Аннотация к рабочей программе дисциплины

«Информационная безопасность инфокоммуникаций»

Цель преподавания дисциплины

Сформировать основы знаний по принципам построения телекоммуникационных систем (ТКС), а также ознакомление с методами, средствами и системами обеспечения их информационной безопасности.

Задачи изучения дисциплины

– научить основным методам исследования и решения задач дискретных процессов;
– выработать умение самостоятельно расширять знания и проводить математический анализ прикладных задач.

Индикаторы компетенций, формируемые в результате освоения дисциплины

УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними
	УК-1.2 Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению
	УК-1.3 Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников
	УК-1.4 Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов
	УК-1.5 Использует логико-методологический инструментарий для критической оценки современных концепций философского и социального характера в своей предметной области
ОПК-2 Способен реализовывать новые принципы и методы исследования современных инфокоммуникационных систем и сетей различных типов передачи, распределения, обработки и хранения информации	ОПК-2.1 Использует принципы и методы исследования современных инфокоммуникационных систем, оценивая их достоинства и недостатки
	ОПК-2.2 Оперирует основными методами и средствами проведения экспериментальных исследований систем передачи, распределения, обработки и хранения информации
	ОПК-2.3 Использует новые принципы и методы обработки и передачи информации в современных инфокоммуникационных системах и сетях
	ОПК-2.4 Анализирует передовой отечественный и зарубежный опыт исследования современных инфокоммуникационных систем и /или их составляющих

Разделы дисциплины

1. Информация, основные информационные процессы, классификация информации. Основные виды телекоммуникационных систем (ТКС), Актуальность задач информационной безопасности ТКС.
2. Доктрина информационной безопасности РФ и ее основные составляющие, понятия «угрозы» и «несанкционированного доступа» (НСД), основные угрозы безопасности и их классификация (угрозы доступности, целостности и конфиденциальности). Уровни обеспечения информационной

безопасности ТКС. Основные программно-технические меры обеспечения информационной безопасности ТКС.
3. Системы телефонной связи и их классификация; аналоговые и цифровые системы телефонной связи с коммутацией каналов, угрозы безопасности и методы защиты; организационные и организационно-технические, аппаратные и программно-аппаратные методы защиты, методы скремблирования, методы и средства шифрации, системы сигнализации, угрозы безопасности и методы защиты; системы телефонной связи с коммутацией пакетов (VoIP-системы), угрозы безопасности и общие методы защиты, методы защиты технологий VoIP H.323 и SIP.
4. Особенности оптических систем связи, уязвимости и каналы утечки информации, методы НСД, аппаратные и программные методы защиты.
5. Архитектура сети GSM, угрозы информационной безопасности в системах сотовой связи GSM, методы и средства обеспечения безопасности в системах GSM.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.О. декана факультета
Фундаментальной и прикладной информатики
(наименование ф-та полностью)

М.О. Таныгин
(подпись, инициалы, фамилия)

«21» 08 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность инфокоммуникаций

(наименование дисциплины)

ОПОП ВО 11.04.02 Инфокоммуникационные технологии и системы связи
(шифр согласно ФГОС и наименование направления подготовки (специальности))

направленность (профиль, специализация) «Проектирование устройств, систем и сетей телекоммуникаций»
наименование направленности (профиля, специализации)

форма обучения очная
(очная, очно-заочная, заочная)

Курск – 202

Рабочая программа дисциплины Информационная безопасность инфокоммуникаций в соответствии с ФГОС ВО – магистратура по направлению подготовки (специальности) 11.04.02 Инфокоммуникационные технологии и системы связи на основании учебного плана ОПОП ВО 11.04.02 Инфокоммуникационные технологии и системы связи, направленность Проектирование устройств, систем и сетей телекоммуникаций, одобренного Ученым советом университета (протокол №6 «20» 02 2021г.).

Рабочая программа дисциплины Информационная безопасность инфокоммуникаций обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 11.04.02 Инфокоммуникационные технологии и системы связи, направленность Проектирование устройств, систем и сетей телекоммуникаций на заседании кафедры информационной безопасности Протокол № 1 «20» 09 2021 г.

Зав. кафедрой Таныгин М.О.

Разработчик программы

к.т.н., доцент Ефремов М.А.

Согласовано: на заседании кафедры космического приборостроения и систем связи Протокол № 1 «27» 09 2021 г.

Зав. кафедрой Андронов В.Г.

Директор научной библиотеки Макаровская В.Г.

Рабочая программа дисциплины Информационная безопасность инфокоммуникаций пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 11.04.02 Инфокоммуникационные технологии и системы связи, направленность Проектирование устройств, систем и сетей телекоммуникаций, одобренного Ученым советом университета протокол №7«28»02 2022 г., на заседании кафедры ИБ протокол №1 от 30.08.2022

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ Таныгин М.О.

Рабочая программа дисциплины Информационная безопасность инфокоммуникаций пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 11.04.02 Инфокоммуникационные технологии и системы связи, направленность Проектирование устройств, систем и сетей телекоммуникаций, одобренного Ученым советом университета протокол №7«28»02 2022 г., на заседании кафедры информационной безопасности протокол №1 от 30.08.2023

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

1 Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1 Цель дисциплины

Целью преподавания дисциплины «Информационная безопасность инфокоммуникаций» (ИнБИ) сформировать основы знаний по принципам построения телекоммуникационных систем (ТКС), а также ознакомление с методами, средствами и системами обеспечения их информационной безопасности.

1.2 Задачи дисциплины

Основными задачами изучения дисциплины является:

- определение места и значения ИНБИ
- в системе принятия хозяйственных решений и ее роли как превентивного механизма
- предупреждения негативных последствий вредоносных воздействий объективного и субъективного характера на функционирование ТКС; ознакомление с принципами передачи сообщений в основных сетях связи, ознакомление с основами информационной безопасности
- систем и сетей связи, ознакомление с методами несанкционированного извлечения информации из сигналов и сообщений различных систем связи.

Знания и умения, которыми должен обладать студент, успешно освоивший данную дисциплину:

- знание уязвимостей основных телекоммуникационных технологий, средств и
- методов обеспечения их информационной безопасности, умение анализировать безопасность
- функционирования ТКС, а также оценивать уязвимость их протоколов и интерфейсов.

1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)	*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*

код компетенции	*наименование компетенции*		
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий		УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними	***Знать:*** критерии соответствия функционала подсистем информационной безопасности угрозам для объектов информатизации ***Уметь:*** выбирать требуемые политики безопасности при обеспечении безопасности ИКС ***Владеть:*** навыками реагирования на нештатные ситуации, возникающие при эксплуатации компонентов безопасности ИКС
		УК-1.2 Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению	***Знать:*** основные угрозы работоспособности прогаммным компонентам СЗИ ***Уметь:*** выявлять каналы утчки информациив ИКС ***Владеть:*** использования особенностей информации, циркулирующей в ИКС, для обеспечения ИБ
		УК-1.3 Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источник	***Знать:*** порядок внедрения, отладки и развития процессов и этапов разработки требований, критериев качества и методов обеспечения информационной безопасности прикладных ИС в процессе их эксплуатации. ***Уметь:*** организовать и управлять внедрением, отладкой и развитием процессами и этапами разработки требований, критериев качества и методов обеспечения информационной безопасности прикладных ИС в процессе их эксплуатации. ***Владеть:*** навыками организации и управления внедрением, отладкой и развитием процессами и этапами разработки требований, критериев качества и методов обеспечения информационной безопасности прикладных ИС в процессе их эксплуатации.

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
		УК-1.4 Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подход	***Знать:*** процессы, этапы разработки и сопровождения требований к информационной безопасности эксплуатируемых прикладных информационных систем (ИС). ***Уметь:*** организовать описание процессов и этапов разработки требований к информационной безопасности прикладных ИС в процессе их эксплуатации. ***Владеть:*** навыками организации описания процессов и этапов разработки требований к информационной безопасности прикладных ИС в процессе их эксплуатации.
		УК-1.5 Использует логико-методологический инструментарий для критической оценки современных концепций философского и социального характера в своей предметной области	***Знать:*** требования к качеству требований и методов обеспечения информационной безопасности прикладных ИС в процессе их эксплуатации; методы защиты информации, способы защиты информационных систем, методы анализа угроз и оценки рисков информационной безопасности ИС. ***Уметь:*** организовать создание и развитие требований к качеству требований и методов обеспечения информационной безопасности прикладных ИС в процессе их эксплуатации; применять средства защиты информации для решения практических задач в области защиты компьютерных систем и сетей; проводить анализ информационных рисков.

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			Владеть: навыками организации создания и развития требования к качеству требований и методов обеспечения информационной безопасности прикладных ИС в процессе их эксплуатации, применения программных средств защиты информации, разработки архитектуры сетевой защиты.
ОПК-2	Способен реализовывать новые принципы и методы исследования современных инфокоммуникационных систем и сетей различных типов передачи, распределения, обработки и хранения информации	ОПК-2.1 Использует принципы и методы исследования современных инфокоммуникационных систем, оценивая их достоинства и недостатки	***Знать:*** номенклатуру современных программно-аппаратных средств современных инфокоммуникационных систем; назначение, организацию и принципы функционировании программно-аппаратных средств современных инфокоммуникационных систем; механизмы защиты программно-аппаратных средств современных инфокоммуникационных систем, основные этапы аудита состава и конфигурации прикладной современных инфокоммуникационных систем, в том числе номенклатуру покупных и вновь разрабатываемых аппаратных средств ИС. ***Уметь:*** устанавливать современные программные средства, подключать аппаратные средства современных инфокоммуникационных систем; настраивать операционные системы и их подсистемы; сопоставлять структурную организацию программных и аппаратных средств требова-

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			ниям политики безопасности; проводить анализ угроз, рисков, применять антивирусные программные комплексы, настраивать режимы работы межсетевых экранов; проводить основные этапы аудита состава и конфигурации прикладной современных инфокоммуникационных систем, в том числе покупных и вновь разрабатываемых программных средства ИС. ***Владеть:*** навыками оценки эффективности программно-аппаратных средств; реализации требуемых политик безопасности с помощью современных программно-аппаратных средств защиты информации; проведения проверок работоспособности и эффективности применения программно-аппаратных средств; проведения основных этапов аудита состава и конфигурации прикладной ИС, в том числе покупных и вновь разрабатываемых аппаратных средств ИС.
		ОПК-2.2 Оперирует основными методами и средствами проведения экспериментальных исследований систем передачи, распределения, обработки и хранения информации	***Знать:*** методологию и основные технические средства для проведения экспериментальных исследований защищенных систем передачи данных. ***Уметь:*** проводить экспериментальные исследования систем передачи, распределения, обработки и хранения информации

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			Владеть: навыками определения характеристик систем передачи, распределения, обработки и хранения информации
		ОПК-2.3 Использует новые принципы и методы обработки и передачи информации в современных инфокоммуникационных системах и сетях	***Знать:*** номенклатуру современных программно-аппаратных средств ИС; назначение, организацию и принципы функционировании программно-аппаратных средств ИС; механизмы защиты программно-аппаратных средств ИС; классификацию и архитектуру ИС. ***Уметь:*** сопоставлять структурную организацию программных и аппаратных средств требованиям политики безопасности; проводить анализ угроз, рисков, применять антивирусные программные комплексы, проводить анализ защищенности локальной вычислительной сети, проводить анализ информационных рисков; проводить основные этапы аудита состава и конфигурации прикладной ИС, в том числе вновь разрабатываемых программных и аппаратных средств ИС. ***Владеть:*** навыками проведения проверок работоспособности и эффективности применения программно-аппаратных средств, защиты информации в компьютерных системах, анализа защищенности современных ин-

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			фокоммуникационных систем и сетей.
		ОПК-2.4 Анализирует передовой отечественный и зарубежный опыт исследования современных инфокоммуникационных систем и /или их составляющи	***Знать:*** источники новой научно-технической информации в области обеспечения безопасности современных инфокоммуникационных систем и сетей. ***Уметь:*** проводить сравнительный анализ предлагаемых решений в области обеспечения безопасности современных инфокоммуникационных систем и сетей ***Владеть:*** навыками реферирования источников научно-технической информации в области обеспечения безопасности современных инфокоммуникационных систем и сетей

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Информационная безопасность инфокоммуникаций» входит в часть, формируемую участниками образовательных отношений блока «Дисциплины (модули)» основной профессиональной образовательной программы магистратуры 11.04.02 Инфокоммуникационные технологии и системы связи, направленность Проектирование устройств, систем и сетей телекоммуникаций. Дисциплина изучается на 1 курсе в 1 семестре.

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 4 зачетные единицы (з.е.), 144 академических часов.

Таблица 3 - Объём дисциплины

Виды учебной работы	Всего, Часов
Общая трудоемкость дисциплины	144
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	44
в том числе:	
Лекции	8
лабораторные занятия	0
практические занятия	36
Самостоятельная работа обучающихся (всего)	62,85
Контроль (подготовка к экзамену)	36
Контактная работа по промежуточной аттестации (всего АттКР)	0,15
в том числе:	
Зачет	не предусмотрен
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	0,15

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1.1 - Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел, (тема) дисциплины	Содержание
1	2	3
1	Введение.	Информация, основные информационные процессы, классификация информации, угрозы информационной безопасности. Основные виды телекоммуникационных систем (ТКС), предмет дисциплины «Информационная безопас-
2	Основные понятия информационной безопасности ТКС	Доктрина информационной безопасности РФ и ее основные составляющие, понятия «угрозы» и «несанкционированного доступа» (НСД), основные угрозы безопасности и их классификация (угрозы доступности, целостности и конфиденциальности). Уровни обеспечения информационной безопасности ТКС. Основные программно-технические меры обеспечения информационной безопасности ТКС.

3	Информационная безопасность систем передачи речевой информации	Системы телефонной связи и их классификация; аналоговые и цифровые системы телефонной связи с коммутацией каналов, угрозы безопасности и методы защиты; организационные и организационно-технические, аппаратные и программно-аппаратные методы защиты, методы скремблиро-
4	Информационная безопасность систем волоконно-оптической связи (ВОЛС)	Особенности оптических систем связи, уязвимости и каналы утечки информации, методы НСД, аппаратные и программные методы защиты.
5	Инфокоммуникационная безопасность систем сотовой связи.	Архитектура сети GSM, угрозы информационной безопасности в системах сотовой связи GSM, методы и средства обеспечения безопасности в системах GSM.

Таблица 4.1.2 - Содержание дисциплины и ее методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		Лек. час	№ лаб	№ пр.			
1	2	3	4	5	6	7	8
1	Введение.	1		1	У-1, МУ-1	С	УК-1, ОПК-2
2	Основные понятия информационной безопасности ТКС	1		2	У-1-3, МУ-2	С	УК-1, ОПК-2
3	Информационная безопасность систем передачи речевой информации	2		3	У-1, МУ-3	С	УК-1, ОПК-2
4	Информационная безопасность систем волоконно-оптической связи	2			У-2,8	С	УК-1, ОПК-2
5	Инфокоммуникационная безопасность систем сотовой связи.	2		4,5	У-1,9 МУ-4,5	С	УК-1, ОПК-2
	Всего	8	-	5			

С – собеседование

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Практические занятия

Таблица 4.2.1 - Практические занятия

№	Наименование практического (семинарского) занятия	Объем, час.
1	Общие вопросы обработки сигналов в программе Adobe Audition	7
2	Маскировка речевого сигнала путем его зашумления	7
3	Определение неизвестного номера абонента аналоговой телефонной сети путем спектральной оценки частотных параметров его сигналов	7
4	Обработка тональных сигналов набора номера	7
5	Исследование методов защиты абонентского терминала сотовой связи GSM в системе Android	8
Итого		36

4.2 Самостоятельная работа студентов (СРС)

Таблица 4.2 - Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	Введение.	1-3 недели	11,85
2	Основные понятия информационной безопасности ТКС	4-6 недели	12
3	Информационная безопасность систем передачи речевой информации	7-10 недели	13
4	Информационная безопасность систем волоконно-оптической связи (ВОЛС)	11-14 недели	13
5	Инфокоммуникационная безопасность систем сотовой связи.	15-18 недели	13
Итого			62,85

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным обо-

рудованием и методическими разработками кафедры в рабочее время, установленное «Правилами внутреннего распорядка работников».

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

– библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

– имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

– путем обеспечения доступности всего необходимого учебно- методического и справочного материала за счёт выкладывания на сайт кафедры ИБ в интернете (адрес http://www.swsu.ru/structura/up/fivt/k_tele/index.php);

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

путем разработки:

- методических рекомендаций, пособий по организации самостоятельной работы студентов;

– заданий для самостоятельной работы;

– вопросов и задач к зачёту;

–методических указаний к выполнению лабораторных и практических работ и т.д.

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

–удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6. Образовательные технологии

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования профессиональных компетенций обучающихся. В рамках дисциплины предусмотрены встречи с экспертами и специалистами Комитета цифрового развития и связи Курской области.

Таблица 6.1 - Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (лекции, практиче-	Используемые интерактивные	Объем

	ского или лабораторного занятия)	образовательные технологии	в часах
1	2	3	4
1	Выполнение практической работы №2 «Маскировка речевого сигнала путем его	Исследование возможности сокрытия речевого сигнала в	3
2	Выполнение практической работы №3 «Определение неизвестного номера або-	Исследование влияния спектральных характеристик сиг-	3
3	Выполнение практической работы №4 «Обработка тональных сигналов набора номера»	Исследование влияния спектральных характеристик сигнала на возможность несанкционированного доступа к передаваемым по сетям дан-	3
4	Выполнение практической работы №3 «Исследование методов защиты абонентского терминала сотовой связи GSM в системе Android»	Составление и исследование студентами модели и системы защиты мобильного терминала	3
Итого			12

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения основной профессиональной образовательной программы

Таблица 7.1 - Этапы формирования компетенций

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули) и практики, при изучении/прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Профессиональный иностранный язык Информационная безопасность инфокоммуникаций Учебная практика (научно-исследовательская работа)	Профессиональный иностранный язык Философские и психологические проблемы творчества Учебная технологическая (проектно-технологическая) практика	Выполнение и защита выпускной квалификационной работы

ОПК-2. Способен реализовывать новые принципы и методы исследования современных инфокоммуникационных систем и сетей различных типов передачи, распределения, обработки и хранения информации	Теория построения инфокоммуникационных сетей и систем Информационная безопасность инфокоммуникаций Учебная практика (научно-исследовательская работа)	Методы моделирования и оптимизации в инфокоммуникациях Учебная технологическая (проектно-технологическая) практика	Выполнение и защита выпускной квалификационной работы

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 7.2 Показатели, критерии и шкала оценивания компетенций

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	*2*	3	4	5
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий (Начальный)	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними	Знать: основные понятия теории проектирования инфокоммуникационных систем Уметь: анализировать взаимосвязи между составом технических средств ИКС и угрозами информационной безопасности Владеть: анализа угроз безопасности ИКС	Знать: принципы организации подсистем безопасности инфокоммуникационных систем Уметь: настраивать компонентов безопасности ИКС Владеть: обеспечения безопасности информации циркулирующей в ИКС	Знать: критерии соответствия функционала подсистем информационной безопасности угрозам для объектов информатизации Уметь: выбирать требуемы политики безопасности при обеспечении безопасности ИКС Владеть: реагировании на

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	*2*	3	4	5
				нештатные ситуации, возникающие при эксплуатации компонентов безопасности ИКС
	УК-1.2 Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению	Знать: используемые в работе с ИКС программные средства Уметь: анализировать угрозы безопасности в ИКС Владеть: навыками выбора средств обеспечения информационной безопасности ИКС	Знать: инструментальные средства проведения проверок информационных систем Уметь: использовать в работе программные средства обеспечения информационной безопасности ИКС Владеть: эксплуатации средств обеспечения информационной безопасности ИКС	Знать: основные угрозы работоспособности програмным компонентам СЗИ Уметь: выявлять каналы утчки информациив ИКС Владеть: использования особенностей информации, циркулирующей в ИКС, для обеспечения ИБ
	УК-1.3 Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источник	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защи-	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства за-

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	*2*	3	4	5
		информации.	щенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	щиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
	УК-1.4 Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подход	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защит информации для решения практических задач в области информационной безопасности, разрабаты-	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	*2*	3	4	5
		средств защиты информации.	вать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
	УК-1.5 Использует логико-методологический инструментарий для критической оценки современных концепций философского и социального характера в своей предметной области	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безо-	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь:

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	*2*	3	4	5
		программных средств защиты информации.	пасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
ОПК-2 Способен реализовывать новые принципы и методы исследования современных инфокоммуникационных систем и сетей различных типов передачи, распределения, обработки и хра-	ОПК-2.1 Использует принципы и методы исследования современных инфокоммуникационных систем, оценивая их достоинства и недостатки	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыка-	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информаци-	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности.

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	*2*	3	4	5
нения информации (Начальный)		ми применения программных средств защиты информации.	онной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
	ОПК-2.2 Оперирует основными методами и средствами проведения экспериментальных исследований систем передачи, распределения, обработки и хранения информа-	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности.	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в об-	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безо-

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	*2*	3	4	5
	ции	Владеть: навыками применения программных средств защиты информации.	ласти информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	пасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	*2*	3	4	5
	ОПК-2.3 Использует новые принципы и методы обработки и передачи информации в современных инфокоммуникационных системах и сетях	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
	ОПК-2.4 Анализирует пе-	Знать: методы защиты	Знать: методы защиты	Знать: методы за-

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	*2*	3	4	5
	редовой отечественный и зарубежный опыт исследования современных инфокоммуникационных систем и /или их составляющие	информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	щиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.

7.3Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

Таблица 7.3 Паспорт комплекта оценочных средств для текущего контроля успеваемости

п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№ заданий	
1	2	3	4	5	6	7
1.	Введение.	УК-1, ОПК-2	Лекция, СРС, практическое занятие	Собеседование	1-3	Согласно табл.7.2
				КВЗПР №1	1-3	
2.	Основные понятия информационной безопасности ТКС	УК-1, ОПК-2	Лекция, СРС, практическое занятие	Собеседование,	1-4	Согласно табл.7.2
				КВЗПР №2	1-4	
3.	Информационная безопасность систем передачи речевой информации	УК-1, ОПК-2	Лекция, СРС, практическое занятие	собеседование	1-7	Согласно табл.7.2
				КВЗПР №3	1-7	
4.	Информационная безопасность систем волоконно-оптической связи (ВОЛС)	УК-1, ОПК-2	Лекция, СРС,	Собеседование	1-3	Согласно табл.7.2
5.	Инфокоммуникационная безо-	УК-1, ОПК-2	Лекция, СРС, практическое	Собеседование	1-3	Согласно табл.7.2

	пасность систем сотовой связи.		занятие	КВЗПР №4,5	1-3	

СРС – самостоятельная работа студента, КВЗПР - контрольные вопросы для защиты практических работ

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного опроса по разделу (теме) 3. «Информационная безопасность систем передачи речевой информации».

1. Системы телефонной связи и их классификация.
2. Аналоговые и цифровые системы телефонной связи с коммутацией каналов
3. Перечислите угрозы безопасности и методы защиты.
4. Перечислите организационные и организационно-технические, аппаратные и программно-аппаратные методы защиты,
5. Опишите методы скремблирования, методы и средства шифрации, системы сигнализации,
6. Назовите угрозы безопасности и методы защиты; системы телефонной связи с коммутацией пакетов (VoIP-системы),
7. Охарактеризуйте угрозы безопасности и общие методы защиты, методы защиты технологий VoIP H.323 и SIP

Контрольные вопросы для защиты практической работы № 1:

1. Что такое дискретизация аналогового сигнала?
2. Что такое АИМ-сигнал?
3. Как происходит кодирование АИМ-сигнала?
4. Объяснить метод преобразования (оцифровки) аналогового сигнала в цифровой
5. Что такое информация?
6. На сколько категорий подразделяются все виды информации (кратко охарактеризовать каждую)?
7. Что такое инфокоммуникационная безопасность?
8. Что такое защита информации?
9. Что такое утечка информации?
10. На какие виды (по назначению) можно условно разделить системы передачи информации?

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

Типовые задания для проведения промежуточной аттестации обучающихся. Промежуточная аттестация по дисциплине проводится в форме экзамена.

Промежуточная аттестация по дисциплине проводится в форме экзамена. Экзамен проводится в виде бланкового тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки (или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

1. Какая угроза информационной безопасности является пассивной:
А) Копирование секретных данных.
Б) Внедрение вредоносного программного обеспечения.

В) Кража носителей информации.
Г) Удаление файла.

Задание в открытой форме:

1. Угрозы нарушения целостности информации приводят к …….
2. В автоматизированной системе перехват данных, передаваемых по каналам связи относится к уровню ……..
3. Пассивной угрозой информационной безопасности является ……...

Задание на установление правильной последовательности.

Установить в порядке увеличения единицы измерения количества информации:

1. 1 ТБ

2. 30 Гбайт

3. 50 Килобайт

4. 100 Мегабайт

Задание на установление соответствия:

между элементами ПК и функциями элементов

1	Процессор	А	Хранение информации
2	Оперативная память	Б	Обработка информации
3	Жесткий диск	В	Отображение информации
4	Монитор	Г	Ввод информации

способов и видов информации

1	По способу кодирования	А	Цифровая, аналоговая
2	По способу представления	Б	Визуальная, звуковая, документ
3	По способу обработки	В	Текстовая, графическая, числовая
4	По способу восприятия	Г	Непрерывная, дискретная

Компетентностно-ориентированная задача:

Определить минимальную длину кодового слова с возможностью исправления 3-х кратных ошибок при кодировании информации длиной 8 бит.

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

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

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– положение П 02.016–2018 О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Устный опрос по темам 1-2	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по темам 3-4	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по темам 5	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Выполнение практической работы №1 «Общие вопросы обработки сигналов в программе Adobe Audition»	4	Выполнил, доля правильных ответов от 50% до 90%	8	Выполнил, доля правильных ответов более 90%
Выполнение практической работы №2 «Маскировка речевого сигнала путем его	4	Выполнил, доля правильных ответов от 50% до 90%	8	Выполнил, доля правильных ответов более 90%

зашумления»				
Выполнение практической работы №3 «Определение неизвестного номера абонента аналоговой телефонной сети путем спектральной оценки частотных параметров его сигналов»	5	Выполнил, доля правильных ответов от 50% до 90%	9	Выполнил, доля правильных ответов более 90%
Выполнение практической работы №4 «Обработка тональных сигналов набора номера»	4	Выполнил, доля правильных ответов от 50% до 90%	8	Выполнил, доля правильных ответов более 90%
Выполнение практической работы №5 «Исследование методов защиты абонентского терминала сотовой связи GSM в системе Android»	4	Выполнил, доля правильных ответов от 50% до 90%	9	Выполнил, доля правильных ответов более 90%
Итого	24		48	
Посещаемость	0		16	
Экзамен	0		36	
Итого	24		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме –2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование –36 баллов.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1. Спеваков, Александр Геннадьевич. Информационная безопасность : учебное пособие : [для студентов, обучающихся по специальностям 100301 «Информационная безопасность», 400301 «Юриспруденция», 380301 «Экономика»] / А. Г. Спеваков, М. О. Таныгин, В. С. Панищев ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2017. - 196 с. : ил., табл. - Библиогр.: с. 188-195. - ISBN 978-5-7681-1196-0 : 290.00 р. - Текст : непосредственный.

2. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учебник для студентов вузов, обучающихся по направлению 552800 "Информатика и вычислительная техника" и по специальностям 220100 "Вычислительные машины, комплексы, системы и сети", 220200 "Автоматизированные системы обработки информации и управления" и 220400 "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Г. Олифер, Н. А. Олифер. - 5-е изд. - Санкт-Петербург : Питер, 2019. - 922 с.

3. Проскуряков, А. В. Компьютерные сети: основы построения компьютерных сетей и телекоммуникаций : учебное пособие / А. В. Проскуряков ; Министерство науки и высшего образования Российской Федерации ; Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» ; Инженерно-технологическая академия. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 202 с. : ил. - URL: http://biblioclub.ru/index.php?page=book&id=561238 - (дата обращения 15.07.2019) . - Режим доступа: по подписке. - Библиогр.: с. 195-196. - ISBN 978-5-9275-2792-2. - Текст : электронный.

8.2 Дополнительная учебная литература

4. Грибунин, В. Г. Комплексная система защиты информации на предприятии [Текст] : учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М.: Академия, 2009. - 416 с.

5. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - Санкт-Петербург : Питер, 2015. - 943 с.

6. Нужнов, Е. В. Компьютерные сети [Электронный ресурс] : учебное пособие / Е. В. Нужнов. - Таганрог : Издательство Южного федерального университета, 2015 -Ч. 2. Технологии локальных и глобальных сетей. - 2015. - 176 с. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=461991

7. Подольский, В. И. Компьютерные информационные системы в аудите [Электронный ресурс] : учебное пособие / В. И. Подольский, Н. С. Щербакова, В. Л. Комиссаров. - Москва : Юнити-Дана, 2015. - 160 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=115315.

8. Безбогов, А. А. Методы и средства защиты компьютерной информации : учебное пособие / А. А. Безбогов, А. Я. Яковлев, В. Н.

Шамкин. - Тамбов : ТГТУ, 2006. - 196 с. - URL: http://window.edu.ru/resource/546/38546. -Текст: электронный.

9. Спеваков, А. Г. Основы правового обеспечения информационной безопасности [Текст] : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013 - .Ч. 1. - 150 с.

10. Спеваков, А. Г. Основы правового обеспечения информационной безопасности [Текст] : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013 - .Ч. 2. - 303 с.

8.3 Перечень методических указаний

1. Общие вопросы обработки сигналов в программе Adobe Audition : [Электронный ресурс] : методические указания по выполнению практической работы по дисциплине «Информационная безопасность телекоммуникационных систем» / Юго-Зап. гос. ун-т ; сост.: В. Л. Лысенко, М. А. Ефремов. - Курск : ЮЗГУ, 2017. - 14 с.

2. Маскировка тонального телефонного сигнала путем его зашумления [Электронный ресурс]: методические указания по выполнению практической работы по дисциплине «Информационная безопасность телекоммуникационных систем» / Юго-Зап. гос. ун-т; сост.: В. Л. Лысенко, М. А. Ефремов. – Курск : ЮЗГУ, 2017. - 8 с.

3. Определение неизвестного номера абонента аналоговой телефонной сети путем спектральной оценки частотных параметров его сигналов [Электронный ресурс]: методические указания по выполнению практической работы по дисциплине «Информационная безопасность телекоммуникационных систем» / Юго-Зап. гос. ун-т; сост.: В. Л. Лысенко, М. А. Ефремов. - Курск : ЮЗГУ, 2017. - 11 с.

4. Обработка тотальных сигналов набора номера [Электронный ресурс]: методические указания по выполнению практической работы по дисциплине «Информационная безопасность телекоммуникационных систем» / Юго-Зап. гос. ун-т; сост.: В. Л. Лысенко, М. А. Ефремов. - Курск : ЮЗГУ, 2017. - 13 с.

5. Исследование методов защиты абонентского терминала сотовой связи GSM в системе Android [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Защита информации в системах беспроводной связи» для студентов укрупненной группы специальностей 10.05.02 / Юго-Зап. гос. ун-т ; сост.: В. Л. Лысенко, М. А. Ефремов. - Курск : ЮЗГУ, 2017. - 9 с.

8.4 Другие учебно-методические материалы

Периодические издания:

1. «Защита информации. Инсайд» [Текст] : информ.-метод. журн./ учредитель ООО "Издательский дом "Афина". - Санкт- Петербург : Афина. - Выходит раз в два месяца
2. Журнал «Information Security/Информационная безопасность.» - http://window.edu.ru/
3. Журнал «Проблемы информационной безопасности. Компьютерные системы» - http://window.edu.ru/
4. Журнал «Вестник УрФО. Безопасность в информационной сфере»
5. Журнал «Вопросы защиты информации»
6. Журнал «БДИ (Безопасность. Достоверность. Информация.)»
7. Журнал «Информация и безопасность»

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://e.lanbook.com - Электронно-библиотечная система «Лань».
2. http://www.iqlib.ru - Электронно-библиотечная система IQLib.
3. http://window.edu.ru -Электронная библиотека «Единое окно доступа к образовательным ресурсам».
4. http://biblioclub.ru – Электронно-библиотечная система «Университетская библиотека онлайн».
5. http://www.fsb.ru - Федеральная служба безопасности [официальный сайт].
6. http://fstec.ru - Федеральная служба по техническому и экспортному контролю [официальный сайт].
7. http://microsoft.com - Корпорация Microsoft[официальный сайт].
8. http://www.consultant.ruКомпания«Консультант Плюс» [официальный сайт].

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Информационная безопасность инфокоммуникаций» являются лекции и практические работы. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации

для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают практические занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Практической работе предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Информационная безопасность инфокоммуникаций»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекций, участие в групповых и индивидуальных консультациях (собеседованиях). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепления освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Информационная безопасность инфокоммуникаций» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Информационная безопасность инфокоммуникаций» - закрепить

теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Программа хранения паролей Password Commander(свободное ПО).

Фаервол Comodo Firewall (свободное ПО).

Программа анализа защищенности операционной системы GFI LANguard Network Security Scanner.

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМС Канал»,

Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,

Windows 7, договор IT000012385

Антивирусная программа Kaspersky Internet Security.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для проведения занятий лекционного и практического типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноутбукASUSX50VLPMDT2330/14"/1024Mb/160Gb/сумка/проектор inFocusIN24+

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

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 при-

сутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. 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).

14.Лист дополнений и изменений, внесенных в рабочую программу Дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	Измененных	Заменённых	Аннулированных	новых			

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.О. декана факультета
Фундаментальной и прикладной информатики
(наименование ф-та полностью)

М.О. Таныгин
(подпись, инициалы, фамилия)

«31» 08 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность инфокоммуникаций

(наименование дисциплины)

ОПОП ВО 11.04.02 Инфокоммуникационные технологии и системы связи
(шифр согласно ФГОС и наименование направления подготовки (специальности))

направленность (профиль, специализация) «Проектирование устройств, систем и сетей телекоммуникаций»
наименование направленности (профиля, специализации)

форма обучения заочная
(очная, очно-заочная, заочная)

Курск – 2021

Рабочая программа дисциплины Информационная безопасность инфокоммуникаций в соответствии с ФГОС ВО – магистратура по направлению подготовки (специальности) 11.04.02 Инфокоммуникационные технологии и системы связи на основании учебного плана ОПОП ВО 11.04.02 Инфокоммуникационные технологии и системы связи, направленность Проектирование устройств, систем и сетей телекоммуникаций, одобренного Ученым советом университета (протокол №6 «26» 07 2021г.).

Рабочая программа дисциплины Информационная безопасность инфокоммуникаций обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 11.04.02 Инфокоммуникационные технологии и системы связи, направленность Проектирование устройств, систем и сетей телекоммуникаций на заседании кафедры информационной безопасности Протокол №1 «30» 08 2021г.

Зав. кафедрой Таныгин М.О.

Разработчик программы

к.т.н., доцент Ефремов М.А.

Согласовано: на заседании кафедры космического приборостроения и систем связи Протокол № 1 «27» 08 2021 г.

Зав. кафедрой Андронов В.Г.

Директор научной библиотеки Макаровская В.Г.

Рабочая программа дисциплины Информационная безопасность инфокоммуникаций пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 11.04.02 Инфокоммуникационные технологии и системы связи, направленность Проектирование устройств, систем и сетей телекоммуникаций, одобренного Ученым советом университета протокол №7«28» 02 2022 г., на заседании кафедры ИБ протокол №1 от 30.08.2022

(наименование кафедры, дата, номер протокола)

Зав. кафедрой Таныгин М.О.

Рабочая программа дисциплины Информационная безопасность инфокоммуникаций пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 11.04.02 Инфокоммуникационные технологии и системы связи, направленность Проектирование устройств, систем и сетей телекоммуникаций, одобренного Ученым советом университета протокол №9«27» 02 2023 г., на заседании кафедры ИБ протокол №1 от 30.08.2023

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

1 Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1 Цель дисциплины

Целью преподавания дисциплины «Информационная безопасность инфокоммуникаций» (ИнБИ) сформировать основы знаний по принципам построения телекоммуникационных систем (ТКС), а также ознакомление с методами, средствами и системами обеспечения их информационной безопасности.

1.2 Задачи дисциплины

Основными задачами изучения дисциплины является:

- определение места и значения ИНБИ
- в системе принятия хозяйственных решений и ее роли как превентивного механизма
- предупреждения негативных последствий вредоносных воздействий объективного и субъективного характера на функционирование ТКС; ознакомление с принципами передачи сообщений в основных сетях связи, ознакомление с основами информационной безопасности
- систем и сетей связи, ознакомление с методами несанкционированного извлечения информации из сигналов и сообщений различных систем связи.

Знания и умения, которыми должен обладать студент, успешно освоивший данную дисциплину:

- знание уязвимостей основных телекоммуникационных технологий, средств и
- методов обеспечения их информационной безопасности, умение анализировать безопасность
- функционирования ТКС, а также оценивать уязвимость их протоколов и интерфейсов.

1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)	*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*

код компетенции	*наименование компетенции*		
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий		УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними	***Знать:*** критерии соответствия функционала подсистем информационной безопасности угрозам для объектов информатизации ***Уметь:*** выбирать требуемые политики безопасности при обеспечении безопасности ИКС ***Владеть:*** навыками реагирования на нештатные ситуации, возникающие при эксплуатации компонентов безопасности ИКС
		УК-1.2 Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению	***Знать:*** основные угрозы работоспособности прогаммным компонентам СЗИ ***Уметь:*** выявлять каналы утчки информациив ИКС ***Владеть:*** использования особенностей информации, циркулирующей в ИКС, для обеспечения ИБ
		УК-1.3 Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источник	***Знать:*** порядок внедрения, отладки и развития процессов и этапов разработки требований, критериев качества и методов обеспечения информационной безопасности прикладных ИС в процессе их эксплуатации. ***Уметь:*** организовать и управлять внедрением, отладкой и развитием процессами и этапами разработки требований, критериев качества и методов обеспечения информационной безопасности прикладных ИС в процессе их эксплуатации. ***Владеть:*** навыками организации и управления внедрением, отладкой и развитием процессами и этапами разработки требований, критериев качества и методов обеспечения информационной безопасности прикладных ИС в процессе их эксплуатации.

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
		УК-1.4 Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подход	***Знать:*** процессы, этапы разработки и сопровождения требований к информационной безопасности эксплуатируемых прикладных информационных систем (ИС). ***Уметь:*** организовать описание процессов и этапов разработки требований к информационной безопасности прикладных ИС в процессе их эксплуатации. ***Владеть:*** навыками организации описания процессов и этапов разработки требований к информационной безопасности прикладных ИС в процессе их эксплуатации.
		УК-1.5 Использует логико-методологический инструментарий для критической оценки современных концепций философского и социального характера в своей предметной области	***Знать:*** требования к качеству требований и методов обеспечения информационной безопасности прикладных ИС в процессе их эксплуатации; методы защиты информации, способы защиты информационных систем, методы анализа угроз и оценки рисков информационной безопасности ИС. ***Уметь:*** организовать создание и развитие требований к качеству требований и методов обеспечения информационной безопасности прикладных ИС в процессе их эксплуатации; применять средства защиты информации для решения практических задач в области защиты компьютерных систем и сетей; проводить анализ информационных рисков.

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			Владеть: навыками организации создания и развития требования к качеству требований и методов обеспечения информационной безопасности прикладных ИС в процессе их эксплуатации, применения программных средств защиты информации, разработки архитектуры сетевой защиты.
ОПК-2	Способен реализовывать новые принципы и методы исследования современных инфокоммуникационных систем и сетей различных типов передачи, распределения, обработки и хранения информации	ОПК-2.1 Использует принципы и методы исследования современных инфокоммуникационных систем, оценивая их достоинства и недостатки	***Знать:*** номенклатуру современных программно-аппаратных средств современных инфокоммуникационных систем; назначение, организацию и принципы функционировании программно-аппаратных средств современных инфокоммуникационных систем; механизмы защиты программно-аппаратных средств современных инфокоммуникационных систем, основные этапы аудита состава и конфигурации прикладной современных инфокоммуникационных систем, в том числе номенклатуру покупных и вновь разрабатываемых аппаратных средств ИС. ***Уметь:*** устанавливать современные программные средства, подключать аппаратные средства современных инфокоммуникационных систем; настраивать операционные системы и их подсистемы; сопоставлять структурную организацию программных и аппаратных средств требова-

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			ниям политики безопасности; проводить анализ угроз, рисков, применять антивирусные программные комплексы, настраивать режимы работы межсетевых экранов; проводить основные этапы аудита состава и конфигурации прикладной современных инфокоммуникационных систем, в том числе покупных и вновь разрабатываемых программных средства ИС. ***Владеть:*** навыками оценки эффективности программно-аппаратных средств; реализации требуемых политик безопасности с помощью современных программно-аппаратных средств защиты информации; проведения проверок работоспособности и эффективности применения программно-аппаратных средств; проведения основных этапов аудита состава и конфигурации прикладной ИС, в том числе покупных и вновь разрабатываемых аппаратных средств ИС.
		ОПК-2.2 Оперирует основными методами и средствами проведения экспериментальных исследований систем передачи, распределения, обработки и хранения информации	***Знать:*** методологию и основные технические средства для проведения экспериментальных исследований защищенных систем передачи данных. ***Уметь:*** проводить экспериментальные исследования систем передачи, распределения, обработки и хранения информации

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			Владеть: навыками определения характеристик систем передачи, распределения, обработки и хранения информации
		ОПК-2.3 Использует новые принципы и методы обработки и передачи информации в современных инфокоммуникационных системах и сетях	***Знать:*** номенклатуру современных программно-аппаратных средств ИС; назначение, организацию и принципы функционировании программно-аппаратных средств ИС; механизмы защиты программно-аппаратных средств ИС; классификацию и архитектуру ИС. ***Уметь:*** сопоставлять структурную организацию программных и аппаратных средств требованиям политики безопасности; проводить анализ угроз, рисков, применять антивирусные программные комплексы, проводить анализ защищенности локальной вычислительной сети, проводить анализ информационных рисков; проводить основные этапы аудита состава и конфигурации прикладной ИС, в том числе вновь разрабатываемых программных и аппаратных средств ИС. ***Владеть:*** навыками проведения проверок работоспособности и эффективности применения программно-аппаратных средств, защиты информации в компьютерных системах, анализа защищенности современных ин-

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			фокоммуникационных систем и сетей.
		ОПК-2.4 Анализирует передовой отечественный и зарубежный опыт исследования современных инфокоммуникационных систем и /или их составляющи	***Знать:*** источники новой научно-технической информации в области обеспечения безопасности современных инфокоммуникационных систем и сетей. ***Уметь:*** проводить сравнительный анализ предлагаемых решений в области обеспечения безопасности современных инфокоммуникационных систем и сетей ***Владеть:*** навыками реферирования источников научно-технической информации в области обеспечения безопасности современных инфокоммуникационных систем и сетей

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Информационная безопасность инфокоммуникаций» входит в обязательную часть блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы магистратуры 11.04.02 Инфокоммуникационные технологии и системы связи, направленность Проектирование устройств, систем и сетей телекоммуникаций. Дисциплина изучается на 2 курсе.

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 4 зачетные единицы (з.е.), 144 академических часов.

Таблица 3 - Объём дисциплины

Виды учебной работы	Всего, Часов
Общая трудоемкость дисциплины	144
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	14
в том числе:	
Лекции	4
лабораторные занятия	0
практические занятия	10
Самостоятельная работа обучающихся (всего)	120,88
Контроль (подготовка к экзамену)	9
Контактная работа по промежуточной аттестации (всего АттКР)	0,12
в том числе:	
Зачет	не предусмотрен
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	0,12

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1.1 - Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел, (тема) дисциплины	Содержание
1	2	3
1	Введение.	Информация, основные информационные процессы, классификация информации, угрозы информационной безопасности. Основные виды телекоммуникационных систем (ТКС), предмет дисциплины «Информационная безопас-
2	Основные понятия информационной безопасности ТКС	Доктрина информационной безопасности РФ и ее основные составляющие, понятия «угрозы» и «несанкционированного доступа» (НСД), основные угрозы безопасности и их классификация (угрозы доступности, целостности и конфиденциальности). Уровни обеспечения информационной безопасности ТКС. Основные программно-технические меры обеспечения информационной безопасности ТКС.

3	Информационная безопасность систем передачи речевой информации	Системы телефонной связи и их классификация; аналоговые и цифровые системы телефонной связи с коммутацией каналов, угрозы безопасности и методы защиты; организационные и организационно-технические, аппаратные и программно-аппаратные методы защиты, методы скремблиро-
4	Информационная безопасность систем волоконно-оптической связи (ВОЛС)	Особенности оптических систем связи, уязвимости и каналы утечки информации, методы НСД, аппаратные и программные методы защиты.
5	Инфокоммуникационная безопасность систем сотовой связи.	Архитектура сети GSM, угрозы информационной безопасности в системах сотовой связи GSM, методы и средства обеспечения безопасности в системах GSM.

Таблица 4.1.2 - Содержание дисциплины и ее методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		Лек. час	№ лаб	№ пр.			
1	2	3	4	5	6	7	8
1	Введение.	0,5		1	У-1, МУ-1	С	УК-1, ОПК-2
2	Основные понятия информационной безопасности ТКС	0,5		2	У-1-3, МУ-2	С	УК-1, ОПК-2
3	Информационная безопасность систем передачи речевой информации	1		3	У-1, МУ-3	С	УК-1, ОПК-2
4	Информационная безопасность систем волоконно-оптической связи	1			У-2,8	С	УК-1, ОПК-2
5	Инфокоммуникационная безопасность систем сотовой связи.	1		4,5	У-1,9 МУ-4,5	С	УК-1, ОПК-2
	Всего	4	-	5			

С – собеседование

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Практические занятия

Таблица 4.2.1 - Практические занятия

№	Наименование практического (семинарского) занятия	Объем, час.
1	Общие вопросы обработки сигналов в программе Adobe Audition	2
2	Маскировка речевого сигнала путем его зашумления	2
3	Определение неизвестного номера абонента аналоговой телефонной сети путем спектральной оценки частотных параметров его сигналов	2
4	Обработка тональных сигналов набора номера	2
5	Исследование методов защиты абонентского терминала сотовой связи GSM в системе Android	2
Итого		10

4.2 Самостоятельная работа студентов (СРС)

Таблица 4.2 - Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	Введение.	1-3 недели	24,88
2	Основные понятия информационной безопасности ТКС	4-6 недели	24
3	Информационная безопасность систем передачи речевой информации	7-10 недели	24
4	Информационная безопасность систем волоконно-оптической связи (ВОЛС)	11-14 недели	24
5	Инфокоммуникационная безопасность систем сотовой связи.	15-18 недели	24
Итого			120,88

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным обо-

рудованием и методическими разработками кафедры в рабочее время, установленное «Правилами внутреннего распорядка работников».

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

– библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

– имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

– путем обеспечения доступности всего необходимого учебно- методического и справочного материала за счёт выкладывания на сайт кафедры ИБ в интернете (адрес http://www.swsu.ru/structura/up/fivt/k_tele/index.php);

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

путем разработки:

- методических рекомендаций, пособий по организации самостоятельной работы студентов;

– заданий для самостоятельной работы;

– вопросов и задач к зачёту;

–методических указаний к выполнению лабораторных и практических работ и т.д.

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

–удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6. Образовательные технологии

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования профессиональных компетенций обучающихся. В рамках дисциплины предусмотрены встречи с экспертами и специалистами Комитета цифрового развития и связи Курской области.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения основной профессиональной образовательной программы

Таблица 7.1 - Этапы формирования компетенций

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули) и практики, при изучении/прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Профессиональный иностранный язык Информационная безопасность инфокоммуникаций Учебная практика (научно-исследовательская работа)	Профессиональный иностранный язык Философские и психологические проблемы творчества Учебная технологическая (проектно-технологическая) практика	Выполнение и защита выпускной квалификационной работы
ОПК-2. Способен реализовывать новые принципы и методы исследования современных инфокоммуникационных систем и сетей различных типов передачи, распределения, обработки и хранения информации	Теория построения инфокоммуникационных сетей и систем Информационная безопасность инфокоммуникаций Учебная практика (научно-исследовательская работа)	Методы моделирования и оптимизации в инфокоммуникациях Учебная технологическая (проектно-технологическая) практика	Выполнение и защита выпускной квалификационной работы

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 7.2 Показатели, критерии и шкала оценивания компетенций

Код компетенции/ этап	Показатели оценивания компе-	Критерии и шкала оценивания компетенций

(указывается название этапа изп.7.1)	тенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	*2*	3	4	5
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий (Начальный)	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними	Знать: основные понятия теории проектирования инфокоммуникационных систем Уметь: анализировать взаимосвязи между составом технических средств ИКС и угрозами информационной безопасности Владеть: анализа угроз безопасности ИКС	Знать: принципы организации подсистем безопасности инфокоммуникационных систем Уметь: настраивать компонентов безопасности ИКС Владеть: обеспечения безопасности информации циркулирующей в ИКС	Знать: критерии соответствия функционала подсистем информационной безопасности угрозам для объектов информатизации Уметь: выбирать требуемы политики безопасности при обеспечении безопасности ИКС Владеть: реагировании на нештатные ситуации, возникающие при эксплуатации компонентов безопасности ИКС
	УК-1.2 Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению	Знать: используемые в работе с ИКС программные средства Уметь: анализировать угрозы безопасности в ИКС Владеть: навыками выбора средств обеспечения информационной безопасности ИКС	Знать: инструментальные средства проведения проверок информационных систем Уметь: использовать в работе программные средства обеспечения информационной безопасности ИКС Владеть: эксплуатации средств обеспечения ин-	Знать: основные угрозы работоспособности прогаммным компонентам СЗИ Уметь: выявлять каналы утчки информациив ИКС Владеть: использования особенностей информации,

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	*2*	3	4	5
			формационной безопасности ИКС	циркулирующей в ИКС, для обеспечения ИБ
	УК-1.3 Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источник	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защи-

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	*2*	3	4	5
				щенных сайтов, разработки архитектуры сетевой защиты.
	УК-1.4 Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подход	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защит информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разра-

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	*2*	3	4	5
				ботки защищенных сайтов, разработки архитектуры сетевой защиты.
	УК-1.5 Использует логико-методологический инструментарий для критической оценки современных концепций философского и социального характера в своей предметной области	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информа-

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	*2*	3	4	5
				ции, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
ОПК-2 Способен реализовывать новые принципы и методы исследования современных инфокоммуникационных систем и сетей различных типов передачи, распределения, обработки и хранения информации (Начальный)	ОПК-2.1 Использует принципы и методы исследования современных инфокоммуникационных систем, оценивая их достоинства и недостатки	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защи-

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	*2*	3	4	5
				ты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
	ОПК-2.2 Оперирует основными методами и средствами проведения экспериментальных исследований систем передачи, распределения, обработки и хранения информации	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	*2*	3	4	5
				средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	*2*	3	4	5
	ОПК-2.3 Использует новые принципы и методы обработки и передачи информации в современных инфокоммуникационных системах и сетях	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	Знать: методы защиты информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	Знать: методы защиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.
	ОПК-2.4 Анализирует пе-	Знать: методы защиты	Знать: методы защиты	Знать: методы за-

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	*2*	3	4	5
	редовой отечественный и зарубежный опыт исследования современных инфокоммуникационных систем и /или их составляющие	информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: навыками применения программных средств защиты информации.	информации, способы защиты сайтов. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов.	щиты информации, способы защиты сайтов, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, разрабатывать защищенные сайты, проводить анализ информационных рисков. Владеть: навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры сетевой защиты.

7.3Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

Таблица 7.3 Паспорт комплекта оценочных средств для текущего контроля успеваемости

п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№ заданий	
1	2	3	4	5	6	7
1.	Введение.	УК-1, ОПК-2	Лекция, СРС, практическое занятие	Собеседование	1-3	Согласно табл.7.2
				КВЗПР №1	1-3	
2.	Основные понятия информационной безопасности ТКС	УК-1, ОПК-2	Лекция, СРС, практическое занятие	Собеседование,	1-4	Согласно табл.7.2
				КВЗПР №2	1-4	
3.	Информационная безопасность систем передачи речевой информации	УК-1, ОПК-2	Лекция, СРС, практическое занятие	собеседование	1-7	Согласно табл.7.2
				КВЗПР №3	1-7	
4.	Информационная безопасность систем волоконно-оптической связи (ВОЛС)	УК-1, ОПК-2	Лекция, СРС,	Собеседование	1-3	Согласно табл.7.2
5.	Инфокоммуникационная безо-	УК-1, ОПК-2	Лекция, СРС, практическое	Собеседование	1-3	Согласно табл.7.2

	пасность систем сотовой связи.		занятие	КВЗПР №4,5	1-3	

СРС – самостоятельная работа студента, КВЗПР - контрольные вопросы для защиты практических работ

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного опроса по разделу (теме) 3. «Информационная безопасность систем передачи речевой информации».

1. Системы телефонной связи и их классификация.
2. Аналоговые и цифровые системы телефонной связи с коммутацией каналов
3. Перечислите угрозы безопасности и методы защиты.
4. Перечислите организационные и организационно-технические, аппаратные и программно-аппаратные методы защиты,
5. Опишите методы скремблирования, методы и средства шифрации, системы сигнализации,
6. Назовите угрозы безопасности и методы защиты; системы телефонной связи с коммутацией пакетов (VoIP-системы),
7. Охарактеризуйте угрозы безопасности и общие методы защиты, методы защиты технологий VoIP H.323 и SIP

Контрольные вопросы для защиты практической работы № 1:

1. Что такое дискретизация аналогового сигнала?
2. Что такое АИМ-сигнал?
3. Как происходит кодирование АИМ-сигнала?
4. Объяснить метод преобразования (оцифровки) аналогового сигнала в цифровой
5. Что такое информация?
6. На сколько категорий подразделяются все виды информации (кратко охарактеризовать каждую)?
7. Что такое инфокоммуникационная безопасность?
8. Что такое защита информации?
9. Что такое утечка информации?
10. На какие виды (по назначению) можно условно разделить системы передачи информации?

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

Типовые задания для проведения промежуточной аттестации обучающихся. Промежуточная аттестация по дисциплине проводится в форме экзамена.

Промежуточная аттестация по дисциплине проводится в форме экзамена. Экзамен проводится в виде компьютерного тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки (или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

1. Какая угроза информационной безопасности является пассивной:
А) Копирование секретных данных.
Б) Внедрение вредоносного программного обеспечения.

В) Кража носителей информации.
Г) Удаление файла.

Задание в открытой форме:

1. Угрозы нарушения целостности информации приводят к …….
2. В автоматизированной системе перехват данных, передаваемых по каналам связи относится к уровню ……..
3. Пассивной угрозой информационной безопасности является ……...

Задание на установление правильной последовательности.

Установить в порядке увеличения единицы измерения количества информации:

1. 1 ТБ

2. 30 Гбайт

3. 50 Килобайт

4. 100 Мегабайт

Задание на установление соответствия:

между элементами ПК и функциями элементов

1	Процессор	А	Хранение информации
2	Оперативная память	Б	Обработка информации
3	Жесткий диск	В	Отображение информации
4	Монитор	Г	Ввод информации

способов и видов информации

1	По способу кодирования	А	Цифровая, аналоговая
2	По способу представления	Б	Визуальная, звуковая, документ
3	По способу обработки	В	Текстовая, графическая, числовая
4	По способу восприятия	Г	Непрерывная, дискретная

Компетентностно-ориентированная задача:

Определить минимальную длину кодового слова с возможностью исправления 3-х кратных ошибок при кодировании информации длиной 8 бит.

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

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

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– положение П 02.016–2018 О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Устный опрос по темам 1-2	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по темам 3-4	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Устный опрос по темам 5	1	Доля правильных ответов от 50% до 90%	2	Доля правильных ответов более 90%
Выполнение практической работы №1 «Общие вопросы обработки сигналов в программе Adobe Audition»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Выполнение практической работы №2 «Маскировка речевого сигнала путем его	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%

зашумления»				
Выполнение практической работы №3 «Определение неизвестного номера абонента аналоговой телефонной сети путем спектральной оценки частотных параметров его сигналов»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Выполнение практической работы №4 «Обработка тональных сигналов набора номера»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Выполнение практической работы №5 «Исследование методов защиты абонентского терминала сотовой связи GSM в системе Android»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Итого	18		36	
Посещаемость	0		14	
Экзамен	0		60	
Итого	18		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме –2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование –60 баллов.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1. Спеваков, Александр Геннадьевич. Информационная безопасность : учебное пособие : [для студентов, обучающихся по специальностям 100301 «Информационная безопасность», 400301 «Юриспруденция», 380301 «Экономика»] / А. Г. Спеваков, М. О. Таныгин, В. С. Панищев ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2017. - 196 с. : ил., табл. - Библиогр.: с. 188-195. - ISBN 978-5-7681-1196-0 : 290.00 р. - Текст : непосредственный.

2. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учебник для студентов вузов, обучающихся по направлению 552800 "Информатика и вычислительная техника" и по специальностям 220100 "Вычислительные машины, комплексы, системы и сети", 220200 "Автоматизированные системы обработки информации и управления" и 220400 "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Г. Олифер, Н. А. Олифер. - 5-е изд. - Санкт-Петербург : Питер, 2019. - 922 с.

3. Проскуряков, А. В. Компьютерные сети: основы построения компьютерных сетей и телекоммуникаций : учебное пособие / А. В. Проскуряков ; Министерство науки и высшего образования Российской Федерации ; Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» ; Инженерно-технологическая академия. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 202 с. : ил. - URL: http://biblioclub.ru/index.php?page=book&id=561238 - (дата обращения 15.07.2019) . - Режим доступа: по подписке. - Библиогр.: с. 195-196. - ISBN 978-5-9275-2792-2. - Текст : электронный.

8.2 Дополнительная учебная литература

4. Грибунин, В. Г. Комплексная система защиты информации на предприятии [Текст] : учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М.: Академия, 2009. - 416 с.

5. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - Санкт-Петербург : Питер, 2015. - 943 с.

6. Нужнов, Е. В. Компьютерные сети [Электронный ресурс] : учебное пособие / Е. В. Нужнов. - Таганрог : Издательство Южного федерального университета, 2015 -Ч. 2. Технологии локальных и глобальных сетей. - 2015. - 176 с. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=461991

7. Подольский, В. И. Компьютерные информационные системы в аудите [Электронный ресурс] : учебное пособие / В. И. Подольский, Н. С. Щербакова, В. Л. Комиссаров. - Москва : Юнити-Дана, 2015. - 160 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=115315.

8. Безбогов, А. А. Методы и средства защиты компьютерной информации : учебное пособие / А. А. Безбогов, А. Я. Яковлев, В. Н.

Шамкин. - Тамбов : ТГТУ, 2006. - 196 с. - URL: http://window.edu.ru/resource/546/38546. -Текст: электронный.

9. Спеваков, А. Г. Основы правового обеспечения информационной безопасности [Текст] : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013 - .Ч. 1. - 150 с.

10. Спеваков, А. Г. Основы правового обеспечения информационной безопасности [Текст] : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013 - .Ч. 2. - 303 с.

8.3 Перечень методических указаний

1. Общие вопросы обработки сигналов в программе Adobe Audition : [Электронный ресурс] : методические указания по выполнению практической работы по дисциплине «Информационная безопасность телекоммуникационных систем» / Юго-Зап. гос. ун-т ; сост.: В. Л. Лысенко, М. А. Ефремов. - Курск : ЮЗГУ, 2017. - 14 с.

2. Маскировка тонального телефонного сигнала путем его зашумления [Электронный ресурс]: методические указания по выполнению практической работы по дисциплине «Информационная безопасность телекоммуникационных систем» / Юго-Зап. гос. ун-т; сост.: В. Л. Лысенко, М. А. Ефремов. – Курск : ЮЗГУ, 2017. - 8 с.

3. Определение неизвестного номера абонента аналоговой телефонной сети путем спектральной оценки частотных параметров его сигналов [Электронный ресурс]: методические указания по выполнению практической работы по дисциплине «Информационная безопасность телекоммуникационных систем» / Юго-Зап. гос. ун-т; сост.: В. Л. Лысенко, М. А. Ефремов. - Курск : ЮЗГУ, 2017. - 11 с.

4. Обработка тотальных сигналов набора номера [Электронный ресурс]: методические указания по выполнению практической работы по дисциплине «Информационная безопасность телекоммуникационных систем» / Юго-Зап. гос. ун-т; сост.: В. Л. Лысенко, М. А. Ефремов. - Курск : ЮЗГУ, 2017. - 13 с.

5. Исследование методов защиты абонентского терминала сотовой связи GSM в системе Android [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплине «Защита информации в системах беспроводной связи» для студентов укрупненной группы специальностей 10.05.02 / Юго-Зап. гос. ун-т ; сост.: В. Л. Лысенко, М. А. Ефремов. - Курск : ЮЗГУ, 2017. - 9 с.

8.4 Другие учебно-методические материалы

Периодические издания:

1. «Защита информации. Инсайд» [Текст] : информ.-метод. журн./ учредитель ООО "Издательский дом "Афина". - Санкт- Петербург : Афина. - Выходит раз в два месяца
2. Журнал «Information Security/Информационная безопасность.» - http://window.edu.ru/
3. Журнал «Проблемы информационной безопасности. Компьютерные системы» - http://window.edu.ru/
4. Журнал «Вестник УрФО. Безопасность в информационной сфере»
5. Журнал «Вопросы защиты информации»
6. Журнал «БДИ (Безопасность. Достоверность. Информация.)»
7. Журнал «Информация и безопасность»

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://e.lanbook.com - Электронно-библиотечная система «Лань».
2. http://www.iqlib.ru - Электронно-библиотечная система IQLib.
3. http://window.edu.ru -Электронная библиотека «Единое окно доступа к образовательным ресурсам».
4. http://biblioclub.ru – Электронно-библиотечная система «Университетская библиотека онлайн».
5. http://www.fsb.ru - Федеральная служба безопасности [официальный сайт].
6. http://fstec.ru - Федеральная служба по техническому и экспортному контролю [официальный сайт].
7. http://microsoft.com - Корпорация Microsoft[официальный сайт].
8. http://www.consultant.ruКомпания«Консультант Плюс» [официальный сайт].

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Информационная безопасность инфокоммуникаций» являются лекции и практические работы. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации

для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают практические занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Практической работе предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Информационная безопасность инфокоммуникаций»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекций, участие в групповых и индивидуальных консультациях (собеседованиях). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепления освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Информационная безопасность инфокоммуникаций» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Информационная безопасность инфокоммуникаций» - закрепить

теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Программа хранения паролей Password Commander(свободное ПО).

Фаервол Comodo Firewall (свободное ПО).

Программа анализа защищенности операционной системы GFI LANguard Network Security Scanner.

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМС Канал»,

Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,

Windows 7, договор IT000012385

Антивирусная программа Kaspersky Internet Security.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для проведения занятий лекционного и практического типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноутбукASUSX50VLPMDT2330/14"/1024Mb/160Gb/сумка/проектор inFocusIN24+

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

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 при-

сутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. 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).

14.Лист дополнений и изменений, внесенных в рабочую программу Дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	Измененных	Заменённых	Аннулированных	новых			