МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

Кафедра №83

«УТВЕРЖДАЮ»
Руководитель направления
д.ю.н., проф.
(должность, уч. степень, звание)
В.В. Цмай
(подпись)
«17» мая 2019 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы информационной безопасности»
(Название дисциплины)

Код направления/ специальности	38.05.02
Наименование направления/ специальности	Таможенное дело
Наименование направленности/ специализации	Таможенные платежи
Форма обучения	очная

Санкт-Петербург 2019 г.

Лист согласования рабочей программы дисциплины

Программу составил(а)

доц.,к.т.н.,доц.	17.05.19	А.А. Овчинников
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Программа одобрена на заседании кафедры № 51
«15» мая 2019 г, протокол № 10

Заведующий кафедрой № 51

доц., к.т.н., доц.	17.05.19	А.А.Овчинников
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Ответственный за ОП 38.05.02(02)

Доц.	17.05.19	Т.В. Колесникова
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Заместитель директора института (декана факультета) № 8 по методической работе

доц.,к.э.н.,доц.	17.05.19	Л.Г. Фетисова
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Аннотация

Дисциплина «Основы информационной безопасности» входит в базовую часть образовательной программы подготовки студентов по направлению/специальности «38.05.02 «Таможенное дело» направленность «Таможенные платежи». Дисциплина реализуется кафедрой №51.

Дисциплина нацелена на формирование у выпускника

общепрофессиональных компетенций:

ОПК-1 «способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности»,

ОПК-3 «способность владеть методами и средствами получения, хранения, обработки информации, навыками использования компьютерной техники, программно-информационных систем, компьютерных сетей»;

профессиональных компетенций:

ПК-17 «умение выявлять и анализировать угрозы экономической безопасности страны при осуществлении профессиональной деятельности».

Содержание дисциплины охватывает круг вопросов, связанных с связанных с защитой компьютерной информации, существующих методов и информационных технологий этой защиты и оценкой их стойкости в информационных системах.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, практические занятия, самостоятельная работа студента.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов.

Язык обучения по дисциплине «русский».

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Цель курса - научить студентов понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности.

В курс включены основные методы криптографии, применяемые в защите информации. Анализ криптографических алгоритмов органически связан с синтезом криптоалгоритмов и криптопротоколов. В результате изучения курса студенты должны получить представление об основном криптографическом инструментарии, необходимом для использования защищенных информационных систем.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-1 «способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности»:

знать – основные теоретико-числовые задачи, использующиеся в задачах защиты информации

уметь – самостоятельно изучать и оценивать методы и алгоритмы информационной безопасности

владеть навыками – оценки эффективности различных средств информационной защиты;

иметь опыт деятельности – по использованию специального математического аппарата для решения практических задач;

ОПК-3 «способность владеть методами и средствами получения, хранения, обработки информации, навыками использования компьютерной техники, программно-информационных систем, компьютерных сетей»:

знать – методы построения информационных средств и технологий защиты информации

уметь – самостоятельно изучать математические модели криптоалгоритмов

владеть навыками - употребления отечественной терминологии в области криптографии для выражения количественных и качественных требований по защите информации;

иметь опыт деятельности – по использованию математического аппарата в проведении исследований;

ПК-17 «умение выявлять и анализировать угрозы экономической безопасности страны при осуществлении профессиональной деятельности»:

знать – основные виды угроз в сфере информационной безопасности и методы противодействия этим угрозам

уметь – оценивать риски от различных угроз в сфере информационной безопасности

владеть навыками – применения технологий информационной защиты в своей профессиональной деятельности

иметь опыт деятельности – в пользовании криптографическими библиотеками для решения прикладных задач в защищенных информационных системах.

2. Место дисциплины в структуре ОП

Дисциплина базируется на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- Информатика;
- Информационные таможенные технологии;
- Экономическая безопасность.

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и используются при изучении других дисциплин:

- Информационное право;
- Основы документооборота в таможенных органах

3. Объем дисциплины в ЗЕ/академ. час

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 1

Таблица 1 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№6
1	2	3
Общая трудоемкость дисциплины, ЗЕ/(час)	3/ 108	3/ 108
Аудиторные занятия, всего час., ***В том числе***	51	51
лекции (Л), (час)	34	34
Практические/семинарские занятия (ПЗ), (час)	17	17
лабораторные работы (ЛР), (час)		
курсовой проект (работа) (КП, КР), (час)		
Экзамен, (час)	27	27
Самостоятельная работа, всего	30	30
Вид промежуточного контроля: зачет, дифф. зачет, экзамен **(Зачет, Дифф. зач, Экз.)**	Экз.	Экз.

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий

Разделы и темы дисциплины и их трудоемкость приведены в таблице 2.

Таблица 2. – Разделы, темы дисциплины и их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 6					
Раздел 1. Основы информационной безопасности. Тема 1.1. Основы информационной безопасности и защиты информации Тема 1.2. Средства защиты информации	6	2			7
Раздел 2. Криптология Тема 2.1. Криптография Тема 2.2 Криптоанализ Тема 2.3. Коды и шифры Тема 2.4 История криптологии Тема 2.5 Криптология 20 века и современность Тема 2.6. Криптография с открытым ключом Тема 2.7. Хэширования Тема 2.8. Криптографические протоколы	24	10			7
Раздел 3. Вирусы и антивирусные программы	2	3			10
Раздел 4. Стеганография	2	2			6
Итого в семестре:	34	17			30
Итого:	34	17	0	0	30

4.2. Содержание разделов и тем лекционных занятий

Содержание разделов и тем лекционных занятий приведено в таблице 3.

Таблица 3 - Содержание разделов и тем лекционных занятий

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	Тема 1.1. Основы информационной безопасности и защиты информации Определение целей и принципов защиты информации; установление, факторов, влияющих на защиту информации; основные опасности и угрозы в области информационной безопасности. Представление информации в цифровом виде Тема 1.2. Средства защиты информации Классификации видов, методов и средств защиты информации. Организационная защита информации. Инженерно-техническая

	защита информации. Криптографическая защита информации.
2	Тема 2.1. Криптография. Составные элементы шифра. Термины. Требования к криптографическим системам. Тема 2.2 Криптоанализ. Методы криптоанализа. Техники социальной инженерии. Основные методы защиты. Тема 2.3. Коды и шифры. Задача обеспечения конфиденциальности. Определение шифра. Определение кодов. Код. Кодирование. Декодирование. Классификация шифров. Тема 2.4 История криптологии. Наивная криптография. Формальная криптография. Военная криптография. Принцип Керкгоффса Тема 2.5 Криптология 20 века и современность. Криптология в первую мировую войну. Шифровальные и дешифровальные машины. Криптология во вторую мировую войну. Шифры и компьютерные технологии. Тема 2.6. Криптография с открытым ключом. Криптографические алгоритмы с открытым ключом. Типы односторонних преобразований. Тема 2.7. Хэширование. Применение хэш-функций. Свойства алгоритмов. Свойства хэш-функций. Хэширование паролей. Тема 2.8. Криптографические протоколы. Протоколы обмена ключами. Протоколы аутентификации. Протоколы электронной подписи. Протоколы электронные платежей. Протоколы голосования.
3	Тема 3.1. Вирусы и антивирусные программы. Классификация вирусов. Методы защиты от вирусов. Антивирусные программы
4	Тема 4.1. Стеганография. Классическая стеганография. Компьютерная стеганография. Цифровая стеганография.

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 4.

Таблица 4 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	№ раздела дисципл-лины
Семестр 6				
	Задачи информационной безопасности	групповая дискуссия	2	1
	Исторические шифры	решение задач	6	2
	Криптографические алгоритмы с открытым ключом	решение задач	2	2
	Алгоритмы электронной подписи	решение задач	2	2
	Антивирусные программы	занятие по моделированию реальных условий	3	3
	Стеганография	групповая дискуссия	2	4

Всего:	17	

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	№ раздела дисциплины
Учебным планом не предусмотрено			

4.5. Курсовое проектирование (работа)

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 6.

Таблица 6 Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 6, час
1	2	3
Самостоятельная работа, всего	30	30
Изучение теоретического материала дисциплины (ТО)	25	25
Подготовка к текущему контролю (ТК)	5	5

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

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 8-10.

6. Перечень основной и дополнительной литературы

6.1. Основная литература

Перечень основной литературы приведен в таблице 7.

Таблица 7 – Перечень основной литературы

Шифр	Библиографическая ссылка / URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
	Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2020. — 180 с https://znanium.com/catalog/product/1018665.	
	Бабаш, А. В. Криптографические методы защиты информации.Т.1:Уч.-метод.пос./Бабаш А. В., 2-е	

	изд. - Москва : ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 413 с.: https://znanium.com/catalog/product/960001	
	Бабаш, А. В. Криптографические методы защиты информации.Т.1:Уч.-метод.пос./Бабаш А. В., 2-е изд. - Москва : ИЦ РИОР, НИЦ ИНФРА-М, 2019. - 413 с.: https://znanium.com/catalog/product/1022055	
	Баранова, Е. К. Основы информационней безопасности : учебник/ Е.К. Баранова, А.В. Бабаш. - Москва : РИОР : ИНФРА-М, 2019. — 202 с. — https://znanium.com/catalog/product/1014830	
	Бабаш Александр Владимирович **Криптографические методы защиты информации**.Т.1:Уч.-метод.пос./Бабаш А. В., 2-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 413 с. http://znanium.com/catalog/product/960001	
	Шабаршина, И. С. Основы компьютерной математики. Задачи системного анализа и управления : учебное пособие / И. С. Шабаршина, Е. В. Корохова, В. В. Корохов ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2019. - 142 с. - https://znanium.com/catalog/product/1088111	

6.2. Дополнительная литература

Перечень дополнительной литературы приведен в таблице 8.

Таблица 8 – Перечень дополнительной литературы

Шифр	Библиографическая ссылка/ URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004.4 К 84	Крук, Е. А. Методы программирования и прикладные алгоритмы [Текст]: учебное пособие в 3 ч. Ч. 1 / Е. А. Крук, А. А. Овчинников; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб.: Изд-во ГУАП, 2014. - 178 с.	40
004 Р69	Романьков, В. А. Введение в криптографию [Текст]: курс лекций / В. А. Романьков. - 2-е изд., испр. и доп. - М.: ФОРУМ, 2015. - 240 с	10
	Романьков, В. А. Введение в криптографию. Курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2020. — 240 с.: https://znanium.com/catalog/product/1046925	
	Торстейнсон, П. Криптография и безопасность в технологии .NET / Торстейнсон П., Ганеш Д.Г., - 3-е изд., (эл.) - Москва :БИНОМ. ЛЗ, 2015. - 482 chttps://znanium.com/catalog/product/478090	

	Руководство к решению задач по дискретной математике / Шубович А.А. - Волгоград: Волгоградский ГАУ, 2015. - 88 с. http://znanium.com/catalog.php?bookinfo=615250	
	Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2020. — 180 с. https://znanium.com/catalog/product/1018665	
	Пантелеев, А. В. Численные методы. Практикум : учебное пособие / А.В. Пантелеев, И.А. Кудрявцева. — Москва : ИНФРА-М, 2020. — 512 с. https://znanium.com/catalog/product/1028969	

7. Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

URL адрес	Наименование
https://www.pgpru.com/	Проект "OpenPGP в России"

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

8.1. Перечень программного обеспечения

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10 – Перечень программного обеспечения

№ п/п	Наименование
1.	Операционная система Microsoft Windows Professional 8 Russian Лицензия № 62047569; бессрочно
2.	Офис Microsoft Office Plus 2013 Russian Лицензия № 61351237; бессрочно

8.2. Перечень информационно-справочных систем

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11 – Перечень информационно-справочных систем

№ п/п	Наименование
1.	ЭБС ZNANIUM
2.	ЭБС Юрайт
3.	ЭБС издательства ЛАНЬ
4.	http://www.consultant.ru/ - Справочно-правовая система «Консультант Плюс»
5.	http://www.garant.ru/ - Информационно-правовой портал «ГАРАНТ»
6.	http://www.kodeks.ru/ - Справочно-правовая система «Кодекс»
7.	Реферативная база данных **Scopus** на платформе **SciVerse®** компании Elsevier;

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Состав материально-технической базы представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	**Учебная аудитории для проведения занятий лекционного типа** – укомплектована специализированной (учебной) мебелью, набором демонстрационного оборудования и учебно-наглядными пособиями, обеспечивающими тематические иллюстрации, соответствующие рабочим учебным программам дисциплин (модулей).	
2	**Учебная аудитории для проведения занятий семинарского типа** - укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.	
3	**Помещение для самостоятельной работы** – укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечено доступом в электронную информационно-образовательную среду организации	
4	**Учебная аудитория для текущего контроля и промежуточной аттестации** - укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.	

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

10.1. Состав фонда оценочных средств приведен в таблице 13

Таблица 13 - Состав фонда оценочных средств для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных средств
Экзамен	Список вопросов к экзамену; Задачи; Тесты.

10.2. Перечень компетенций, относящихся к дисциплине, и этапы их формирования в процессе освоения образовательной программы приведены в таблице 14.

Таблица 14 – Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Номер семестра	Этапы формирования компетенций по дисциплинам/практикам в процессе освоения ОП
ОПК-1 «способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-	

коммуникационных технологий и с учетом основных требований информационной безопасности»	
1	Общая теория права и государства
1	История таможенного дела и таможенной политики России
2	Информатика
3	Правовая охрана культурных ценностей
3	Гражданское право
3	Информационные таможенные технологии
3	Таможенные органы Северо-Западного Федерального округа
4	Таможенная статистика
5	Транспортное право
5	Европейское право
6	Декларирование товаров и транспортных средств
6	Основы информационной безопасности
6	Валютное регулирование и валютный контроль
6	Основы технических средств таможенного контроля
6	Международное таможенное право
6	Таможенное оформление товаров и транспортных средств
7	Административно-правовые основы деятельности таможенных органов
7	Таможенные процедуры
7	Технологии таможенного контроля (практикум)
7	Противодействие преступлениям в сфере экономической деятельности
7	Организация таможенного контроля товаров и транспортных средств
8	Защита интеллектуальной собственности
8	Таможенные платежи
ОПК-3 «способность владеть методами и средствами получения, хранения, обработки информации, навыками использования компьютерной техники, программно-информационных систем, компьютерных сетей»	
2	Информатика
2	Учебная практика по получению первичных профессиональных умений и навыков
3	Информационные таможенные технологии
4	Производственная практика по получению профессиональных умений и опыта профессиональной деятельности
6	Производственная практика по получению профессиональных умений и опыта профессиональной деятельности
6	Основы информационной безопасности
7	Учет таможенных платежей

8	Производственная практика по получению профессиональных умений и опыта профессиональной деятельности
10	Производственная преддипломная практика
ПК-17 «умение выявлять и анализировать угрозы экономической безопасности страны при осуществлении профессиональной деятельности»	
4	Экономическая безопасность
6	Основы информационной безопасности
7	Финансовые системы развитых и развивающихся стран
7	Международное предпринимательство
8	Взаимодействие таможенных органов и бизнеса
8	Международная интеграция
8	Национальная экспортная стратегия
9	Международные организации
9	Финансовая инфраструктура устойчивого развития
9	Экономика и политика стран постсоветского пространства
9	Свободные экономические зоны
9	Экономический потенциал таможенной территории России
9	Производственная практика научно-исследовательская работа
9	Таможенное регулирование в ЕАЭС
10	Производственная практика научно-исследовательская работа
10	Производственная преддипломная практика

10.3. В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала модульно–рейтинговой системы университета. В таблице 15 представлена 100–балльная и 4-балльная шкалы для оценки сформированности компетенций.

Таблица 15 –Критерии оценки уровня сформированности компетенций

Оценка компетенции		Характеристика сформированных компетенций
100-балльная шкала	4-балльная шкала	
85≤К ≤10	«отлично» «зачтено»	- обучающийся глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.
70≤К ≤84	«хорошо» «зачтено»	- обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой специализированных понятий.

55≤К ≤69	«удовлетво-рительно» «зачтено»	- обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.
К≤54	«неудовлетво рительно» «не зачтено»	- обучающийся не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

10.4. Типовые контрольные задания или иные материалы:

1. Вопросы (задачи) для экзамена (таблица 16)

Таблица 16 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена
1	Информация и информационная безопасность. Основные составляющие и термины.
2	Объекты, категории и носители информации.
3	Средства защиты и способы передачи информации.
4	Код. Кодирование и декодирование информации.
5	Стойкость шифров и существующие угрозы.
6	Техники социальной инженерии.
7	Выбор криптографических методов защиты и требования, предъявляемые к системам.
8	Основные определения криптографии и классификации шифров
9	История криптографии
10	Исторические шифры перестановки. Привести пример
11	Шифры перестановки. Решетка Кардано
12	Шифры замены. Шифр Виженера
13	Шифры замены. Цилиндр Джефферсона
14	Составные шифры. Подстановочно-перестановочная сеть.
15	Составные шифры. Сеть Файстеля.
16	Шифры замены. Привести пример
17	Шифры перестановки. Привести пример
18	Современный этап развития криптографии
19	Симметричные алгоритмы шифрования
20	Шифрование с открытым ключом
21	Хэш-функции
22	Криптографические протоколы
23	Протоколы обмена ключами
24	Протоколы аутентификации
25	Протоколы электронной подписи
26	Протоколы электронных платежей
27	Протоколы голосования
28	Основы криптоанализа
29	Стеганография

30	Подпись RSA
31	Система Эль-Гамаля
32	Подпись Эль-Гамаля
33	Криптосистема Меркле-Хеллмана
34	Подпись ГОСТ Р 34.10-2012
35	Классификация вирусов и антивирусных
36	программ Стандарт шифрования DES

2. Вопросы (задачи) для зачета / дифференцированного зачета (таблица 17)

Таблица 17 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	Учебным планом не предусмотрено

3. Темы и задание для выполнения курсовой работы / выполнения курсового проекта (таблица 18)

Таблица 18 – Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта

№ п/п	Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта
	Учебным планом не предусмотрено

4. Вопросы для проведения промежуточной аттестации при тестировании (таблица 19)

Таблица 19 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
1	Необходимое условие "совершенной стойкости" шифра
2	Наибольшая угроза при криптоанализе шифра
3	Принцип Кирхгофа
4	Функция Эйлера
5	Взаимно простые числа
6	Анализ подстановочного шифра
7	Анализ перестановочного шифра
8	Сеть Файстеля
9	Симметричный шифр
10	Асимметричный шифр
11	Шифр Цезаря
12	Одноразовый блокнот
13	Полиалфавитный подстановочный шифр
14	Роторные машины
15	Стандарт шифрования России
16	Длины ключей шифров-стандартов
17	Сравнение шифров ГОСТ и DES
18	Операции функции шифрования DES
19	Взлом симметричного блокового шифра перебором по ключу
20	Количество раундов шифров-стандартов
	Многократное шифрование
	Построение генераторов ключевых потоков
	"Трудные" задачи в криптографии

21	Система RSA
22	Система Меркли-Хеллмана
23	Система Эль-Гамаля
24	Функции с закрытыми дверями
25	Протокол Диффи-Хеллмана
26	Цифровая подпись RSA
27	Цифровая подпись Эль-Гамаля
28	Стандарт цифровой подписи в России

5. Контрольные и практические задачи / задания по дисциплине (таблица 20)

Таблица 20 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
	Задание 1. Основы модульной арифметики (50 вариантов) Пример задания: Вариант 1. Вычислить: -17 mod 44 -31 mod 17 -49 mod 16 -76 mod 11 23 mod 50 Задание 2. Нахождение мультипликативных обратных с помощью алгоритма Евклида (50 вариантов) Пример задания: Вариант 1. Вычислить: $8011^{-1} \bmod 16732$ Задание 3. Быстрое возведение в степень (50 вариантов) Пример задания: Вариант 1. Вычислить: $19^{220} \bmod 73$ Задание 4. Системы с открытым ключом: системы RSA, Мак-Элиса, Эль-Гамаля (индивидуальные варианты) Пример задания: Построить открытый и секретный ключи, зашифровать и расшифровать сообщение с помощью системы Мак-Элиса, для сообщения m = 100101. Параметр M определяется индивидуальным номером студента, остальные параметры системы выбрать самостоятельно. Задание 5. Системы ЭЦП: системы RSA, Эль-Гамаля (индивидуальные варианты) Пример задания: Построить открытый и секретный ключи, подписать и проверить подпись сообщения с помощью системы Эль-Гамаля. Сообщение M определяется индивидуальным номером студента, размер открытого модуля $p > 19$, остальные параметры ЭЦП выбрать самостоятельно.

10.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и / или опыта деятельности, характеризующих этапы формирования компетенций, содержатся в Положениях «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-

рейтинговой системе оценки качества учебной работы студентов в ГУАП».

11. Методические указания для обучающихся по освоению дисциплины

Цель дисциплины - научить студентов понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности.

Методические указания для обучающихся по освоению лекционного материала

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемы результаты при освоении обучающимся лекционного материала:

– получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;

– получение опыта творческой работы совместно с преподавателем;

– развитие профессионально–деловых качеств, любви к предмету и самостоятельного творческого мышления.

– появление необходимого интереса, необходимого для самостоятельной работы;

– получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;

– научится методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);

– получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

Раздел 1. Основы информационной безопасности.

Тема 1.1. Основы информационной безопасности и защиты информации

Тема 1.2. Средства защиты информации

Раздел 2. Криптология

Тема 2.1. Криптография

Тема 2.2 Криптоанализ

Тема 2.3. Коды и шифры

Тема 2.4 История криптологии

Тема 2.5 Криптология 20 века и современность

Тема 2.6. Криптография с открытым ключом

Тема 2.7. Хэширования

Тема 2.8. Криптографические протоколы

Раздел 3. Вирусы и антивирусные программы

Тема 3.1. Вирусы

Тема 3.2. Антивирусные программы

Раздел 4. Стеганография

Методические указания для обучающихся по прохождению практических занятий

Практическое занятие является одной из основных форм организации учебного процесса, заключающаяся в выполнении обучающимися под руководством преподавателя комплекса учебных заданий с целью усвоения научно-теоретических основ учебной дисциплины, приобретения умений и навыков, опыта творческой деятельности.

Целью практического занятия для обучающегося является привитие обучающемся умений и навыков практической деятельности по изучаемой дисциплине.

Планируемые результаты при освоении обучающемся практических занятий:

– закрепление, углубление, расширение и детализация знаний при решении конкретных задач;

– развитие познавательных способностей, самостоятельности мышления, творческой активности;

– овладение новыми методами и методиками изучения конкретной учебной дисциплины;

– выработка способности логического осмысления полученных знаний для выполнения заданий;

– обеспечение рационального сочетания коллективной и индивидуальной форм обучения.

Функции практических занятий:

– познавательная;

– развивающая;

– воспитательная.

По характеру выполняемых обучающимся заданий по практическим занятиям подразделяются на:

– ознакомительные, проводимые с целью закрепления и конкретизации изученного теоретического материала;

– аналитические, ставящие своей целью получение новой информации на основе формализованных методов;

– творческие, связанные с получением новой информации путем самостоятельно выбранных подходов к решению задач.

Формы организации практических занятий определяются в соответствии со специфическими особенностями учебной дисциплины и целями обучения. Они могут проводиться:

– в интерактивной форме (решение ситуационных задач, занятия по моделированию реальных условий, деловые игры, игровое проектирование, имитационные занятия, выездные занятия в организации (предприятия), деловая учебная игра, ролевая игра, психологический тренинг, кейс, мозговой штурм, групповые дискуссии);

– в не интерактивной форме (выполнение упражнений, решение типовых задач, решение ситуационных задач и другое).

Методика проведения практического занятия может быть различной, при этом важно достижение общей цели дисциплины.

Требования к проведению практических занятий

Вариант задания по каждой задаче при выполнении практических и контрольных заданий обучающийся получает в соответствии с номером в списке группы. Перед решением задачи обучающемуся следует внимательно ознакомиться с условием задачи, с рассмотренными примерами, а также содержанием соответствующих тем лекционного курса.

В соответствии с заданием обучающийся должен привести решение с необходимыми вычислениями и пояснениями, получить требуемые результаты, оформить задание для сдачи преподавателю.

Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

В процессе выполнения самостоятельной работы, у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет им развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся являются:

– учебно-методический материал по дисциплине;

– методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

Для развития у студентов навыков самостоятельного овладения теоретическим материалом ряд тем дисциплины на лекционных занятиях дается обзорно, что предполагает их самостоятельное детальное изучение.

Примерные темы для самостоятельного изучения:

1. Метод тотального опробования ключей. Определение числа ключей в ряде конкретных схем шифраторов.
2. Протоколы цифровых денег
3. Роторные машины.
4. Многократное шифрование.
5. Методы построения больших периодов в поточных шифрах.
6. m-последовательности.
7. Нелинейное комбинирование РСЛОС
8. Методы целочисленной факторизации
9. Методы вычисления дискретных логарифмов
10. Постквантовая криптография
11. Доказательства с нулевым разглашением
12. Защищенные распределенные вычисления
13. Методы анализа хэш-функций. Вычисление вероятностей коллизий

Методические указания для обучающихся по прохождению текущего контроля

Текущий контроль осуществляется по усмотрению преподавателя в рабочем порядке на практических (семинарских) занятиях. Формой текущего контроля могут быть устный опрос, проверка домашнего задания, контрольная работа, отчет по сделанному докладу, написание реферата, эссе, подготовка презентации по теме занятия, реферирование первоисточников и др.

Результаты текущего контроля сообщаются обучающимся непосредственно на занятии или аккумулируются в Личном кабинете обучающегося. Оценка текущих знаний может осуществляться либо в рейтинговых баллах, либо по пятибалльной системе («неудовлетворительно», «удовлетворительно», «хорошо», «отлично»). Количество заработанных баллов или средняя оценка сообщаются обучающимся. Наличие текущих оценок (баллов) у обучающегося является условием допуска к промежуточной аттестации и является составной частью итоговой оценки уровня усвоения программы дисциплины.

Методические указания для обучающихся по прохождению промежуточной аттестации

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя экзамен. Экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программы высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой