Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ И ДИЗАЙНА»

УТВЕРЖДАЮ
Первый проректор, проректор по учебной работе

_____ А.Е. Рудин

«30» 06 2020 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.07	Защита информационных и телекоммуникационных систем
(Индекс дисциплины)	*(Наименование дисциплины)*

Кафедра: 20 Интеллектуальных систем и защиты информации
Код *Наименование кафедры*

Направление подготовки: 10.03.01 Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем (в коммерческих структурах)

Уровень образования: **бакалавриат**

План учебного процесса

Составляющие учебного процесса		Очное обучение	Очно-заочное обучение	Заочное обучение
Контактная работа обучающихся с преподавателем по видам учебных занятий и самостоятельная работа обучающихся (часы)	Всего	324		
	Аудиторные занятия	125		
	Лекции	54		
	Лабораторные занятия	17		
	Практические занятия	54		
	Самостоятельная работа	163		
	Промежуточная аттестация	36		
Формы контроля по семестрам (номер семестра)	Экзамен	8		
	Зачет	7		
	Контрольная работа			
	Курсовой проект (работа)			
Общая трудоемкость дисциплины (зачетные единицы)		9		

Форма обучения:	Распределение зачетных единиц трудоемкости по семестрам											
	1	2	3	4	5	6	7	8	9	10	11	12
Очная							4	5				
Очно-заочная												
Заочная												

Санкт-Петербург
2020

Программа государственной итоговой аттестации составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по соответствующему направлению подготовки

и на основании учебного плана № 1/1/704

1. ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1. Место преподаваемой дисциплины в структуре образовательной программы

Блок 1:	Базовая		Обязательная	X	Дополнительно является факультативом
	Вариативная	X	По выбору		

1.2. Цель дисциплины

Сформировать компетенции обучающегося в области защиты современных информационных и телекоммуникационных систем.

1.3. Задачи дисциплины

- Рассмотреть теоретические аспекты в области построения и функционирования защиты информационных систем;
- Раскрыть принципы современных информационных технологий, предназначенных для оптимизации процесса безопасности телекоммуникаций;
- Продемонстрировать особенности современных методов защиты информационных систем и телекоммуникаций.

1.4. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Формулировка компетенции	Этап формирования
ПК-3	Способность администрировать подсистемы информационной безопасности объекта защиты	Второй
Планируемые результаты обучения Знать: 1) технологии обнаружения компьютерных атак и их возможности Уметь: 1) использовать программные продукты, выявляющие недостатки систем защиты Владеть: 1) средствами администрирования систем обнаружения компьютерных атак		
ПК-4	Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Второй
Планируемые результаты обучения Знать: 1) Методики управления процессом информационной безопасности Уметь: 1) Управлять процессами, оценивать и контролировать качество процесса управления информационной безопасностью Владеть: 1) Навыками согласования (отклонение) ключевых решений по информационной безопасности ресурсов ИТ		
ПК-12	Способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Второй
Планируемые результаты обучения Знать: 1) Задачи защиты информации телекоммуникационных систем Уметь: 1) выполнять установку специализированного оборудования для максимальной защищенности объекта Владеть: 1) Навыками конфигурировании автоматизированных систем и информационно-коммуникационных сетей		

1.5. Дисциплины (практики) образовательной программы, в которых было начато формирование компетенций, указанных в п.1.4:

- Сети и системы передачи информации (ПК-3)
- Операционные системы (ПК-3)
- Среды и оболочки операционных систем с открытым кодом (ПК-3)
- Безопасность корпоративных компьютерных сетей (ПК-3)
- Основы информационной безопасности (ПК-4)
- Аппаратные средства вычислительной техники (ПК-6)
- Программно-аппаратные средства защиты информации (ПК-6)

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
Учебный модуль 1. Основы информационной безопасности в сфере телекоммуникаций.			
Тема 1. Классификация и анализ угроз информационной безопасности в многоканальных телекоммуникационных системах. Виды уязвимости информации и формы ее проявления	15		
Тема 2. Уровни информационной безопасности – законодательно-правовой, административно-организационный, программно-технический. Принципы построения систем защиты информации.	15		
Текущий контроль 1 (опрос)	2		
Учебный модуль 2. Технология применения комплексной системы защиты информации.			
Тема 3. Информационная безопасность в многоканальных телекоммуникационных системах и сетях электросвязи.	16		
Тема 4. Структурные схемы систем защиты информации в типовых информационных системах. Показатели защищенности телекоммуникационных систем.	16		
Текущий контроль 2 (опрос)	2		
Учебный модуль 3. Сервисы, атаки, вирусы, криптозащита.			
Тема 5. Сервисы, обеспечивающие информационную безопасность в телекоммуникационных системах и сетях электросвязи: ограничение физического доступа к автоматизированным системам; идентификация и аутентификация пользователей; ограничение доступа в систему; разграничение доступа; регистрация событий (аудит).	17		
Тема 6. Криптографическая защита; контроль целостности; управление политиками безопасности; уничтожение остаточной информации; резервирование данных; сетевая защита; защита от утечки и перехвата информации по техническим каналам. Подсистемы безопасности.	16		
Тема 7. Типовые удаленные сетевые атаки и их характеристика. Компьютерные вирусы и защита от них. Антивирусные программы и комплексы.	16		
Текущий контроль 3 (опрос)	2		
Учебный модуль 4. Системы защиты.			
Тема 8. Построение систем антивирусной защиты телекоммуникационных систем и сетей.	16		
Тема 9. Технологии защиты данных.	15		
Текущий контроль 4 (опрос)	2		
Учебный модуль 5. Технологии криптозащиты и межсетевого обмена.			
Тема 10. Принципы криптографической защиты информации (симметричные и асимметричные алгоритмы шифрования, электронная цифровая подпись, стеганография).	17		
Тема 11. Различные технологии аутентификации. Технологии защиты межсетевого обмена данных.	17		
Текущий контроль 5 (опрос)	2		
Промежуточная аттестация по дисциплине (зачет)	4		
Учебный модуль 6. Администрирование ОС.			
Тема 12. Администрирование телекоммуникационных систем и сетей связи.	15		
Тема 13. Технология обеспечения безопасности сетевых операционных систем.	16		
Текущий контроль 6 (опрос)	2		
Учебный модуль 7. VPN, Snort.			
Тема 14. Основы технологии виртуальных защищенных сетей VPN.	15		

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
Тема 15. Технология обнаружения вторжений (анализ защищенности и обнаружения сетевых атак).	16		
Текущий контроль 7 (опрос)	2		
Учебный модуль 8. НСД и технические средства защиты от него.			
Тема 16. Требования по защите от несанкционированного доступа.	15		
Тема 17. Технические средства обеспечения безопасности телекоммуникационных систем	15		
Текущий контроль 8 (опрос)	2		
Промежуточная аттестация по дисциплине (экзамен)	**36**		
ВСЕГО:	**324**		

3. ТЕМАТИЧЕСКИЙ ПЛАН

3.1. Лекции

Номера изучаемых тем	Очное обучение		Очно-заочное обучение		Заочное обучение	
	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
1	7	3				
2	7	3				
3	7	3				
4	7	3				
5	7	3				
6	7	3				
7	7	3				
8	7	3				
9	7	3				
10	7	3				
11	7	3				
12	8	3				
13	8	3				
14	8	3				
15	8	4				
16	8	4				
17	8	4				
ВСЕГО:		54				

3.2. Практические и семинарские занятия

Номера изучаемых тем	Наименование и форма занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
1	Защита конфиденциальной информации на рабочих станциях с помощью ПО Secret Disc. (практикум)	7	3				
2	Создание программного - аппаратного ключа для получения доступа. (практикум)	7	3				
3	Криптографические методы защиты информации. (практикум)	7	3				
4	Настройка и установка программного обеспечения биометрической системы. (практикум)	7	3				
5	Применение биометрической системы для разграничения прав доступа. (практикум)	7	3				

Номера изучаемых тем	Наименование и форма занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
6	Диагностика сетевых подключений с помощью встроенных утилит операционной системы Microsoft Windows. (практикум)	7	3				
7	Wireshark: выделение ключевых кадров, сохранение данных захвата, просмотр кадра в отдельном окне, печать. (практикум)	7	3				
8	Wireshark: анализ протоколов Ethernet и ARP. (практикум)	7	3				
9	Wireshark: анализ протоколов IP и ICMP. (практикум)	7	3				
10	Wireshark: анализ протокола TCP. (практикум)	7	3				
11	Настройка и конфигурирование VPN-туннелей L2, IP SEC L3, защищенные приложения L4 SSL, SSH. (практикум)	7	3				
12	Установка, настройка специализированного оборудования по защите информации. (практикум)	8	3				
13	Выявление возможных атак на автоматизированные системы. (практикум)	8	3				
14	Установка и настройка программных средств защиты автоматизированных систем и информационно-коммуникационных сетей. (практикум)	8	3				
15	Конфигурирование автоматизированных систем и информационно-коммуникационных сетей (практикум)	8	4				
16	Проверка защищенности автоматизированных систем и информационно-коммуникационных сетей (практикум)	8	4				
17	Организации защиты в различных операционных системах и средах. (практикум)	8	4				
		ВСЕГО:	54				

3.3. Лабораторные занятия

Номера изучаемых тем	Наименование и форма занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
1	Программная аутентификация и идентификация в сетевых операционных системах.	7	2				
2	Резервное копирование информации.	7	2				
3	Методы разграничения доступа в сетевых операционных системах.	7	1				
4	Регистрация и аудит в сетевой операционной системе.	7	1				
5	Методы защиты информации. Шифр простой перестановки. Шифр Цезаря.	7	2				

Номера изучаемых тем	Наименование и форма занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
6	Защита информации с помощью пароля. Количественная оценка стойкости парольной защиты.	7	1				
7	Применение антивирусной защиты в информационных системах.	7	2				
8	Программные решения механизмов межсетевого экранирования.	7	2				
9	Программно-аппаратные решения механизмов межсетевого экранирования.	7	2				
10	Защита информации с использованием криптографических шифров.	7	1				
11	Скрытая передача информации в изображениях.	7	1				
		ВСЕГО:	**17**				

4. КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Не предусмотрено

5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ ОБУЧАЮЩЕГОСЯ

Номера учебных модулей, по которым проводится контроль	Форма контроля знаний	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Кол-во	Номер семестра	Кол-во	Номер семестра	Кол-во
1-5	Опрос	7	5				
6-8	Опрос	8	3				

6. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ

Виды самостоятельной работы обучающегося	Очное обучение		Очно-заочное обучение		Заочное обучение	
	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
Усвоение теоретического материала	7 8	29 76				
Подготовка к практическим и лабораторным занятиям	7 8	26 28				
Подготовка к зачету	7	4				
Подготовка к экзамену	8	36				
	ВСЕГО:	199				

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

7.1. Характеристика видов и используемых инновационных форм учебных занятий

Наименование видов учебных занятий	Используемые инновационные формы	Объем занятий в инновационных формах (часы)		
		очное обучение	очно-заочное обучение	заочное обучение
Лекции	проблемная лекция, разбор конкретных ситуаций, лекция-диалог	27		
Лабораторные занятия	Проведение экспериментов при проектировании ЛВС в виртуальной среде	7		

Наименование видов учебных занятий	Используемые инновационные формы	Объем занятий в инновационных формах (часы)		
		очное обучение	очно-заочное обучение	заочное обучение
Практические и семинарские занятия	решения проблемных ситуаций (case-study), командное соревнование малых групп	27		
	ВСЕГО:	61		

7.2. Балльно-рейтинговая система оценивания успеваемости и достижений обучающихся

Перечень и параметры оценивания видов деятельности обучающегося

№ п/п	Вид деятельности обучающегося	Весовой коэффициент значимости, %	Критерии (условия) начисления баллов
1	Аудиторная активность: посещение лекций и практических (семинарских) и лабораторных занятий, прохождение промежуточного опроса	20	• 3 балла за каждое занятие (всего 17 занятия в семестре), максимум **51** баллов • 1 балл за каждый правильный ответ на вопрос опроса **текущего контроля** (всего 10 вопросов в опросе, три опроса в семестр), максимум **30** баллов • 19 баллов за ответ на дополнительный вопрос текущего контроля № 3
2	Выполнение и защита практических работ	40	• 3 баллов за каждую работу, всего 17 практических работ, максимум 51 баллов • Качество защиты (полнота ответов на вопросы, владение специальной терминологией, затраченное на ответы время) – максимум **49** баллов.
3	Сдача зачета	40	• Ответ на теоретический вопрос (полнота, владение терминологией, затраченное время) – максимум **40** баллов; • Решение практической задачи – до 60 баллов
	Итого (%):	100	

№ п/п	Вид деятельности обучающегося	Весовой коэффициент значимости, %	Критерии (условия) начисления баллов
1	Аудиторная активность: посещение лекций и практических (семинарских) и лабораторных занятий, прохождение промежуточного опроса	60	• 3 балла за каждое занятие (всего 17 занятия в семестре), максимум **51** баллов • 1 балл за каждый правильный ответ на вопрос опроса **текущего контроля** (всего 10 вопросов в опросе, три опроса в семестр), максимум **30** баллов • 19 баллов за ответ на дополнительный вопрос текущего контроля № 3
3	Сдача экзамена	40	• Ответ на теоретический вопрос (полнота, владение терминологией, затраченное время) – максимум **40** баллов; • Решение практической задачи – до 60 баллов
	Итого (%):	100	

Перевод балльной шкалы в традиционную систему оценивания

Баллы	Оценка по нормативной шкале	
86 - 100	5 (отлично)	Зачтено
75 – 85	4 (хорошо)	

61 – 74		
51 - 60	3 (удовлетворительно)	
40 – 50		
17 – 39	2 (неудовлетворительно)	Не зачтено
1 – 16		
0		

8. ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Учебная литература

а) основная учебная литература

1. Щеглов А.Ю. Математические модели и методы формального проектирования систем защиты информационных систем [Электронный ресурс]: учебное пособие/ А.Ю. Щеглов, К.А. Щеглов— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2015.— 93 с.— Режим доступа: http://www.iprbookshop.ru/67260.html.— ЭБС «IPRbooks»
2. Демидов А.А. Проблемы контроля безопасности информации на объектах телекоммуникационных систем органов государственного управления [Электронный ресурс]: учебное пособие/ А.А. Демидов— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2015.— 70 с.— Режим доступа: http://www.iprbookshop.ru/67555.html.— ЭБС «IPRbooks»
3. Чуянов А. Г. Проблемы защищенности телекоммуникационных систем [Электронный ресурс]: учебное пособие/ А. Чуянов— Электрон. текстовые данные.— Омск: Омская академия МВД России, 2015.— 164 с.— Режим доступа: http://www.iprbookshop.ru/61873.html.— ЭБС «IPRbooks»

б) дополнительная учебная литература

1. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс]: лабораторный практикум/ М.А. Лапина [и др.].— Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2016.— 242 с.— Режим доступа: http://www.iprbookshop.ru/62945.html.— ЭБС «IPRbooks»
2. Заляжных В.А. Экспертные системы комплексной оценки безопасности автоматизированных информационных и коммуникационных систем [Электронный ресурс]/ В.А. Заляжных, А.В. Гирик— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2014.— 139 с.— Режим доступа: http://www.iprbookshop.ru/65733.html.— ЭБС «IPRbooks»
3. Душин В.К. Теоретические основы информационных процессов и систем [Электронный ресурс]: учебник/ В.К. Душин— Электрон. текстовые данные.— М.: Дашков и К, 2014.— 348 с.— Режим доступа: http://www.iprbookshop.ru/24764.html.— ЭБС «IPRbooks»

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

1. Методы защиты информации [Электронный ресурс]: методические указания / Сост. Зурахов В. С. — СПб.: СПГУТД, 2016.— 47 с.— Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=3008, по паролю.
2. Сети и системы передачи информации [Электронный ресурс]: методические указания / Сост. Зурахов В. С., Макаров А. Г. — СПб.: СПГУТД, 2014.— 19 с.— Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=1814, по паролю.
3. Спицкий, С. В. Эффективная аудиторная и самостоятельная работа обучающихся: методические указания / С. В. Спицкий. – СПб.: СПбГУПТД, 2015. – Режим доступа: http://publish.sutd.ru/tp_get_file.php?id=2015811, по паролю.
4. Караулова, И. Б. Организация самостоятельной работы обучающихся / И. Б. Караулова, Г. И. Мелешкова, Г. А. Новоселов. – СПб.: СПГУТД, 2014. – 26 с. – Режим доступа http://publish.sutd.ru/tp_get_file.php?id=2014550, по паролю

8.3. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины

1. http://www.iprbookshop.ru
2. http://publish.sutd.ru/

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

1. Microsoft Office Standart 2016 Russian Open No Level Academic)
2. Microsoft Windows 10 Home Russian Open No Level Academic Legalization Get Genuine (GGK) + Microsoft Windows 10 Professional (Pro – профессиональная) Russian Upgrade Open No Level Academic

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

1. Стандартно оборудованная аудитория;
2. Персональный компьютер, оснащенный сетевым адаптером и доступом в Internet;
3. Проектор.

8.6. Иные сведения и (или) материалы

Не предусмотрены

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Виды учебных занятий и самостоятельная работа обучающихся	Организация деятельности обучающегося
Лекции	• проработка рабочей программы в соответствии с целями и задачами, структурой и содержанием дисциплины; • конспект лекций: кратко, схематично, последовательно фиксировать основные положения, выводы и формулировки; помечать важные мысли, выделять ключевые слова, термины. • Проверка терминов, понятий: осуществлять с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь; • работа с теоретическим материалом (конспектирование источников): найти ответ на вопросы в рекомендуемой литературе.
Практические занятия	• подготовка ответов к контрольным вопросам, опросам; • решение задач по алгоритму, решение кейсов
Лабораторные занятия	Лабораторные занятия способствуют развитию практических навыков владения изучаемыми методами, оборудованием, технологиями и др. в процессе взаимодействия со специально разработанными образцами реально действующего оборудования, предполагают проведение учебного эксперимента (самостоятельно либо под руководством преподавателя);
Самостоятельная работа	При подготовке к экзамену (зачету) необходимо ознакомиться с демонстрационным вариантом задания (теста, перечнем вопросов, пр.), проработать конспекты лекций и практических занятий, рекомендуемую литературу, получить консультацию у преподавателя, подготовить презентацию материалов.

10. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

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

10.1.1. Показатели оценивания компетенций на этапах их формирования

Код компетенции / этап освоения	Показатели оценивания компетенций	Наименование оценочного средства	Представление оценочного средства в фонде
ПК-3/второй	Перечисляет основные уязвимости и типовые атаки на современные информационные и телекоммуникационные системы и возможности их обнаружения	Вопросы для устного собеседования	Перечень вопросов для устного собеседования (17 вопросов)
	Сравнивает программы по обеспечению защиты информационных и телекоммуникационных систем	Практическое задание	Перечень практических заданий (8 заданий)
	Выбирает методики и необходимые средств защиты вычислительных систем		
ПК-4/второй	Воспроизводит способы управления информационной безопасности в информационных и телекоммуникационных системах	Вопросы для устного собеседования	Перечень вопросов для устного собеседования (8 вопросов)
	Систематизирует данные, полученные в результате оценки качества защиты информационных систем	Практическое задание	Перечень практических заданий (8 заданий)

Код компетенции / этап освоения	Показатели оценивания компетенций	Наименование оценочного средства	Представление оценочного средства в фонде
	Предлагает рекомендации по усовершенствованию защиты систем коммуникации на предприятии		
	Распознает проблемы, возникающие в процессе эксплуатации и защиты систем	Практическое задание	Перечень практических заданий (8 заданий)
	Проводит суждение об эффективности программно-аппаратного обеспечения в области информационной безопасности		
ПК-12/Второй	Перечисляет особенности защиты информации в телекоммуникационных и информационных системах	Вопросы для устного собеседования	Перечень вопросов для устного собеседования (16 вопросов)
	Проводит тестирование систем с целью определения уровня защищенности	Практическое задание	Перечень практических заданий (8 заданий)
	Осуществляет проверку защищенности автоматизированных систем и информационно-коммуникационных сетей		

10.1.2. Описание шкал и критериев оценивания сформированности компетенций

Критерии оценивания сформированности компетенций

Баллы	Оценка по традиционной шкале	Критерии оценивания сформированности компетенций
		Устное собеседование
86 - 100	5 (отлично)	Полный, исчерпывающий ответ, явно демонстрирующий глубокое понимание предмета и широкую эрудицию в оцениваемой области. Критический, оригинальный подход к материалу. **Учитываются баллы, накопленные в течение семестра.**
75 – 85	4 (хорошо)	Ответ полный, основанный на проработке всех обязательных источников информации. Подход к материалу ответственный, но стандартный. **Учитываются баллы, накопленные в течение семестра**.
61 – 74		Ответ стандартный, в целом качественный, основан на всех обязательных источниках информации. Присутствуют небольшие пробелы в знаниях или несущественные ошибки. **Учитываются баллы, накопленные в течение семестра.**
51 - 60	3 (удовлетво-рительно)	Ответ воспроизводит в основном только лекционные материалы, без самостоятельной работы с рекомендованной литературой. Демонстрирует понимание предмета в целом, без углубления в детали. Присутствуют существенные ошибки или пробелы в знаниях по некоторым темам. **Учитываются баллы, накопленные в течение семестра**.
40 – 50		Ответ неполный, основанный только на лекционных материалах. При понимании сущности предмета в целом – существенные ошибки или пробелы в знаниях сразу по нескольким темам, незнание (путаница) важных терминов. **Учитываются баллы, накопленные в течение семестра**.
17 – 39	2 (неудовлетво-рительно)	Неспособность ответить на вопрос без помощи экзаменатора. Незнание значительной части принципиально важных элементов дисциплины. Многочисленные грубые ошибки. **Не учитываются баллы, накопленные в течение семестра.**
1 – 16		Непонимание заданного вопроса. Неспособность сформулировать хотя бы отдельные концепции дисциплины. **Не учитываются баллы, накопленные в течение семестра.**
0		Попытка списывания, использования неразрешенных технических устройств или пользования подсказкой другого человека (вне зависимости от успешности такой попытки). **Не учитываются баллы, накопленные в течение семестра.**
40 – 100	Зачтено	Обучающийся своевременно выполнил практические задания; в соответствии с требованиями выполнил и защитил курсовую работу по дисциплине и представил результаты в форме презентации (Microsoft Office Power Point), возможно допуская несущественные ошибки в ответе на вопросы преподавателя.

		Учитываются баллы, накопленные в течение семестра.
0 – 39	Не зачтено	Обучающийся не выполнил (выполнил частично) практические задания; не смог изложить содержание и выводы своей курсовой работы и не представил результаты в форме презентации (Microsoft Office Power Point), допустил существенные ошибки в ответе на вопросы преподавателя. **Не учитываются баллы, накопленные в течение семестра.**

10.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

10.2.1. Перечень вопросов (тестовых заданий), разработанный в соответствии с установленными этапами формирования компетенций

№ п/п	Формулировка вопросов	№ темы
1	Основные принципы построения и реализации компьютерных систем обработки информации.	1
2	Классы программного обеспечения компьютерных систем.	1
3	Роль и принципы реализации компьютерных технологий в современных телекоммуникационных системах.	1
4	Программная поддержку информационных технологий в телекоммуникационных системах.	2
5	Процессы создания, сбора, передачи, обработки, накопления и хранения информации.	2
6	Приведите в виде схемы логическую последовательность действий для спецификации построения системы защиты ИТС, перечислите типы угроз в сетях связи и способы защиты.	2
7	Изложите теоретико-информационные основы криптозащиты сообщений в телекоммуникационных системах.	3
8	Опишите реализацию процедуры аутентификации, авторизации и криптографической защиты в сетях с пакетной коммутацией.	3
9	Какие требования необходимо выполнить для обеспечения заданного уровня информационной безопасности в ИТС.	3
10	Особенности трафика различного типа в мультисервисных сетях, какие протоколы и технологии используются для построения сети связи, которая поддерживает обслуживание «Triple-play services».	4
11	Реализуйте и поясните структурную схему обмена речевыми сообщениями между двумя аналоговыми абонентскими устройствами с учетом использования технологий построения цифровых систем связи.	4
12	Поясните сущность термина «система связи», укажите особенности и принципы реализации различных способов формирования сигналов при передаче информации по каналам связи.	4
13	Охарактеризуйте принципы передачи сигналов управления и взаимодействия в телекоммуникационных системах.	5
14	Поясните сущность термина «канал связи», охарактеризуйте математические модели каналов связи, методы повышения качества передачи информации и снижения уровня мешающих воздействий, применяемые в ИТС.	5
15	Цифровые методы приёмо-передачи речевых сигналов в информационно-телекоммуникационных системах с позиций уменьшения объема трафика.	5
16	Обоснуйте классификацию показателей качества обслуживания QoS, какие способы обеспечения показателей качества используют в сетях с пакетной коммутацией.	6
17	Роль и виды модуляции в системах связи.	6
18	Роль и место теории телетрафика в решении проблемы качества обслуживания QoS в современных мультисервисных сетях связи.	6
19	Существующие методы уплотнения каналов, обоснуйте процесс выбора структуры приемо-передающего тракта и приведите примеры их технической реализации в реальных системах связи.	7
20	Способы повышения надежности, пропускной способности канала, увеличения дальности связи, которые применяют при проектировании и реконструкции сетей связи.	7
21	Основные этапы проектирования цифровых телекоммуникационных систем. Перечислите группы задач, решаемых в процессе планирования мультисервисной сети.	7
22	Требования стандартизации метрологического обеспечения и безопасности жизнедеятельности, предъявляемые при разработке и эксплуатации устройств и систем электросвязи.	7
23	Охарактеризуйте базовые принципы концепции сетей связи следующего поколения Next Generation Networks (NGN), и основные компоненты, приведите модели перехода городских и сельских сетей связи к NGN.	8
24	Передовые методы технического контроля и диагностики, применяемые в процессе настройки и эксплуатации средств связи. Приборы какого типа используются для технического контроля и диагностики телекоммуникационной системы в целом.	8
25	Методы обеспечения безопасности жизнедеятельности и экологичности систем и средств связи, которые используются при разработке требований к телекоммуникационным системам.	8
26	Особенности реализации каждого поколения телекоммуникационных сетей с позиций основных тенденций эволюции сетей и систем связи, приведите перечень услуг, реализуемых каждым	8

	типом сети.	
27	Раскройте определения «Информационно- коммуникационные технологии», «информационно-телекоммуникационные системы» с позиций основных аспектов создания и внедрения ИКТ. Что такое конвергенция в телекоммуникациях, что является результатом конвергенции в области ИКТ?	9
28	Охарактеризуйте передовые методы технического контроля и диагностики в процессе настройки и эксплуатации средств связи.	9
29	Процесс создания, предоставления и продвижения телекоммуникационных услуг на базе технологии ADSL (Asymmetric Digital Subscriber Line).	10
30	Процесс создания, предоставления и продвижения телекоммуникационных услуг на базе технологии HDSL (High Bit-Rate Digital Subscriber Line).	10
31	Процесс создания, предоставления и продвижения телекоммуникационных услуг на базе технологии VDSL (Very High Bit-Rate Digital Subscriber Line).	10
32	Процесс создания, предоставления и продвижения телекоммуникационных услуг на базе технологии PON (Passive Optical Network).	11
33	Процесс создания, предоставления и продвижения телекоммуникационных услуг на базе протокола Ethernet.	11
34	Процесс создания, предоставления и продвижения телекоммуникационных услуг на базе технологии FTTx (Fiber To The…).	11
35	Процесс создания, предоставления и продвижения телекоммуникационных услуг на базе технологии Wi-Fi (Wireless Fidelity).	12
36	Процесс создания, предоставления и продвижения телекоммуникационных услуг на базе технологии WiMAX (Worldwide Interoperability for Microwave Access).	12
37	Информационная безопасность автоматизированной системы – это состояние автоматизированной системы.	12
38	Методы повышения достоверности входных данных.	13
39	Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ).	13
40	Сервисы безопасности.	14
41	Под угрозой удаленного администрирования в компьютерной сети понимается угроза….	14
42	Причины возникновения ошибки в данных.	14
43	Наиболее эффективное средство для защиты от сетевых атак.	14
44	Разделы современной криптографии.	15
45	Основные угрозы конфиденциальности информации.	15
46	Основы нормативно-методического обеспечения создания телекоммуникационных систем.	15
47	Каков жизненный цикл телекоммуникационных систем?	16
48	Какие модели жизненного цикла телекоммуникационных систем наиболее распространены?	16
49	Оценка процессов создания телекоммуникационных систем.	17
50	В чем заключаются основные принципы проектирования телекоммуникационных систем?	17
51	В чем заключаются общая постановка задачи управления процессом проектирования?	17
52	Назовите основные свойства конфиденциальной информации (КИ) как объекта защиты информации.	17
53	Охарактеризуйте жизненный цикл КИ.	17
54	В чем заключается взаимодействие источников КИ с внешней средой?	17
55	Общие принципы обеспечения инфокоммуникационной безопасности.	17
56	Перечислите основные информационные угрозы.	17
57	Какие подходы к декомпозиции процесса проектирования существуют?	17

Вариант тестовых заданий, разработанных в соответствии с установленными этапами формирования компетенций

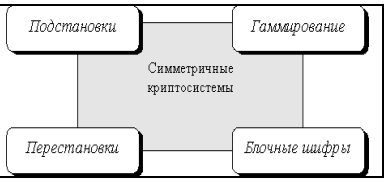
Не предусмотрено

10.2.2. Перечень тем докладов *(рефератов, эссе, пр.)***, разработанных в соответствии с установленными этапами формирования компетенций**

Не предусмотрено

Вариант типовых заданий (задач, кейсов), разработанных в соответствии с установленными этапами формирования компетенций

№ п/п	Условия типовых задач (задач, кейсов)	Ответ
1	К формам защиты информации не относится…	a) аналитическая; b) правовая; c) организационно-техническая; d) страховая.
2	Информация, составляющая государственную тайну не может иметь гриф…	a) «для служебного пользования»; b) «секретно»; c) «совершенно секретно»; d) «особой важности».

3	Все многообразие существующих криптографических методов можно свести к следующим классам преобразований:	

10.3. Методические материалы,
определяющие процедуры оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности), характеризующих этапы формирования компетенций

10.3.1. Условия допуска обучающегося к сдаче зачета и экзамена и порядок ликвидации академической задолженности

К экзамену (зачету) допускается студент, выполнивший в течение семестра все виды учебных заданий по соответствующему предмету (практические работы, курсовая работа). В случае пропуска учебных занятий по уважительной причине (подтвержденной документально) студент обязан отработать пропущенные занятия.

Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся

10.3.2. Форма проведения промежуточной аттестации по дисциплине

устная [X] письменная [X] компьютерное тестирование [ ] иная* [ ]

**В случае указания формы «Иная» требуется дать подробное пояснение*

10.3.3. Особенности проведения экзамена, зачета

Обучающийся тянет билет, в котором теоретический вопрос и практическое задание. После этого готовится в течении как минимум 20 минут с использованием конспекта лекций и других материалов. Обучающийся в устной форме доводит до преподавателя ответ на вопрос, при необходимости прямо во время ответа составляет необходимые схемы или диаграммы.

После ответа на теоретический вопрос обучающийся приступает к решению практического задания, гарантированно на решение задачи времени дается 30 минут, решение формулируется с использованием конспекта лекций и иных материалов, при правильном решении задачи преподаватель задает вопросы по методам или технологиям решения.