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

Кафедра №51

«УТВЕРЖДАЮ»
Руководитель направления
д.т.н.,проф.
(должность, уч. степень, звание)
К.В. Зайченко
(подпись)
«16» мая 2018 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы информационной безопасности»

Код направления	11.05.01
Наименование направления/ специальности	Радиоэлектронные системы и комплексы
Наименование направленности	Радиоэлектронные системы передачи информации
Форма обучения	очная

Санкт-Петербург 2018 г.

Лист согласования рабочей программы дисциплины

Программу составил

доц., к.т.н., доц. _____16.05.2018 А.А. Овчинников
должность, уч. степень, звание подпись, дата инициалы, фамилия

Программа одобрена на заседании кафедры № 51

«16» мая 2018 г, протокол №9

Заведующий кафедрой № 51

доц., к.т.н., _____16.05.2018 А.А. Овчинников
подпись, дата

Ответственный за ОП 12.04.04(01)

к.т.н.,доц. _____16.05.2018 К.Н. Тимофеев
должность, уч. степень, звание подпись, дата инициалы, фамилия

Заместитель директора института (декана факультета) № 2 по методической работе

доц.,к.т.н.,доц. _____16.05.2018 О.Л. Балышева
должность, уч. степень, звание подпись, дата инициалы, фамилия

Аннотация

Дисциплина «Основы информационной безопасности» входит в базовую часть образовательной программы подготовки студентов по направлению/специальности «11.05.01 «Радиоэлектронные системы и комплексы» направленность «Радиоэлектронные системы передачи информации». 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»;

профессионально-специализированных компетенций:

ПСК-2.3 «способность проводить оптимизацию радиосистем передачи информации и отдельных её подсистем».

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

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, 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 образовательной программы

В результате освоения дисциплины студент 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 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 решении задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ПСК-2.3 «способность проводить оптимизацию радиосистем передачи информации и отдельных её подсистем»:

знать – методы оптимизации радиосистем передачи информации и отдельных её подсистем с учетом существующих рисков от различных угроз информационной безопасности;

уметь – применять методы оптимизации радиосистем передачи информации и отдельных её подсистем с учетом существующих рисков от различных угроз информационной безопасности;

владеть навыками – применения методов оптимизации радиосистем передачи информации и отдельных её подсистем с учетом рисков от различных угроз информационной безопасности

иметь опыт деятельности – в реализации радиосистем передачи информации и отдельных её подсистем в защищенном исполнении.

2. Место дисциплины в структуре ОП

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

- Информатика;
- Информационные технологии;
- Основы теории связи.

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

- Проектирование, разработка и исследование РЭС.

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
			№7
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)		
Лабораторные работы (ЛР),	(час)	17	17
Курсовой проект (работа) (КП, КР),	(час)		
Экзамен,	(час)	36	36
Самостоятельная работа, всего	(час)	21	21
Вид промежуточной аттестации: зачет, экзамен, дифференцированный зачет **(Зачет. Экз. Дифф. зач)**		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 7					
Раздел 1. Основные понятия криптографии Тема 1.1. Основные определения Тема 1.2. Задачи информационной безопасности	6		-		2
Раздел 2. Симметричные шифры Тема 2.1. Исторические шифры Тема 2.2. Блоковые шифры Тема 2.3. Потоковые шифры	10		8		6
Раздел 3. Криптография с открытым ключом Тема 3.1. Математические основы систем с открытым ключом Тема 3.2. Основные алгоритмы с открытым ключом	10		5		6
Раздел 4. Криптографические протоколы Тема 4.1. Основные протоколы с открытым ключом Тема 4.2. Специальные протоколы	8		4		7
Итого в семестре:	34		17		21
Итого:	34	0	17	0	21

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	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	Формы практических занятий	Трудоемкость, (час)	№ раздела дисциплины
Учебным планом не предусмотрено				

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
Семестр 7			
1	Реализация исторического (подстановочного или перестановочного) шифра	2	2
2	Криптоанализ исторического шифра	2	2
3	Реализация симметричного блокового шифра	2	2
4	Реализация потокового генератора	2	2
5	Реализация системы с открытым ключом	2	3
6	Реализация ЭЦП	3	3
7	Реализация криптографического протокола по управлению ключами	2	4
8	Реализация специального криптографического протокола	2	4
	Всего:	17	

4.5. Курсовое проектирование (работа)

Учебным планом не предусмотрено.

4.6. Самостоятельная работа студентов

Виды самостоятельной работы и ее трудоемкость приведены в таблице 6.

Таблица 6 - Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 7, час
1	2	3
Самостоятельная работа, всего	21	21
Изучение теоретического материала дисциплины (ТО)	9	9
Подготовка к текущему контролю (ТК)	4	4
Подготовка лабораторных работ (ЛР)	8	8

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

Учебно-методические материалы для самостоятельной работы студентов 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)
004 Р 98	Рябко, Б. Я. Криптографические методы защиты информации [Текст]: учебное пособие / Б. Я. Рябко, А. Н. Фионов. - 2-е изд., стер. - М.: Горячая линия - Телеком, 2014. - 229 с.	10
004 М 75	Молдовян, Н. А. Теоретический минимум и алгоритмы цифровой подписи [Текст]: учебное пособие / Н. А. Молдовян. - СПб.: БХВ - Петербург, 2014. - 304 с.	4
004 М 87	Мошак Н. Н. Организация безопасного доступа к информационным ресурсам [Текст]: учебное пособие / Н. Н. Мошак, Т. М. Татарникова. приборостроения. - СПб.: Изд- во ГУАП, 2014. - 121 с.	40
Х404.3 М 48	Информационная безопасность и защита информации: учебное пособие/ В. П. Мельников, С. А. Клейменов, А. М. Петраков; ред. С. А Клейменов. - 5-е изд., стер. - М.: Академия, 2011. - 331 с.	25
	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)
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 М 87-604316-ED	Мошак Н.Н. Защищенные инфотелекоммуникации. Анализ и синтез [Электронный ресурс]: монография /Н.Н. Мошак. – Электрон. Текстовые дан. – СПб.: Изд-во ГУАП, 2014. – 197 с.	40
004.056.55(075) Б 70	Блоковые шифры: Учебное пособие/ С. В. Беззатеев, Е. А. Крук, А.А. Овчинников, В. Б. Прохорова. - СПб.: РИО ГУАП, 2003. - 63 с.	49
004 Р 69	Романьков, В. А. Введение в криптографию [Текст]: курс лекций / В. А. Романьков. - 2-е изд., испр. и	10

	доп. - М.: ФОРУМ, 2015. - 240 с	
004.056(075) К84	Крук, Е. А., Линский Е.М. Криптография с открытым ключом. Кодовые системы: Учебное пособие. СПб.: РИО ГУАП, 2004. - 52 с.	20
004.056.55(075) Б 70	Блоковые шифры: Учебное пособие/ С. В. Беззатеев, Е. А. Крук, А.А. Овчинников, В. Б. Прохорова; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб.: РИО ГУАП, 2003. - 63 с.	49
	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 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	Программный комплекс PGP
2	Менеджер паролей KeePass

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	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	Лекционная аудитория	
2	Вычислительная лаборатория с компьютерами под управлением ОС Windows версии не ранее XP, объединенных в локальную сеть	

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	Информатика
2	Информатика
2	Информационные технологии
2	Учебная (информационно-вычислительная) практика
4	Основы теории связи
7	Основы информационной безопасности
8	Высокоуровневые методы информатики и программирования
ПСК-2.3 «способность проводить оптимизацию радиосистем передачи информации и отдельных её подсистем»	
7	Основы информационной безопасности
7	Методы оптимального измерения параметров сигналов
9	Проектирование, разработка и исследование РЭС
10	Проектирование, разработка и исследование РЭС

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	
$85 \le К \le 100$	«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.
$70 \le К \le 84$	«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.
$55 \le К \le 69$	«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.
$К \le 54$	«неудовлетворительно» «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
	Учебным планом не предусмотрено

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

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

№ 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	Распределение симметричных ключей. Цифровой конверт.
22	Распределение открытых ключей. Сертификаты открытых ключей

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
21	Многократное шифрование
22	Построение генераторов ключевых потоков
23	"Трудные" задачи в криптографии

24	Система RSA
25	Система Меркли-Хеллмана
26	Система Эль-Гамаля
27	Функции с закрытыми дверями
28	Протокол Диффи-Хеллмана
29	Цифровая подпись RSA
30	Цифровая подпись Эль-Гамаля
31	Стандарт цифровой подписи в России
32	Хеш-функции в цифровой подписи
33	Цель цифровой подписи
34	Протоколы цифровых денег
35	Протоколы идентификации с нулевым разглашением
36	Защищенные распределенные (облачные) вычисления

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
1	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
2	Задание 2. Нахождение мультипликативных обратных с помощью алгоритма Евклида (50 вариантов) Пример задания: Вариант 1. Вычислить: $8011^{-1} \bmod 16732$
3	Задание 3. Быстрое возведение в степень (50 вариантов) Пример задания: Вариант 1. Вычислить: $19^{220} \bmod 73$
4	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.
5	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 программы 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. 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 прохождению лабораторных работ

В ходе выполнения лабораторных работа обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом и относится к средствам, обеспечивающим решение следующих основных задач у обучающегося:

– приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;

– закрепление, развитие и детализация теоретических знаний, полученных на лекциях;

– получение новой информации по изучаемой дисциплине;

– приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ

Вариант задания по каждой лабораторной работе обучающийся получает в соответствии с номером в списке группы. Перед проведением лабораторной работы обучающемуся следует внимательно ознакомиться с методическими указаниями по ее выполнению, а также с содержанием соответствующего лекционного курса, при необходимости – изучить самостоятельно дополнительную литературу. В соответствии с заданием обучающийся должен подготовить необходимые данные, выполнить задание лабораторной работы, получить требуемые результаты, оформить и защитить отчет по лабораторной работе

Структура и форма отчета о лабораторной работе

Отчет о лабораторной работе должен включать в себя: титульный лист, формулировку задания, теоретические положения, используемые при выполнении лабораторной работы, описание процесса выполнения лабораторной работы, полученные результаты и выводы.

Требования к оформлению отчета о лабораторной работе

По каждой лабораторной работе выполняется отдельный отчет. Титульный лист оформляется в соответствии с шаблоном (образцом) приведенным на сайте ГУАП (www.guap.ru) в разделе «Сектор нормативной документации». Текстовые и графические материалы оформляются в соответствии с действующими ГОСТами и требованиями, приведенными на сайте ГУАП (www.guap.ru) в разделе «Сектор нормативной документации».

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.

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.

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