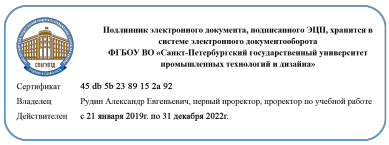
Министерство науки и высшего образования Российской Федерации

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» июня 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.23	Криптографические методы защиты информации
(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	252		
	Аудиторные занятия	102		
	Лекции	51		
	Лабораторные занятия			
	Практические занятия	51		
	Самостоятельная работа	114		
	Промежуточная аттестация	36		
Формы контроля по семестрам (номер семестра)	Экзамен	7		
	Зачет	6		
	Контрольная работа			
	Курсовой проект (работа)	7		
Общая трудоемкость дисциплины (зачетные единицы)		7		

Форма обучения:	Распределение зачетных единиц трудоемкости по семестрам											
	1	2	3	4	5	6	7	8	9	10	11	12
Очная						4	3					
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 [X] Обязательная [X] Дополнительно является факультативом [ ]
Вариативная [ ] По выбору [ ]

1.2. Цель дисциплины

Сформировать компетенции обучающегося в области анализа и использования криптографических методов защиты информации

1.3. Задачи дисциплины

- Раскрытие принципов особенностей различных криптографических методов ЗИ.
- Освоение методики анализа криптостойкости методов ЗИ.
- Развитие навыка использования криптографических методов для решения задач ЗИ

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

Код компетенции	Формулировка компетенции	Этап формирования
ОПК-2	Способность применять соответствующий математический аппарат для решения профессиональных задач	**Второй**
Планируемые результаты обучения Знать: 1) понятия математического аппарата криптографии Уметь: 1) использовать методы дискретной математики при решении практических задач криптографии … Владеть: 1) навыками применения современных методов криптографической защиты информации		
ПК-1	Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	**Второй**
Планируемые результаты обучения Знать: 1) математические методы расчета надежности криптографических систем Уметь: 1) защищать информацию с помощью современных криптографических средств Владеть: 1) навыками применения методов криптографического анализа		
ПК-6	Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Второй
Планируемые результаты обучения Знать: места уязвимости программного обеспечения и программно-аппаратных средств защиты Уметь: определять направления использования аппаратного и программного обеспечения определенного класса для решения служебных задач Владеть:		

Код компетенции	Формулировка компетенции	Этап формирования
навыками выявления и уничтожения компьютерных вирусов		

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

- Математика (ОПК-2)
- Математическая логика (ОПК-2)
- Аппаратные средства вычислительной техники (ПК-1)
- Программно-аппаратные средства защиты информации (ПК-1)

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
Учебный модуль 1. Введение в криптографию			
Тема 1. Возникновение и развитие криптографии и криптоанализа. Общие методы криптографии и криптоанализа	10		
Тема 2. Виды конфиденциальной информации и их защита. Способы и средства криптографической защиты информации (СКЗИ).	10		
Тема 3. Криптографические преобразования. Шифрование и дешифрование информации. Взлом криптоалгоритмов	10		
Тема 4. Виды атак на криптографические протоколы. Причины нарушения безопасности информации при ее обработке СКЗИ	10		
Текущий контроль 1 (опрос)	2		
Учебный модуль 2. Простейшие шифры и их свойства			
Тема 5. Шифр Цезаря. Шифр Вижинера. Шифры простой замены.	8		
Тема 6. Шифры с одноалфавитной и полиалфавитной подстановкой. Перестановочные шифры. Шифр гаммирования. Композиционные шифры.	8		
Тема 7. Основные требования к шифрам. Принцип Керхкоффа.	8		
Тема 8. Теоретико-информационный подход к оценке стойкости шифров. Условная и безусловная стойкость. Теоретическая и практическая стойкость.	8		
Тема 9. Проблема распределения секретных ключей. Модели шифров. Формальное представление шифра. Защищенный канал.	8		
Тема 10. Теорема К. Шеннона. Условная и безусловная стойкость. Совершенные шифры. Шифр с бесконечной ключевой гаммой	8		
Текущий контроль 2 (опрос)	2		
Учебный модуль 3. Шифрсистемы. Электронная цифровая подпись			
Тема 11. Системы шифрования с открытыми ключами. Система открытого распределения ключей Диффи-Хеллмана.	10		
Тема 12. Шифрсистема RSA. Шифрсистема Эль-Гамаля. Шифрсистема Мак-Элиса. Шифрсистемы на основе "проблемы рюкзака"	10		
Тема 13. Электронная цифровая подпись. Общие положения. Цифровые подписи на основе шифрсистем с открытыми ключами. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля. Одноразовые цифровые подписи	16		
Тема 14. Инфраструктура электронных цифровых подписей. Сертификаты электронных цифровых подписей. Центры сертификации электронных цифровых подписей	10		
Текущий контроль 3 (опрос)	2		
Промежуточная аттестация по дисциплине (зачет)	4		
Учебный модуль 4. Модели шифров и открытых текстов			
Тема 15. Алгебраическая модель шифра замены. Алгебраическая модель шифра перестановки. Алгебраическая модель шифра RSA.	4		

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
Вероятностные модели шифров замены и перестановки.			
Тема 16. Модели открытых текстов. Алгебраические модели открытого текста. Вероятностные модели открытого текста.	4		
Тема 17. Критерии распознавания открытого текста. Энтропия и избыточность языка. Расстояние единственности.	4		
Текущий контроль 4 (опрос)	2		
Учебный модуль 5. Принципы построения криптографических алгоритмов			
Тема 18. «Перемешивающие» и «рассеивающие» преобразования. Криптографические параметры «перемешивающих» и «рассеивающих» блоков. Композиции шифров. Комбинирование алгоритмов блочного шифрования	4		
Тема 19. Синтез шифров DES алгоритма. Синтез шифров алгоритма ГОСТа 28147-89.	4		
Тема 20. Режимы использования блочных шифров. Принципы построения криптографических алгоритмов поточного шифрования	4		
Тема 21. Управляющий и шифрующий блоки. Требования, предъявляемые к криптографическим параметрам управляющих и шифрующих блоков. Примеры синтеза поточных шифрсистем	4		
Текущий контроль 5 (опрос)	2		
Учебный модуль 6. Криптографические методы в современных средствах защиты информации в компьютерных системах			
Тема 22. Организация защищенного окружения при использовании криптосистем. Криптографические механизмы в средствах защиты информации в компьютерных системах	4		
Тема 23. Принцип глобального шифрования в масштабе реального времени. Дисковое шифрование с помощью скоростных программных шифров.	2		
Тема 24. Файловое шифрование и его особенности. Криптографические загрузчики и использование «минишифров». Скоростные программные хэш-функции. Контроль целостности эталонного состояния рабочей среды. Защита информации на технологическом уровне	2		
Текущий контроль 6 (опрос)	2		
Курсовая работа (проект)	**30**		
Промежуточная аттестация по дисциплине (экзамен)	**36**		
ВСЕГО:	**252**		

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	6	2				
2	6	2				
3	6	2				
4	6	2				
5	6	4				
6	6	4				
7	6	4				
8	6	2				
9	6	2				
10	6	2				
11	6	2				
12	6	2				
13	6	2				
14	6	2				
15	7	2				
16	7	2				

Номера изучаемых тем	Очное обучение		Очно-заочное обучение		Заочное обучение	
	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
17	7	2				
18	7	2				
19	7	2				
20	7	2				
21	7	2				
22	7	1				
23	7	1				
24	7	1				
	ВСЕГО:	51				

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	Общие методы криптографии и криптоанализа (практикум)	6	2				
2	Способы и средства криптографической защиты информации (СКЗИ) (практикум)	6	2				
3	Криптографические преобразования. Шифрование и дешифрование информации (практикум)	6	2				
5	Шифр Цезаря. Шифр Вижинера. Шифры простой замены. (практикум)	6	4				
6	Шифры с одноалфавитной и полиалфавитной подстановкой. Перестановочные шифры. Шифр гаммирования. Композиционные шифры. (практикум)	6	4				
8	Теоретико-информационный подход к оценке стойкости шифров. Условная и безусловная стойкость. Теоретическая и практическая стойкость (практикум)	6	4				
9	Проблема распределения секретных ключей. Модели шифров. Формальное представление шифра. Защищенный канал (практикум-семинар)	6	2				
10	Условная и безусловная стойкость. Совершенные шифры. Шифр с бесконечной ключевой гаммой (практикум-семинар)	6	4				
11	Системы шифрования с открытыми ключами. Система открытого распределения ключей	6	4				

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)
	Диффи-Хеллмана (практикум-семинар)						
12	Шифрсистема RSA. Шифрсистема Эль-Гамаля. Шифрсистема Мак-Элиса. Шифрсистемы на основе "проблемы рюкзака" (практикум-семинар)	6	4				
13	Электронная цифровая подпись. Общие положения. Цифровые подписи на основе шифрсистем с открытыми ключами. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля. Одноразовые цифровые подписи (практикум-семинар)	6	2				
15	Алгебраическая модель шифра замены. Алгебраическая модель шифра перестановки. Алгебраическая модель шифра RSA. Вероятностные модели шифров замены и перестановки (практикум)	7	2				
16	Модели открытых текстов. Алгебраические модели открытого текста. Вероятностные модели открытого текста (практикум)	7	2				
18	Криптографические параметры «перемешивающих» и «рассеивающих» блоков. Композиции шифров. Комбинирование алгоритмов блочного шифрования (практикум)	7	2				
19	Синтез шифров DES алгоритма. Синтез шифров алгоритма ГОСТа 28147-89 (практикум)	7	2				
20	Режимы использования блочных шифров. Принципы построения криптографических алгоритмов поточного шифрования (практикум)	7	2				
21	Управляющий и шифрующий блоки. Требования, предъявляемые к криптографическим параметрам управляющих и шифрующих блоков (семинар)	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)
22	Организация защищенного окружения при использовании криптосистем. Криптографические механизмы в средствах защиты информации в компьютерных системах (семинар)	7	3				
23	Принцип глобального шифрования в масштабе реального времени. Дисковое шифрование с помощью скоростных программных шифров (семинар)	7	1				
24	Файловое шифрование и его особенности. Криптографические загрузчики и использование «минишифров». Скоростные программные хэш-функции. Контроль целостности эталонного состояния рабочей среды. Защита информации на технологическом уровне (семинар)	7	1				
		ВСЕГО:	51				

3.3. Лабораторные занятия

Не предусмотрены

4. КУРСОВОЕ ПРОЕКТИРОВАНИЕ

4.1. Цели и задачи курсовой работы (проекта)

Целью курсовой работы является исследование структуры, свойств и криптографической стойкости потокового шифра A5/1.

Задачи курсовой работы:

- Реализовать алгоритм A5/1, используемый в современных сотовых сетях второго поколения.
- Наглядно описать внутреннюю структуру шифра.
- Создать инструменты для изучения свойств баланса, серий, окна и автокорреляционной функции выходной гаммы потокового шифра.
- Создать инструменты для криптографического анализа потокового шифра, реализующие оценку ЭЛС по алгоритму Берликемпа-Месси, а также корреляционную атаку и атаку со вставкой

4.2. Тематика курсовой работы (проекта)

Исследование структуры, свойств и криптографической стойкости потокового шифра (по заданию преподавателя)

4.3. Требования к выполнению и представлению результатов курсовой работы

Работа выполняется индивидуально и самостоятельно, с использованием специального программного обеспечения.

Результаты представляются в виде пояснительной записки, объемом не менее 20 страниц содержащего следующие обязательные элементы:

- Введение
- Основная часть работы
- Выводы и заключение

- Список используемой литературы

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
1-3	Опрос	6	3				
4-6	Опрос	7	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	6 7	36 4				
Подготовка к практическим занятиям	6 7	36 4				
Выполнение курсовой работы	7	30				
Подготовка к зачету	6	4				
Подготовка к экзамену	7	36				
	ВСЕГО:	150				

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	10		
Практические и семинарские занятия	решения проблемных ситуаций (case-study), командное соревнование малых групп	10		
	ВСЕГО:	20		

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) 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	• 5 баллов за каждую работу, всего 11 практических работ, максимум 55 баллов • Качество защиты (полнота ответов на вопросы, владение специальной терминологией, затраченное на ответы время) – максимум **45**

			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) 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 курсовой работы	40	• Представление в срок и качество оформления – максимум **15** баллов; • Содержание (соответствие заданию, наличие всех требуемых элементов, наличие и значимость ошибок) – максимум **50** баллов; • Качество защиты (полнота ответов на вопросы, владение специальной терминологией, затраченное на ответы время) – максимум **35** баллов.
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. Гатченко Н.А. Криптографическая защита информации [Электронный ресурс]/ Н.А. Гатченко, А.С. Исаев, А.Д. Яковлев— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2012.— 142 с.— Режим доступа: http://www.iprbookshop.ru/68658.html.— ЭБС «IPRbooks»

2. Басалова Г.В. Основы криптографии [Электронный ресурс]/ Г.В. Басалова— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 282 с.— Режим доступа: http://www.iprbookshop.ru/52158.html.— ЭБС «IPRbooks»

3. Ожиганов А.А. Криптография [Электронный ресурс]: учебное пособие/ А.А. Ожиганов— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2016.— 142 с.— Режим доступа: http://www.iprbookshop.ru/67231.html.— ЭБС «IPRbooks»

б) дополнительная учебная литература

1. Кукина Е.Г. Введение в криптографию [Электронный ресурс]: сборник задач и упражнений/ Е.Г. Кукина, В.А. Романьков— Электрон. текстовые данные.— Омск: Омский государственный университет им. Ф.М. Достоевского, 2013.— 91 с.— Режим доступа: http://www.iprbookshop.ru/24876.html.— ЭБС «IPRbooks»
2. Практикум по выполнению лабораторных работ по дисциплине Криптографические методы защиты информации [Электронный ресурс]/ — Электрон. текстовые данные.— М.: Московский технический университет связи и информатики, 2015.— 67 с.— Режим доступа: http://www.iprbookshop.ru/61738.html.— ЭБС «IPRbooks»
3. Калмыков И.А. Криптографические методы защиты информации [Электронный ресурс]: лабораторный практикум/ И.А. Калмыков, Д.О. Науменко, Т.А. Гиш— Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2015.— 109 с.— Режим доступа: http://www.iprbookshop.ru/63099.html.— ЭБС «IPRbooks»
4. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс]/ А.А. Петров— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 446 с.— Режим доступа: http://www.iprbookshop.ru/63800.html.— ЭБС «IPRbooks»

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

1. Криптографические методы защиты информации [Электронный ресурс]: методические указания / Сост. Бусыгин К. Н. — СПб.: СПГУТД, 2014.— 44 с.— Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=1722, по паролю.
2. Математические основы криптологии [Электронный ресурс]: методические указания / Сост. Бусыгин К. Н. — СПб.: СПГУТД, 2014.— 44 с.— Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=1721, 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 компьютер

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

Виды учебных занятий и самостоятельная работа обучающихся	Организация деятельности обучающегося
	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	Не предусмотрено
Самостоятельная работа	Следует предварительно изучить методические указания по выполнению самостоятельной работы, курсовой работы (проекта), контрольной работы (можно указать реквизиты изданий и электронный ресурс, где они находятся). 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
ОПК-2/второй	воспроизводит основные методы применения математических инструментов при решении профессиональных задач	Вопросы для устного собеседования	Перечень вопросов для устного собеседования (67 вопросов)
	Демонстрирует применение математического аппарата для решения задач криптографии	Практическое задание	Перечень практических заданий (8 заданий)
	выполняет решение поставленных задач с использованием современных методов криптографической защиты информации		
ПК-1/второй	называет и интерпретирует методы решения конкретных алгебраических, теоретико-числовых и алгоритмических задач криптографического анализа и синтеза криптографических систем и криптографических протоколов	Вопросы для устного собеседования	Перечень вопросов для устного собеседования (67 вопросов)
	анализирует и осуществляет выбор современных криптографических средств для защиты информации	Практическое задание	Перечень практических заданий (8 заданий)
	применяет на практике общую методологию криптографического анализа и построения оценок криптографической стойкости криптографических систем		
ПК-6/второй	Формулирует направления, методы и средства защиты информации от утечки, хищения, искажения, подделки, несанкционированного уничтожения, копирования и блокирования	Вопросы для устного собеседования	Вопросы (5)
	выбирает, строит и анализирует показатели защищенности программно-аппаратных средств защиты информации	Практическое задание	Задания (10)
	настраивает средства обнаружения вторжений и антивирусные системы		

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	Курсоваяработа
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.***	*Критическое и разностороннее рассмотрение вопросов, свидетельствующее о значительной самостоятельной работе с источниками. Качество исполнения всех элементов задания полностью соответствует всем требованиям.* ***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****.*	*Все заданные вопросы освещены в необходимой полноте и с требуемым качеством. Ошибки отсутствуют. Самостоятельная работа проведена в достаточном объеме, но ограничивается только основными рекомендованными источниками информации.* ***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.***	*Работа выполнена в соответствии с заданием. Имеются отдельные несущественные ошибки или отступления от правил оформления работы.* ***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****.*	*Задание выполнено полностью, но в работе есть отдельные существенные ошибки, либо качество представления работы низкое, либо работа представлена с опозданием.* ***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****.*	*Задание выполнено полностью, но с многочисленными существенными ошибками. При этом нарушены правила оформления или сроки представления работы.* ***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.***	*Отсутствие одного или нескольких обязательных элементов задания, либо многочисленные грубые ошибки в работе, либо грубое нарушение правил оформления или сроков представления работы.* ***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.***	*Содержание работы полностью не соответствует заданию.* ***Не учитываются баллы, накопленные в течение семестра.***
0		*Попытка списывания, использования*	*Представление чужой работы,*

		неразрешенных технических устройств или пользования подсказкой другого человека (вне зависимости от успешности такой попытки). ***Не учитываются баллы, накопленные в течение семестра.***	*плагиат, либо отказ от представления работы.* ***Не учитываются баллы, накопленные в течение семестра.***
40 – 100	Зачтено	***Например****, обучающийся своевременно выполнил лабораторные работы и представил результаты в форме презентации (Microsoft Office Power Point); в соответствии с требованиями выполнил и защитил курсовую работу по дисциплине, возможно допуская несущественные ошибки в ответе на вопросы преподавателя.* ***Учитываются баллы, накопленные в течение семестра.***	
0 – 39	Не зачтено	***Например****, обучающийся не выполнил (выполнил частично) лабораторные работы, не представил результаты в форме презентации (Microsoft Office Power Point); не смог изложить содержание и выводы своей курсовой работы, 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	Возникновение и развитие криптографии и криптоанализа.	1
2	Общие методы криптографии и криптоанализа	1
3	Виды конфиденциальной информации и их защита.	2
4	Способы и средства криптографической защиты информации (СКЗИ).	2
5	Криптографические преобразования	3
6	Шифрование и дешифрование информации.	3
7	Взлом криптоалгоритмов	3
8	Виды атак на криптографические протоколы	4
9	Причины нарушения безопасности информации при ее обработке СКЗИ	4
10	Шифр Цезаря	5
11	Шифр Вижинера	5
12	Шифры простой замены	5
13	Шифры с одноалфавитной и полиалфавитной подстановкой	6
14	Перестановочные шифры	6
15	Шифр гаммирования	6
16	Композиционные шифры.	6
17	Основные требования к шифрам	7
18	Принцип Керхкоффа	7
19	Теоретико-информационный подход к оценке стойкости шифров	8
20	Условная и безусловная стойкость	8
21	Теоретическая и практическая стойкость.	8
22	Проблема распределения секретных ключей	9
23	Модели шифров. Формальное представление шифра.	9
24	Теорема К. Шеннона	10
25	Условная и безусловная стойкость	10
26	Совершенные шифры	10
27	Шифр с бесконечной ключевой гаммой	10
28	Системы шифрования с открытыми ключами	11
29	Система открытого распределения ключей Диффи-Хеллмана.	11
30	Шифрсистема RSA	12
31	Шифрсистема Эль-Гамаля	12
32	Шифрсистема Мак-Элиса	12
33	Шифрсистемы на основе «проблемы рюкзака»	12
34	Электронная цифровая подпись. Общие положения	13
35	Цифровые подписи на основе шифрсистем с открытыми ключами.	13
36	Цифровая подпись Фиата-Шамира.	13
37	Цифровая подпись Эль-Гамаля	13
38	Одноразовые цифровые подписи	13
39	Инфраструктура электронных цифровых подписей.	14
40	Сертификаты электронных цифровых подписей	14
41	Алгебраическая модель шифра замены	15
42	Алгебраическая модель шифра перестановки	15
43	Алгебраическая модель шифра RSA.	15
44	Вероятностные модели шифров замены и перестановки.	15

45	Модели открытых текстов	16
46	Алгебраические модели открытого текста	16
47	Вероятностные модели открытого текста.	16
48	Критерии распознавания открытого текста	17
49	Энтропия и избыточность языка. Расстояние единственности.	17
50	Криптографические параметры «перемешивающих» и «рассеивающих» блоков.	18
51	Композиции шифров	18
52	Комбинирование алгоритмов блочного шифрования	18
53	Синтез шифров DES алгоритма	19
54	Синтез шифров алгоритма ГОСТа 28147-89.	19
55	Режимы использования блочных шифров	20
56	Принципы построения криптографических алгоритмов поточного шифрования	20
57	Управляющий и шифрующий блоки. Требования, предъявляемые к криптографическим параметрам управляющих и шифрующих блоков	21
58	Примеры синтеза поточных шифрсистем	21
59	Организация защищенного окружения при использовании криптосистем	22
60	Криптографические механизмы в средствах защиты информации в компьютерных системах	22
61	Принцип глобального шифрования в масштабе реального времени	23
62	Дисковое шифрование с помощью скоростных программных шифров	23
63	Файловое шифрование и его особенности	24
64	Криптографические загрузчики и использование «минишифров	24
65	Скоростные программные хэш-функции.	24
66	Контроль целостности эталонного состояния рабочей среды.	24
67	Защита информации на технологическом уровне	24

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	Вычислить НОД(a,b) при помощи алгоритма Евклида с делением с остатком и бинарного алгоритма Евклида. Сравнить количество итераций a = 715, b = 195	13
2	Зашифруйте слово STUDENT с помощью модулярного шифра $f : Z_{26} \to Z_{26}$; $f(x) = 3x + 1$.	06 09 12 13 16 17 9 ~ FILMPQI
3	Вычислите закрытый ключ÷ d криптосистемы RSA с параметром p = 53, q = 79, e = 97. Зашифруйте с помощью полученной системы сообщение ” 123 ”. Выполните проверку	Зашифрованное сообщение 2288.

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 экзамена, зачета и защите курсовой работы 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* [ ]

10.3.3. Особенности проведения экзамена, зачета защиты курсовой работы

Студент получает вопрос и практическое задание для выполнения и готовится в течение 40 минут. Возможно использование лекционного материала и калькулятора. В процессе ответа также требуется теоретически обосновать выполненные практические задания.