью практических занятий является закрепление теоретических знаний, полученных при изучении дисциплины.

При подготовке к практическому занятию целесообразно выполнить следующие рекомендации:

- изучить основную литературу; ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д.;
- при необходимости доработать конспект лекций. При этом учесть рекомендации преподавателя и требования учебной программы.

При выполнении практических занятий основным методом обучения является самостоятельная работа студента под управлением преподавателя. На них пополняются теоретические знания студентов, их умение творчески мыслить, анализировать, обобщать изученный материал, проверяется отношение студентов к будущей профессиональной деятельности.

Оценка выполненной работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению и оформлению работы.

После подведения итогов занятия студент обязан устранить недостатки, отмеченные преподавателем при оценке его работы.

3. Методические рекомендации для обучающихся по самостоятельной работе

Самостоятельная работа студентов является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам.

Самостоятельная работа во внеаудиторное время включает в себя:

- повторение лекционного материала;
- подготовки к лабораторным работам (практическим занятиям);
- изучения учебной и научной литературы;
- решения задач, выданных на практических занятиях;
- подготовки к тестированию;
- выполнение курсовой работы;
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях;
- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов.

Перед выполнением внеаудиторной самостоятельной работы преподаватель проводит инструктаж (консультацию) с определением цели задания, его содержания, сроков

выполнения, основных требований к результатам работы, критериев оценки, форм контроля и перечня источников и литературы.

Обычно постановку задачи обучаемым на проведение самостоятельной работы преподаватель осуществляет на одном из занятий, предшествующему данному.

Методику самостоятельной работы все обучаемые выбирают индивидуально.