МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

Кафедра №51

«УТВЕРЖДАЮ»
Руководитель направления
д.э.н.,проф.
ность, уч. степень, звание)
В.Б. Сироткин
(подпись)

«21» мая 2019г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы информационной безопасности»
(Название дисциплины)

Код направления	38.03.02
Наименование направления/ специальности	Менеджмент
Наименование направленности	Финансовый менеджмент
Форма обучения	заочная

Санкт-Петербург2019г.

Лист согласования рабочей программы дисциплины

Программу составил(а)

доц., к.т.н., доц. _____ 27.04.19 А.А.Овчинников

должность, уч. степень, звание подпись, дата инициалы, фамилия

Программа одобрена на заседании кафедры № 51

«27»апреля 2019 г, протокол № 9

Заведующий кафедрой № 51

проф.,д.т.н.,проф. _____ 27.04.19 Е.А. Крук

должность, уч. степень, звание подпись, дата инициалы, фамилия

Ответственный за ОП 38.03.02(02)

доц.,к.э.н.,доц. _____ 27.04.19 Ю.А. Мартынова

должность, уч. степень, звание подпись, дата инициалы, фамилия

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

доц.,к.э.н.,доц. _____27.04.19 Л.Г. Фетисова

должность, уч. степень, звание подпись, дата инициалы, фамилия

Аннотация

Дисциплина «Основы информационной безопасности» входит в базовую часть образовательной программы подготовки обучающихся по направлению 38.03.02 «Менеджмент» направленность «Финансовый менеджмент». Дисциплина реализуется кафедрой №51.

Дисциплина нацелена на формирование у выпускника

общекультурных компетенций:

ОК-6 «способность к самоорганизации и самообразованию»;

общепрофессиональных компетенций:

ОПК-7 «способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности».

Содержание дисциплины охватывает круг вопросов, 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. Целипреподаваниядисциплины

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:

ОК-6 «способность к самоорганизации и самообразованию»:

знать - содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности;

уметь - планировать цели и устанавливать приоритеты при выборе способов принятия решений с учетом условий, средств, личностных возможностей и временной перспективы достижения, осуществления профессиональной деятельности;

владеть навыками - саморегуляции эмоциональных и функциональных состояний при выполнении профессиональной деятельности;

иметь опыт деятельности - самостоятельной работы с научной и практической литературой по дисциплине «Основы информационной безопасности», публично представить результаты.

ОПК-7 «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 - методы построения информационных средств и технологий защиты информации

уметь - самостоятельно изучать и строить 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.

2. Местодисциплины в структуре ОП

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

- Информатика
- Математика. Теория вероятностей и математическая статистика
- Информационныесистемы в менеджменте.

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

- Риск-менеджмент.

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 трудоемкостьдисциплины

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***	16	16
лекции (Л), (час)	8	8
Практические/семинарские занятия (ПЗ), (час)	8	8
лабораторные работы (ЛР), (час)		
курсовой проект (работа) (КП, КР), (час)		
Экзамен, (час)	9	9
Самостоятельная работа, всего (час)	83	83
Вид промежуточного контроля: зачет, дифф. зачет, экзамен **(Зачет, Дифф. зач, Экз.)**	Экз.	Экз.

4. Содержаниедисциплины

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, темыдисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 6					
Раздел 1. Основные понятия криптографии Тема 1.1. Основные определения Тема 1.2. Задачи информационной безопасности	2				15
Раздел 2. Симметричные шифры Тема 2.1. Исторические шифры Тема 2.2. Блоковые шифры Тема 2.3. Потоковые шифры	2	2			20
Раздел 3. Криптография с открытым ключом Тема 3.1. Математические основы систем с открытым ключом Тема 3.2. Основные алгоритмы с открытым ключом	3	4			20
Раздел 4. Криптографические протоколы Тема 4.1. Основные протоколы с открытым	1	2			20

ключом Тема 4.2. Специальные протоколы					
Текущий контроль					8
Итого в семестре:	8	8			83
Итого:	8	8	0	0	83

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. Основные определения Определение целей и принципов защиты информации; установление, факторов, влияющих на защиту информации; основные опасности и угрозы в области информационной безопасности. Классификации видов, методов и средств защиты информации. Организационная защита информации. Инженерно-техническая защита информации. Криптографическая защита информации. Представление информации в цифровом виде. Тема 1.2. Задачи информационной безопасности Задача обеспечения конфиденциальности. Определение шифра. Задача обеспечения аутентификации, понятия об электронной цифровой подписи (ЭЦП). Основные задачи в области управления ключами. Криптопротоколы: обеспечение идентификации, разделение секрета, выработка ключа, цифровые деньги.
2	Тема 2.1. Исторические шифры Подстановочные шифры и перестановочные шифры. Шифр Цезаря, аффинный шифр, шифр моноалфавитной замены. Шифр Виженера. Цилиндр Джефферсона. Полиалфавитные шифры. Роторные машины. Тема 2.2. Блоковые шифры Понятие стойкости, предположения об исходных условиях криптоанализа, совершенная стойкость. Одноразовый блокнот. Шифр Вернама. Принципы построения блоковых шифров. Свойства смешивания и рассеивания. Составные шифры, итеративные шифры. SP-сети, сети Файстеля. Современные системы шифрования: алгоритмы DES, ГОСТ 28147-89, AES. Режимы блокового шифрования: ECB, CBC, CFB, OFB. Режим счетчика. Многократное шифрование. Тема 2.3. Потоковые шифры Требования к поточным шифрам. Методы построения больших периодов в поточных шифрах. Регистры сдвига с линейной обратной связью (РСЛОС). m-последовательности. Алгоритм Берлекэмпа-Месси. Построение потоковых шифров на основе РСЛОС. Нелинейное комбинирование РСЛОС: генератор Геффе, шифры с контролем тактов. Применение поточного шифрования.
3	Раздел 3. Криптография с открытым ключом Тема 3.1. Математические основы систем с открытым ключом Модульная арифметика. Алгоритм Евклида и его сложность. Расширенный алгоритм Евклида. Основные теоремы о вычетах. Функция Эйлера. Теоремы Эйлера, Ферма. Факторизация. Логарифмирование в конечных полях. Оценки сложности “трудных” проблем, на которых строятся системы с открытым ключом. Быстрое возведение в степень. Тема 3.2. Основные алгоритмы с открытым ключом Система Меркли-Хеллмана. Схема RSA. Атаки на RSA. Схема шифрования Эль-Гамаля. Система Мак-Элиса. Криптографические хэш-функции. Понятие о цифровой подписи. Подпись RSA. Подпись Эль-Гамаля. Подпись DSA. ЭЦП ГОСТ Р 34.10-94 и ГОСТ Р 34.10-01.
4	Тема 4.1. Основные протоколы с открытым ключом

	Выработка ключа. Протокол Диффи-Хелмана. Гибридные системы шифрования: цифровой конверт. Доказательство с нулевым разглашением. Схема идентификации Фиата-Шамира. Схема идентификации Гиллу-Квискуотера. Инфраструктура открытых ключей. Сертификаты открытых ключей. Тема 4.2. Специальные протоколы Слепая подпись. Протоколы разделения секрета и вручения бит. Протоколы цифровых денег и электронного голосования. Защищенные распределенные вычисления.

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	Формыпрактических занятий	Трудоемкость, (час)	№ раздела дисцип-лины
Семестр 6				
1	Задачи информационной безопасности	групповая дискуссия	1	1
2	Исторические шифры	решение ситуационных задач	1	2
3	Блоковые шифры	решение ситуационных задач	1	2
4	Математические основы систем с открытым ключом	решение ситуационных задач	2	3
5	Основные алгоритмы с открытым ключом	решение ситуационных задач	1	3
6	Основные протоколы с открытым ключом	занятие по моделированию реальных условий	1	4
7	Специальные протоколы	деловая учебная игра	1	4
		Всего:	8	

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
Учебнымпланомнепредусмотрено			

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	83	83
Изучение теоретического материала дисциплины (ТО)	35	35
Подготовка к текущему контролю (ТК)	8	8
Домашнее задание (ДЗ)	40	40

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. Переченьосновной и дополнительнойлитературы

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)
	Компьютерная математика: Учебное пособие /К.В.Титов - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 261 с. http://znanium.com/catalog.php?bookinfo=523231	
	Теоретико-численные методы в криптографии: Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. – 160 с. http://www.znanium.com/catalog.php?bookinfo=441493	

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)
	Торстейнсон, П. Криптография и безопасность в технологии .NET [Электронный ресурс] / П. Торстейнсон, Г.А. Ганеш; пер. с англ. - 2-е изд. - М.: БИНОМ. Лаборатория знаний, 2013. - 480 с. http://znanium.com/catalog.php?bookinfo=478090	
	Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие /	

	Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск: Сибирский федеральный университет, 2011. - 160 с. http://znanium.com/catalog.php?bookinfo=441493	
	Руководство к решению задач по дискретной математике / Шубович А.А. - Волгоград: Волгоградский ГАУ, 2015. - 88 с. http://znanium.com/catalog.php?bookinfo=615250	

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

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплиныприведен 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	Microsoft Windows
2	Microsoft Office

*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 «ЛАНЬ»
3	http://libgost.ru/ Библиотека ГОСТов и нормативных документов

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 аудитория 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 практических занятий** - Аудитория укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации большой аудитории.	

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.

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
ОК-6 «способность к самоорганизации и самообразованию»	
1	Математика. Аналитическая геометрия и линейная алгебра
1	Математика. Математический анализ
1	Информатика
1	Основы социального государства
1	Иностранный язык
1	Прикладная физическая культура (элективный модуль)
1	История
1	Экономическая география и регионалистика
2	Иностранный язык
2	Культурология
2	Математика. Математический анализ
2	История управленческой мысли
2	Прикладная физическая культура (элективный модуль)
2	Информатика
2	Экономика. Микроэкономика
2	Концепции современного естествознания
2	Учебная практика
3	Математика. Теория вероятностей и математическая статистика
3	Экономика организации
3	Прикладная физическая культура (элективный модуль)
3	Экономика. Макроэкономика

3	Философия
3	Иностранный язык
3	Социология и политология
4	Институциональная экономика
4	Прикладная физическая культура (элективный модуль)
4	Иностранный язык
4	Психология и педагогика
4	Мировая экономика и международные экономические отношения
4	Статистика
4	Основы менеджмента
4	Производственная практика
4	Организация связей с общественностью
4	Безопасность жизнедеятельности
4	Деловая этика
5	Экология
5	Теория организации
5	Информационные системы в менеджменте
5	Финансовый учет
5	Основы менеджмента
5	Институциональная экономика
5	Социально-экономическая статистика
5	Иностранный язык (второй)
5	Прикладная физическая культура (элективный модуль)
5	Деловой иностранный язык
5	Мировая экономика и международные экономические отношения
6	Правоведение
6	Физическая культура
6	Финансовый анализ
6	Основы информационной безопасности
6	Деловой иностранный язык
6	Исследование систем управления
6	Иностранный язык (второй)
6	Информационные технологии
6	Производственная практика
7	Организационное поведение
7	Финансовые рынки и институты
7	Методы принятия управленческих решений
7	Деловые коммуникации
7	Маркетинг
7	Моделирование бизнес-процессов
7	Государственное и муниципальное управление
8	Финансовый менеджмент
8	Управление проектами

8	Бизнес-планирование
8	Управленческий учет
8	Управление человеческими ресурсами
8	Управление качеством
8	Финансовые рынки и институты
9	Управление развитием персонала
9	Финансовый менеджмент
9	Управление изменениями
9	Антикризисное управление
9	Управление вознаграждением персонала
9	Оценка инвестиций
9	Управление операциями
9	Стратегический менеджмент
10	Риск-менеджмент
10	Корпоративная социальная ответственность
10	Стратегический менеджмент
10	Конфликтология
10	Управленческое консультирование
10	Деловое администрирование
10	Управление изменениями
10	Производственная преддипломная практика
ОПК-7 «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	Информатика
2	Информатика
4	Производственная практика
6	Основы информационной безопасности
6	Информационные технологии
7	Деловые коммуникации

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	
$85 \le K \le 100$	«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.
$70 \le K \le 84$	«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.
$55 \le K \le 69$	«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.
$K \le 54$	«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	Задача обеспечения секретности.
2	Шифры подстановок. Примеры.
3	Шифры перестановок. Примеры.
4	Стойкость шифров. Модель атакующего. Уровни атаки
5	Симметричные шифры. Свойства, принципы построения.
6	Итеративные блоковые шифры. Сети Файстеля. Примеры.
7	Шифр DES.
8	Шифр FEAL
9	Шифр ГОСТ 28147-89.
10	Шифр AES
11	Режимы блокового шифрования.
12	Асимметричные шифры. Свойства, принципы построения.
13	Система RSA.
14	Система Меркли-Хеллмана
15	Система Эль-Гамаля
16	Задача обеспечения аутентификации. Цифровая подпись.
17	Подпись RSA.
18	Подпись Эль-Гамаля.
19	Криптографические хэш-функции. Свойства, применение
20	Распределение симметричных ключей. Протокол Диффи-Хеллмана.

21 22	Распределение симметричных ключей. Цифровой конверт. Распределение открытых ключей. Сертификаты открытых ключей

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 выполнениякурсовой 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
	Учебным планом не предусмотрено

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} mod16732 Задание 3. Быстрое возведение в степень (50 вариантов) Пример задания: Вариант 1. Вычислить: 19^{220}mod 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.

Планируемые 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. Основные понятия криптографии
Тема 1.1. Основные определения
Тема 1.2. Задачи информационной безопасности
Раздел 2. Симметричные шифры
Тема 2.1 Исторические шифры
Тема 2.2 Блоковые шифры
Тема 2.3 Потоковые шифры
Раздел 3. Криптография с открытым ключом
Тема 3.1 Математические основы систем с открытым ключом
Тема 3.2 Основные алгоритмы с открытым ключом
Раздел 4. Криптографические протоколы
Тема 4.1 Основные протоколы с открытым ключом
Тема 4.2 Специальные протоколы

Методические указания для обучающихся по прохождениюпрактических занятий

Практическое занятие является одной из основных форм организации учебного процесса, заключающейся 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.

Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.

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.

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 промежуточной аттестации

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

– 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 программам 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