Федеральное государственное бюджетное образовательное учреждение высшего образования

САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АРХИТЕКТУРНО-СТРОИТЕЛЬНЫЙ УНИВЕРСИТЕТ

Кафедра Информационных систем и технологий

УТВЕРЖДАЮ
Начальник учебно-методического управления

Михайлова Анна Олеговна
Подписано цифровой подписью: Михайлова Анна Олеговна

«29» июня 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Методы и средства защиты информации

направление подготовки/специальность 01.04.02 Прикладная математика и информатика

направленность (профиль)/специализация образовательной программы Информационные технологии и математическое моделирование в строительстве

Форма обучения очная

Санкт-Петербург, 2023

1. Цели и задачи освоения дисциплины (модуля)

Целями освоения дисциплины (модуля) является изложение принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Задачи дисциплины (модуля):

− дать студентам основы системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;

− дать основы принципов синтеза и анализа шифров;

− дать основы математических методов, используемых в криптоанализе.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов освоения ОПОП
ПК-1 Способен управлять процессом разработки программного обеспечения	ПК-1.1 Осуществляет декомпозицию технического задания на разработку программного обеспечения на отдельные задачи	**знает** Алгоритмы защиты информации при разработке программного обеспечения Паттерны разработки программного обеспечения **умеет** Писать и отлаживать код, тестировать работоспособность программы на предмет информационной безопасности Строить блок-схемы работы программного обеспечения Вырабатывать варианты реализации требований к программному обеспечению **владеет** Навыками работы с автоматизированными системами подготовки и проектирования Приемами разработки компонентов программных комплексов

3. Указание места дисциплины (модуля) в структуре образовательной программы

Данная дисциплина (модуль) включена в Блок «Дисциплины, модули» Б1.В.ДВ.01.02 основной профессиональной образовательной программы 01.04.02 Прикладная математика и информатика и относится к части, формируемой участниками образовательных отношений учебного плана.

№ п/п	Предшествующие дисциплины	Код и наименование индикатора достижения компетенции
1	Методы обработки данных и анализ временных рядов	ОПК-1.1, ОПК-1.3

знать:

- основные понятия информатики;
- основы структуры данных;

уметь:

- работать на персональном компьютере;
- пользоваться операционной системой;
- использовать данные получаемые в интернете.

владеть:

- навыками работы с учебной литературой;
- основными приёмами работы на компьютере с прикладным программным обеспечением

№ п/п	Последующие дисциплины	Код и наименование индикатора достижения компетенции
1	Выполнение и защита выпускной квалификационной работы	УК-1.1, УК-1.2, УК-1.3, УК-1.4, УК-1.5, УК-1.6, УК-2.1, УК-2.2, УК-2.3, УК-2.4, УК-2.5, УК-3.1, УК-3.2, УК-3.3, УК-3.4, УК-4.1, УК-4.2, УК-4.3, УК-4.4, УК-5.1, УК-5.2, УК-5.3, УК-6.1, УК-6.2, УК-6.3, ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-4.1, ОПК-4.2, ОПК-4.3, ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК(Ц)-1.1, ПК (Ц)-1.2, ПК(Ц)-1.3, ПК(Ц)-1.4, ПК (Ц)-1.5, ПК(Ц)-1.6
2	Выполнение и защита выпускной квалификационной работы	УК-1.1, УК-1.2, УК-1.3, УК-1.4, УК-1.5, УК-1.6, УК-2.1, УК-2.2, УК-2.3, УК-2.4, УК-2.5, УК-3.1, УК-3.2, УК-3.3, УК-3.4, УК-4.1, УК-4.2, УК-4.3, УК-4.4, УК-5.1, УК-5.2, УК-5.3, УК-6.1, УК-6.2, УК-6.3, ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-4.1, ОПК-4.2, ОПК-4.3, ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК(Ц)-1.1, ПК (Ц)-1.2, ПК(Ц)-1.3, ПК(Ц)-1.4, ПК (Ц)-1.5, ПК(Ц)-1.6
3	Выполнение и защита выпускной квалификационной работы	УК-1.1, УК-1.2, УК-1.3, УК-1.4, УК-1.5, УК-1.6, УК-2.1, УК-2.2, УК-2.3, УК-2.4, УК-2.5, УК-3.1, УК-3.2, УК-3.3, УК-3.4, УК-4.1, УК-4.2, УК-4.3, УК-4.4, УК-5.1, УК-5.2, УК-5.3, УК-6.1, УК-6.2, УК-6.3, ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-4.1, ОПК-4.2, ОПК-4.3, ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК(Ц)-1.1, ПК (Ц)-1.2, ПК(Ц)-1.3, ПК(Ц)-1.4, ПК (Ц)-1.5, ПК(Ц)-1.6

4	Выполнение и защита выпускной квалификационной работы	УК-1.1, УК-1.2, УК-1.3, УК-1.4, УК-1.5, УК-1.6, УК-2.1, УК-2.2, УК-2.3, УК-2.4, УК-2.5, УК-3.1, УК-3.2, УК-3.3, УК-3.4, УК-4.1, УК-4.2, УК-4.3, УК-4.4, УК-5.1, УК-5.2, УК-5.3, УК-6.1, УК-6.2, УК-6.3, ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-4.1, ОПК-4.2, ОПК-4.3, ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК(Ц)-1.1, ПК(Ц)-1.2, ПК(Ц)-1.3, ПК(Ц)-1.4, ПК(Ц)-1.5, ПК(Ц)-1.6

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

Вид учебной работы	Всего часов	Из них часы на практическую подготовку	Семестр
			3
Контактная работа	32		32
Практические занятия (Пр)	32	0	32
Иная контактная работа, в том числе:			
консультации по курсовой работе (проекту), контрольным работам (РГР)			
контактная работа на аттестацию (сдача зачета, зачета с оценкой; защита курсовой работы (проекта); сдача контрольных работ (РГР))			
контактная работа на аттестацию в сессию (консультация перед экзаменом и сдача			
Часы на контроль	4		4
Самостоятельная работа (СР)	72		72
Общая трудоемкость дисциплины (модуля)			
часы:	108		108
зачетные единицы:	3		3

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

5.1. Тематический план дисциплины (модуля)

№	Разделы дисциплины	Семестр	Контактная работа (по учебным занятиям), час.						СР	Всего, час.	Код индикатора достижения компетенции
			лекции		ПЗ		ЛР				
			всего	из них на практическую подготовку	всего	из них на практическую подготовку	всего	из них на практическую подготовку			
1.	1 раздел. Классические шифры криптографии										
1.1.	Основные понятия и определения криптографии	3			2				6	8	ПК-1.1

1.2.	Шифры замены и перестановки	3			2				6	8	ПК-1.1
1.3.	Классические шифры перестановки	3			2				6	8	ПК-1.1
1.4.	Блочные и потоковые шифры	3			2				6	8	ПК-1.1
1.5.	Шифры простой замены	3			2				6	8	ПК-1.1
1.6.	Шифры сложной замены	3			2				6	8	ПК-1.1
1.7.	Шифры гаммирования и колонной замены	3			4				6	10	ПК-1.1
2.	2 раздел. Современные системы симметричной криптографии										
2.1.	Основы теории Шеннона и её развитие.	3			2				6	8	ПК-1.1
2.2.	Композиции шифров. Алгоритмы шифрования DES.	3			4				6	10	ПК-1.1
2.3.	Режимы работы блочных шифров.	3			2				6	8	ПК-1.1
2.4.	Вычислительная стойкость криптоалгоритмов. Атаки на алгоритмы шифрования. Методы криптоанализа блочных шифров.	3			4				6	10	ПК-1.1
2.5.	Требования, предъявляемые к современным блочным алгоритмам шифрования. Шифр AES.	3			4				6	10	ПК-1.1
3.	3 раздел. Контроль										
3.1.	Зачёт	3								4	ПК-1.1

5.1. Практические занятия

№ разд	Наименование раздела и темы практических занятий	Наименование и содержание практических занятий
1	Основные понятия и определения криптографии	Основные понятия и определения криптографии Основные понятия и определения криптографии
2	Шифры замены и перестановки	Шифры замены и перестановки Классификация классических шифров по типу преобразования
3	Классические шифры перестановки	Классические шифры перестановки Изучение классических шифров перестановки
4	Блочные и потоковые шифры	Блочные и потоковые шифры Классификация шифров по размеру преобразуемой информации
5	Шифры простой замены	Шифры простой замены Изучение шифров простой замены
6	Шифры сложной замены	Шифры сложной замены Изучение шифров сложной замены
7	Шифры гаммирования и колонной замены	Шифры гаммирования и колонной замены Изучение шифров гаммирования и колонной замены
8	Основы теории	Основы теории Шеннона и её развитие.

	Шеннона и её развитие.	Основы теории Шеннона и её развитие
9	Композиции шифров. Алгоритмы шифрования DES.	Композиции шифров. Алгоритмы шифрования DES. Алгоритмы шифрования DES
10	Режимы работы блочных шифров.	Режимы работы блочных шифров. Режимы работы блочных шифров
11	Вычислительная стойкость криптоалгоритмов. Атаки на алгоритмы шифрования. Методы криптоанализа блочных шифров.	Вычислительная стойкость криптоалгоритмов. Атаки на алгоритмы шифрования. Методы криптоанализа блочных шифров. Методы криптоанализа блочных шифров
12	Требования, предъявляемые к современным блочным алгоритмам шифрования. Шифр AES.	Требования, предъявляемые к современным блочным алгоритмам шифрования. Шифр AES. Изучения шифра AES

5.2. Самостоятельная работа обучающихся

№ разд	Наименование раздела дисциплины и темы	Содержание самостоятельной работы
1	Основные понятия и определения криптографии	Основные понятия и определения криптографии Подготовка к практическим занятиям. Подготовка к промежуточной аттестации
2	Шифры замены и перестановки	Шифры замены и перестановки Подготовка к практическим занятиям. Подготовка к промежуточной аттестации
3	Классические шифры перестановки	Классические шифры перестановки Подготовка к практическим занятиям. Подготовка к контрольной работе на тему «Криптоанализ шифров табличной перестановки». Подготовка к промежуточной аттестации
4	Блочные и потоковые шифры	Блочные и потоковые шифры Подготовка к практическим занятиям.
5	Шифры простой замены	Шифры простой замены Подготовка к практическим занятиям. Подготовка к контрольной работе на тему «Шифры простой замены». Подготовка к промежуточной аттестации.
6	Шифры сложной замены	Шифры сложной замены Подготовка к практическим занятиям. Подготовка к контрольной работе на тему «Шифры сложной замены». Подготовка к промежуточной аттестации.
7	Шифры гаммирования и колонной замены	Шифры гаммирования и колонной замены Подготовка к практическим занятиям. Подготовка к тесту по 1-му разделу «Классические шифры криптографии». Подготовка к промежуточной аттестации.
8	Основы теории Шеннона и её развитие.	Основы теории Шеннона и её развитие. Подготовка к практическим занятиям. Подготовка к промежуточной аттестации
9	Композиции шифров.	Композиции шифров. Алгоритмы шифрования DES.

	Алгоритмы шифрования DES.	Подготовка к практическим занятиям. Подготовка к промежуточной аттестации
10	Режимы работы блочных шифров.	Режимы работы блочных шифров. Подготовка к практическим занятиям. Подготовка к промежуточной аттестации
11	Вычислительная стойкость криптоалгоритмов. Атаки на алгоритмы шифрования. Методы криптоанализа блочных шифров.	Вычислительная стойкость криптоалгоритмов. Атаки на алгоритмы шифрования. Методы криптоанализа блочных шифров. Подготовка к практическим занятиям. Подготовка к промежуточной аттестации
12	Требования, предъявляемые к современным блочным алгоритмам шифрования. Шифр AES.	Требования, предъявляемые к современным блочным алгоритмам шифрования. Шифр AES. Подготовка к практическим занятиям. Подготовка к промежуточной аттестации

6. Методические материалы для самостоятельной работы обучающихся по дисциплине (модулю)

Программой дисциплины предусмотрено проведение практических занятий, предполагающих закрепление изученного материала и формирование у обучающихся необходимых знаний, умений и навыков. Кроме того, важнейшим этапом изучения дисциплины является самостоятельная работа обучающихся с использованием всех средств и возможностей современных образовательных технологий.

В объем самостоятельной работы по дисциплине включается следующее:

− подготовка к практическим занятиям;

− подготовка к текущему контролю успеваемости студентов;

− подготовка к зачету.

Залогом успешного освоения дисциплины является обязательное посещение практических занятий, так как пропуск одного (тем более, нескольких) занятий может осложнить освоение разделов курса.

Приступая к изучению дисциплины, необходимо в первую очередь ознакомиться с содержанием РПД, а также методическими указаниями по организации самостоятельной работы.

При подготовке к практическим занятиям и в рамках самостоятельной работы по изучению дисциплины обучающимся необходимо:

− выполнить практические задания в рамках изучаемой темы;

− ответить на контрольные вопросы по теме, используя материалы ФОС;

− подготовиться к проверочной работе, предусмотренной в контрольных точках;

− подготовиться к промежуточной аттестации.

Итогом изучения дисциплины является зачет. Зачет проводится по расписанию. Форма проведения занятия может быть устная, письменная и в электронном виде. Студенты, не прошедшие аттестацию, должны ликвидировать задолженность в установленном порядке.

7. Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине (модулю)

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

№ п/п	Контролируемые разделы дисциплины (модуля)	Код и наименование индикатора контролируемой компетенции	Вид оценочного средства
1	Основные понятия и определения криптографии	ПК-1.1	Тест по 1-му разделу «Классические шифры криптографии». Теоретические вопросы и практические задания для проведения промежуточной аттестации
2	Шифры замены и перестановки	ПК-1.1	Тест по 1-му разделу «Классические шифры криптографии». Теоретические вопросы и практические задания для проведения промежуточной аттестации
3	Классические шифры перестановки	ПК-1.1	Тест по 1-му разделу «Классические шифры

			криптографии». Теоретические вопросы и практические задания для проведения промежуточной аттестации
4	Блочные и потоковые шифры	ПК-1.1	Тест по 1-му разделу «Классические шифры криптографии». Теоретические вопросы и практические задания для проведения промежуточной аттестации
5	Шифры простой замены	ПК-1.1	Тест по 1-му разделу «Классические шифры криптографии». Теоретические вопросы и практические задания для проведения промежуточной аттестации
6	Шифры сложной замены	ПК-1.1	Тест по 1-му разделу «Классические шифры криптографии». Теоретические вопросы и практические задания для проведения промежуточной аттестации
7	Шифры гаммирования и колонной замены	ПК-1.1	Тест по 1-му разделу «Классические шифры криптографии». Теоретические вопросы и практические задания для проведения промежуточной аттестации
8	Основы теории Шеннона и её развитие.	ПК-1.1	Тест по 2-му разделу «Современные системы симметричной криптографии». Теоретические вопросы и практические задания для проведения

			промежуточной аттестации
9	Композиции шифров. Алгоритмы шифрования DES.	ПК-1.1	Тест по 2-му разделу «Современные системы симметричной криптографии». Теоретические вопросы и практические задания для проведения промежуточной аттестации
10	Режимы работы блочных шифров.	ПК-1.1	Тест по 2-му разделу «Современные системы симметричной криптографии». Теоретические вопросы и практические задания для проведения промежуточной аттестации
11	Вычислительная стойкость криптоалгоритмов. Атаки на алгоритмы шифрования. Методы криптоанализа блочных шифров.	ПК-1.1	Тест по 2-му разделу «Современные системы симметричной криптографии». Теоретические вопросы и практические задания для проведения промежуточной аттестации
12	Требования, предъявляемые к современным блочным алгоритмам шифрования. Шифр AES.	ПК-1.1	Тест по 2-му разделу «Современные системы симметричной криптографии». Теоретические вопросы и практические задания для проведения промежуточной аттестации
13	Зачёт	ПК-1.1	

7.2. Типовые контрольные задания или иные материалы текущего контроля успеваемости, необходимые для оценки знаний, умений и навыков и (или) опыта профессиональной деятельности, характеризующих этапы формирования компетенций в процессе освоения дисциплины

для проверки сформированности индикатора достижения компетенции ПК-1.1

Типовые контрольные задания и иные материалы текущего контроля успеваемости размещены по адресу ЭИОС Moodle (https://moodle.spbgasu.ru/ Кафедры / Информационные технологии / Курсы для магистров ПМИ и ИСТ / Методы и средства защиты информации)

7.3. Система оценивания результатов обучения по дисциплине (модулю) при проведении текущего контроля успеваемости

Оценка «отлично» (зачтено)	знания: - систематизированные, глубокие и полные знания по всем разделам дисциплины, а также по основным вопросам, выходящим за пределы учебной программы; - точное использование научной терминологии, систематически грамотное и логически правильное изложение ответа на вопросы; - полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой по дисциплине (модулю) умения: - умеет ориентироваться в теориях, концепциях и направлениях дисциплины и давать им критическую оценку, используя научные достижения других дисциплин навыки: - высокий уровень сформированности заявленных в рабочей программе компетенций; - владеет навыками самостоятельно и творчески решать сложные проблемы и нестандартные ситуации; - применяет теоретические знания для выбора методики выполнения заданий; - грамотно обосновывает ход решения задач; - безупречно владеет инструментарием учебной дисциплины, умение его эффективно использовать в постановке научных и практических задач; - творческая самостоятельная работа на практических/семинарских/лабораторных занятиях, активно участвует в групповых обсуждениях, высокий уровень культуры исполнения заданий
Оценка «хорошо» (зачтено)	знания: - достаточно полные и систематизированные знания по дисциплине; - усвоение основной и дополнительной литературы, рекомендованной рабочей программой по дисциплине (модулю) умения: - умеет ориентироваться в основных теориях, концепциях и направлениях дисциплины и давать им критическую оценку; - использует научную терминологию, лингвистически и логически правильно излагает ответы на вопросы, умеет делать обоснованные выводы; - владеет инструментарием по дисциплине, умение его использовать в постановке и решении научных и профессиональных задач навыки: - самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий; - средний уровень сформированности заявленных в рабочей программе компетенций; - без затруднений выбирает стандартную методику выполнения заданий; - обосновывает ход решения задач без затруднений

Оценка «удовлетворительно» (зачтено)	знания: - достаточный минимальный объем знаний по дисциплине; - усвоение основной литературы, рекомендованной рабочей программой; - использование научной терминологии, стилистическое и логическое изложение ответа на вопросы, умение делать выводы без существенных ошибок умения: - умеет ориентироваться в основных теориях, концепциях и направлениях по дисциплине и давать им оценку; - владеет инструментарием учебной дисциплины, умение его использовать в решении типовых задач; - умеет под руководством преподавателя решать стандартные задачи навыки: - работа под руководством преподавателя на практических занятиях, допустимый уровень культуры исполнения заданий; - достаточный минимальный уровень сформированности заявленных в рабочей программе компетенций; - испытывает затруднения при обосновании алгоритма выполнения заданий
Оценка «неудовлетворительно» (не зачтено)	знания: - фрагментарные знания по дисциплине; - отказ от ответа (выполнения письменной работы); - знание отдельных источников, рекомендованных рабочей программой по дисциплине; умения: - не умеет использовать научную терминологию; - наличие грубых ошибок навыки: - низкий уровень культуры исполнения заданий; - низкий уровень сформированности заявленных в рабочей программе компетенций; - отсутствие навыков самостоятельной работы; - не может обосновать алгоритм выполнения заданий

7.4. Теоретические вопросы и практические задания для проведения промежуточной аттестации обучающихся, необходимые для оценки знаний, умений и навыков и (или) опыта профессиональной деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

7.4.1. Теоретические вопросы для проведения промежуточной аттестации обучающихся

1. Приведите классификацию классических шифров по типу преобразования.
2. В чем заключается криптографическое преобразование в шифрах замены?
3. В чем заключается криптографическое преобразование в шифрах перестановки?
4. Приведите примеры шифров простой и сложной замены.
5. В чем принципиальное различие шифров простой и сложной многоалфавитной замены?
6. Почему омофонический шифр замены не является многоалфавитным шифром?
7. Приведите классификацию шифров по размеру преобразуемой информации.
8. Приведите примеры блочных и потоковых шифров.
9. В чем заключается различие блочных и потоковых шифров?
10. Сколько различных вариантов ключа имеет шифрующая система Цезаря?
11. Сколько различных вариантов ключа имеет шифр столбцовой перестановки, если шифрующая таблица имеет раз мер 5*5?
12. Сколько различных вариантов ключа имеет шифр табличной замены, если шифр-алфавит представляет собой случайную перестановку символов нормативного алфавита?
13. На каких принципах строится криптоанализ шифров простой замены?
14. На каких принципах строится криптоанализ табличной перестановки?
15. На каких принципах строится криптоанализ шифра Виженера?

16. Каковы основные этапы криптоанализа шифра Виженера?

17. Какие шифры называются гаммированием? Что такое гамма?

18. Какие ограничения требуется наложить на ключи шифра гаммирования, чтобы он был безусловно стойким?

19. Как производится гаммирование для двоичных данных?

20. Каковы проблемы при реализации безусловно стойкого шифра гаммирования?

21. Какая идея лежит в основе шифров колонной замены, в чем их отличие от шифров Виженера?

22. Перечислите модели шифров, введенных К. Шенноном. Чем вызвана необходимость введения обобщенной модели шифра?

23. Что понимается под энтропией криптосистемы? Как связана надежность криптосистемы с величиной ее энтропии?

24. Что понимается под интенсивностью и абсолютной интенсивностью языка (источника) сообщений? В каком случае их значения совпадают?

25. Что понимается под избыточностью языка, мерой чего она является?

26. Что понимается под расстоянием единственности шифра? Сможет ли криптоаналитик однозначно дешифровать криптограмму, если ее длина меньше расстояния единственности шифра?

27. Как связаны значения избыточности и расстояния единственности?

28. Какие шифры называются совершенными? Какая модель используется при определении совершенного шифра?

29. Какие условия накладываются на ключевую последовательность совершенного шифра? Приведите пример совершенного шифра.

30. Каковы принципы построения композиционных шифров?

31. Приведите примеры шифров, основанных на схеме Фейстеля.

32. Что такое ключ раунда? В каком порядке используются раундовые ключи при расшифровке сообщений?

33. Какие элементарные операции типа «перестановка» используются в раунде алгоритма DES?

34. Какие элементы раунда алгоритмов блочных шифров осуществляют элементарные операции тина «замена»?

35. Перечислите режимы работы блочных шифров. Какой из режимов является наиболее слабым? Какие режимы могут быть использованы для потокового шифрования?

36. В чем заключается суть лавинного эффекта алгоритма шифрования?

37. Какие алгоритмы считаются практически стойкими?

38. Каковы цели атак на криптографические алгоритмы?

39. Приведите классификацию атак на алгоритмы шифрования по типу известной информации. Какую из атак легче всего реализовать на практике?

40. В чем заключается метод грубой силы взлома криптосистем?

41. Сколько тестовых операций шифрования потребуется для вскрытия методом грубой силы алгоритма шифрования с ключом длиной n бит?

42. Как увеличивается трудоемкость вскрытия шифра методом грубой силы при увеличении длины ключа на один бит?

43. В каких случаях применим метод «встреча посередине»?

44. К каким типам атак относятся линейный, дифференциальный криптоанализ? Зависит ли их трудоемкость от числа раундов блочного алгоритма шифрования?

45. Назовите криитоаналитическую атаку, трудоемкость которой не зависят от количества раундов алгоритма шифрования.

46. Какие криитоаналитические атаки используют не слабости внутренней структуры шифров, а особенности их реализации?

47. Какие требования предъявляются к современным алгоритмам шифрования?

7.4.2. Практические задания для проведения промежуточной аттестации обучающихся

Типовые контрольные задания и иные материалы текущего контроля успеваемости размещены по адресу ЭИОС Moodle (https://moodle.spbgasu.ru/ Кафедры / Информационные технологии / Курсы для магистров ПМИ и ИСТ / Методы и средства защиты информации)

7.4.3. Примерные темы курсовой работы (проекта) (при наличии)

Курсовые работы (проекты) учебным планом не предусмотрены

7.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта профессиональной деятельности, характеризующие этапы формирования компетенций

Процедура проведения промежуточной аттестации и текущего контроля успеваемости регламентируется локальным нормативным актом, определяющим порядок организации и проведения текущего контроля успеваемости и промежуточной аттестации обучающихся.

Процедура оценивания формирования компетенций при проведении текущего контроля приведена в п. 7.2.

Типовые контрольные задания или иные материалы текущего контроля приведены в п. 7.3.

Промежуточная аттестация по дисциплине проводится в форме зачета.

7.6. Критерии оценивания сформированности компетенций при проведении промежуточной аттестации

	Уровень освоения и оценка			
	Оценка «неудовлетворительно»	Оценка «удовлетворительно»	Оценка «хорошо»	Оценка «отлично»
	«не зачтено»	«зачтено»		
Критерии оценивания	Уровень освоения компетенции «недостаточный». Компетенции не сформированы. Знания отсутствуют, умения и навыки не сформированы	Уровень освоения компетенции «пороговый». Компетенции сформированы. Сформированы базовые структуры знаний. Умения фрагментарны и носят репродуктивный характер. Демонстрируется низкий уровень самостоятельности практического навыка.	Уровень освоения компетенции «продвинутый». Компетенции сформированы. Знания обширные, системные. Умения носят репродуктивный характер, применяются к решению типовых заданий. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.	Уровень освоения компетенции «высокий». Компетенции сформированы. Знания аргументированные, всесторонние. Умения успешно применяются к решению как типовых, так и нестандартных творческих заданий. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка

знания	Обучающийся демонстрирует: -существенные пробелы в знаниях учебного материала; -допускаются принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; -непонимание сущности дополнительных вопросов в рамках заданий билета.	Обучающийся демонстрирует: -знания теоретического материала; -неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; -неуверенные и неточные ответы на дополнительные вопросы.	Обучающийся демонстрирует: -знание и понимание основных вопросов контролируемого объема программного материала; - знания теоретического материала -способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; -правильные и конкретные, без грубых ошибок, ответы на поставленные вопросы.	Обучающийся демонстрирует: -глубокие, всесторонние и аргументированные знания программного материала; -полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий, в рамках обсуждаемых заданий; -способность устанавливать и объяснять связь практики и теории, -логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора.
умения	При выполнении практического задания билета обучающийся продемонстрировал недостаточный уровень умений. Практические задания не выполнены Обучающийся не отвечает на вопросы билета при дополнительных наводящих вопросах преподавателя.	Обучающийся выполнил практическое задание билета с существенными неточностями. Допускаются ошибки в содержании ответа и решении практических заданий. При ответах на дополнительные вопросы было допущено много неточностей.	Обучающийся выполнил практическое задание билета с небольшими неточностями. Показал хорошие умения в рамках освоенного учебного материала. Предложенные практические задания решены с небольшими неточностями. Ответил на большинство дополнительных вопросов.	Обучающийся правильно выполнил практическое задание билета. Показал отличные умения в рамках освоенного учебного материала. Решает предложенные практические задания без ошибок Ответил на все дополнительные вопросы.

владение навыками	Не может выбрать методику выполнения заданий. Допускает грубые ошибки при выполнении заданий, нарушающие логику решения задач. Делает некорректные выводы. Не может обосновать алгоритм выполнения заданий.	Испытывает затруднения по выбору методики выполнения заданий. Допускает ошибки при выполнении заданий, нарушения логики решения задач. Испытывает затруднения с формулированием корректных выводов. Испытывает затруднения при обосновании алгоритма выполнения заданий.	Без затруднений выбирает стандартную методику выполнения заданий. Допускает ошибки при выполнении заданий, не нарушающие логику решения задач Делает корректные выводы по результатам решения задачи. Обосновывает ход решения задач без затруднений.	Применяет теоретические знания для выбора методики выполнения заданий. Не допускает ошибок при выполнении заданий. Самостоятельно анализирует результаты выполнения заданий. Грамотно обосновывает ход решения задач.

Оценка по дисциплине зависит от уровня сформированности компетенций, закрепленных за дисциплиной, и представляет собой среднее арифметическое от выставленных оценок по отдельным результатам обучения (знания, умения, владение навыками).

Оценка «отлично»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 4,5 до 5,0.

Оценка «хорошо»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 3,5 до 4,4.

Оценка «удовлетворительно»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 2,5 до 3,4.

Оценка «неудовлетворительно»/«не зачтено» выставляется, если среднее арифметическое находится в интервале от 0 до 2,4.

8. Учебно-методическое и материально-техническое обеспечение дисциплины (модуля)

8.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

№ п/п	Автор, название, место издания, издательство, год издания учебной и учебно-методической литературы	Количество экземпляров/электронный адрес ЭБС
	Основная литература	
1	Бескид П. П., Тагарникова Т. М., Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации, , 2010	http://www.iprbookshop.ru/17926.html
2	Башлы П. Н., Бабаш А. В., Баранова Е. К., Информационная безопасность и защита информации, Москва: Евразийский открытый институт, 2012	http://www.iprbookshop.ru/10677.html
3	Бескид П. П., Тагарникова Т. М., Криптографические методы защиты информации. Часть 1. Основы криптографии, , 2010	http://www.iprbookshop.ru/17925.html
4	Никифоров С. Н., Защита информации. Защищенные сети, СПб., 2017	http://ntb.spbgasu.ru/elib/00815/
5	Никифоров С. Н., Ромаданова М. М., Защита информации. Шифрование, СПб., 2017	74

	Дополнительная литература	
1	Никифоров С. Н., Защита информации, Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2015	http://www.iprbookshop.ru/74365.html
2	Новиков С. Н., Солонская О. И., Методы защиты информации, Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2009	http://www.iprbookshop.ru/54767.html
3	Никифоров С. Н., Защита информации. Защита от внешних вторжений, Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017	http://www.iprbookshop.ru/74381.html

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечиваются печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

8.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
Теоретико-числовые алгоритмы в криптографии	http://window.edu.ru/resource/845/23845/files/book.pdf
Технические средства и методы защиты информации	http://window.edu.ru/resource/611/63611/files/tsmzi.pdf

8.3. Перечень современных профессиональных баз данных и информационных справочных систем

Наименование	Электронный адрес ресурса
Система дистанционного обучения СПбГАСУ Moodle	https://moodle.spbgasu.ru/
Электронно-библиотечная система издательства "Лань"	https://e.lanbook.com/
Электронно-библиотечная система издательства "ЮРАЙТ"	https://www.biblio-online.ru/
Электронно-библиотечная система издательства "IPRsmart"	http://www.iprbookshop.ru/
Научная электронная библиотека eLIBRARY.RU	Научная электронная библиотека eLIBRARY.RU

8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного и свободно распространяемого программного обеспечения

Наименование	Способ распространения (лицензионное или свободно распространяемое)
Microsoft Windows 10 Pro	Договор № Д32009689201 от 18.12.2020г
IntelliJ IDEA Community	Свободно распространяемое

8.5. Материально-техническое обеспечение дисциплины
Сведения об оснащенности учебных аудиторий и помещений для самостоятельной работы

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность оборудованием и техническими средствами обучения
47. Компьютерный класс	Рабочие места с ПК (стол компьютерный, системный блок, монитор, клавиатура, мышь), стол рабочий, подключение к компьютерной сети СПбГАСУ, выход в Internet.

47. Помещения для самостоятельной работы	Помещение для самостоятельной работы (читальный зал библиотеки, ауд. 217): ПК-23 шт., в т.ч. 1 шт.- ПК для лиц с ОВЗ (системный блок, монитор, клавиатура, мышь) с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду СПбГАСУ. ПО Microsoft Windows 10
47. Учебные аудитории для проведения практических занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Учебная аудитория для проведения практических занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации – комплект мультимедийного оборудования (персональный компьютер, мультимедийный проектор, экран, аудио-система), доска маркерная белая эмалевая, комплект учебной мебели, подключение к компьютерной сети СПбГАСУ, выход в Интернет.

Для инвалидов и лиц с ОВЗ обеспечиваются специальные условия для получения образования в соответствии с требованиями нормативно-правовых документов.