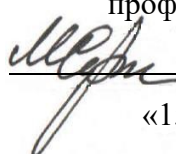


МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ  
Федеральное государственное автономное образовательное учреждение высшего  
профессионального образования  
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

---

Кафедра №51

«УТВЕРЖДАЮ»  
Руководитель направления  
проф., д.т.н., проф.  
 М.Б. Сергеев  
«15» мая 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита информации»

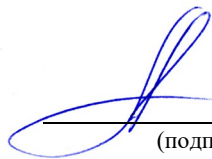
Код направления	09.03.01
Наименование направления	Информатика и вычислительная техника
Наименование направленности	Вычислительные машины, комплексы, системы и сети
Форма обучения	заочная

Санкт-Петербург 2019 г.

## Лист согласования рабочей программы дисциплины

Программу составил (а)

к.т.н., доц.  
(должность, уч. степень, звание)

15.05.2019

(подпись, дата)

А.А. Овчинников

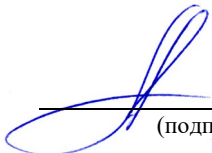
(инициалы, фамилия)

Программа одобрена на заседании кафедры № 51

«15» мая 2019 г, протокол № 10

Заведующий кафедрой № 51

к.т.н., доц.  
(уч. степень, звание)

15.05.2019

(подпись, дата)

А.А. Овчинников

(инициалы, фамилия)

Ответственный за ОП ВО 09.03.01(02)

доц., к.т.н., доц.  
(должность, уч. степень, звание)

15.05.2019

(подпись, дата)

Н.В. Соловьев

(инициалы, фамилия)

Заместитель директора института №4 по методической работе

доц., к.т.н., доц.  
(должность, уч. степень, звание)

15.05.2019

(подпись, дата)

А.А. Ключарев

(инициалы, фамилия)

## Аннотация

Дисциплина «Защита информации» входит в базовую часть образовательной программы подготовки студентов по направлению «09.03.01 «Информатика и вычислительная техника» направленность «Вычислительные машины, комплексы, системы и сети». Дисциплина реализуется кафедрой №51

Дисциплина нацелена на формирование у выпускника общепрофессиональных компетенций:

ОПК-1 «Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности»

ОПК-2 «Способен использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности»

ОПК-3 «Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности»

ОПК-8 «Способен разрабатывать алгоритмы и программы, пригодные для практического применения».

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, лабораторные работы, самостоятельная работа студента.

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

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа.

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. Дисциплина входит в состав обязательной части образовательной программы высшего образования (далее – ОП ВО).

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

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Общепрофессиональные компетенции	ОПК-1 Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	ОПК-1.3.1 знать основы математики, физики, вычислительной техники и программирования ОПК-1.У.1 уметь решать стандартные профессиональные задачи с применением естественнонаучных и обще-инженерных знаний, методов математического анализа и моделирования ОПК-1.В.1 владеть навыками теоретического и экспериментального исследования объектов профессиональной деятельности
Общепрофессиональные компетенции	ОПК-2 Способен использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	ОПК-2.3.1 знать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности ОПК-2.У.1 уметь выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности ОПК-2.В.1 владеть навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности
Общепрофессиональные компетенции	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе	ОПК-3.3.1 знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом

	информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	основных требований информационной безопасности ОПК-3.У.1 уметь 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.В.1 владеть навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
Общепрофессиональные компетенции	ОПК-8 Способен разрабатывать алгоритмы и программы, пригодные для практического применения	ОПК-8.3.1 знать алгоритмические языки программирования, операционные системы и оболочки, современные среды разработки программного обеспечения ОПК-8.У.1 уметь составлять алгоритмы, писать и отлаживать коды на языке программирования, тестировать работоспособность программы, интегрировать программные модули ОПК-8.В.1 владеть языком программирования; навыками отладки и тестирования работоспособности программы

## 2. Место дисциплины в структуре ОП

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

- Информатика;
- Теория информации;
- Введение в направление.

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

- Проектирование АСОИУ.

## 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 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№7
1	2	3
<b>Общая трудоемкость дисциплины,</b> ЗЕ/(час)	4/ 144	4/ 144
<b>Аудиторные занятия,</b> всего час., <b>В том числе</b>	12	12
Лекции (Л), (час)	6	6
Практические/семинарские занятия (ПЗ), (час)		
Лабораторные работы (ЛР), (час)	6	6
Курсовой проект (работа) (КП, КР), (час)		

Экзамен,	(час)	9	9
<i>Самостоятельная работа</i> , всего	(час)	123	123
<b>Вид промежуточной аттестации:</b> зачет, экзамен, дифференцированный зачет ( <b>Зачет. Экз. Дифф. зач</b> )		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 3 – 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	1		-		25
Раздел 2. Симметричные шифры	2		3		25
Раздел 3. Криптография с открытым ключом	2		2		25
Раздел 4. Криптографические протоколы	1		1		25
Текущий контроль					23
Итого в семестре:	6		6		123
Итого:	6	0	6	0	123

##### 4.2. Содержание разделов и тем лекционных занятий

Содержание разделов и тем лекционных занятий приведено в таблице 3.

Таблица 4 - Содержание разделов и тем лекционных занятий

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	<p>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.</p> <p>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.</p>
2	<p>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.</p> <p>Тема 2.2. Блочные шифры  Понятие стойкости, предположения об исходных условиях криптоанализа, совершенная стойкость. Одноразовый блокнот. Шифр Вернама. Принципы построения блочных шифров. Свойства смешивания и рассеивания. Составные шифры, итеративные шифры. SP-сети, сети Файстеля. Современные системы шифрования: алгоритмы DES, ГОСТ 28147-89, AES. Режимы блочного шифрования: ECB, CBC,</p>

	CFB, OFB. Режим счетчика. Многократное шифрование. Тема 2.3. Поточковые шифры Требования к поточным шифрам. Методы построения больших периодов в поточных шифрах. Регистры сдвига с линейной обратной связью (РСЛОС). m-последовательности. Алгоритм Берлекэмпа-Мессис. Построение поточковых 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-Гамала. Система Мак-Элиса. Криптографические хэш-функции. Понятие о цифровой подписи. Подпись RSA. Подпись Эль-Гамала. 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-Хеллмана. 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 5 – 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 6 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	№ раздела дисциплины
Семестр 7			
1	Реализация исторического (подстановочного или перестановочного) шифра	1	2
2	Криптоанализ исторического шифра	1	2
3	Реализация симметричного блочного шифра	1	2
4	Реализация системы с открытым ключом	1	3
5	Реализация ЭЦП	1	3
6	Реализация криптографического протокола	1	4
Всего:		6	

#### 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 7 - Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 3, час
1	2	3
<b>Самостоятельная работа, всего</b>	123	123
Изучение теоретического материала дисциплины (ТО)	70	70
Подготовка лабораторных работ (ЛР)	30	30
Подготовка к текущему контролю (ТК)	23	23

### 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 8 – 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
X404.3 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. <a href="http://znanium.com/catalog.php?bookinfo=523231">http://znanium.com/catalog.php?bookinfo=523231</a>	
	Теоретико-численные методы в криптографии: Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. – 160 с. <a href="http://www.znanium.com/catalog.php?bookinfo=441493">http://www.znanium.com/catalog.php?bookinfo=441493</a>	



## 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
<a href="https://www.pgpru.com/">https://www.pgpru.com/</a>	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	<a href="http://libgost.ru/">http://libgost.ru/</a> 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; Экзаменационные билеты; Задачи; Тесты.

10.2. В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала модульно–рейтинговой системы университета. В таблице 14 представлена 100–балльная и 4–балльная шкалы для оценки сформированности компетенций.

Таблица 14 –Критерии оценки уровня сформированности компетенций

Оценка компетенции
--------------------

100- бальная шкала	4-бальная шкала	Характеристика сформированных компетенций
$85 \leq K \leq 100$	«отлично» «зачтено»	<ul style="list-style-type: none"> <li>- обучающийся глубоко и всесторонне усвоил программный материал;</li> <li>- уверенно, логично, последовательно и грамотно его излагает;</li> <li>- опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления;</li> <li>- умело обосновывает и аргументирует выдвигаемые им идеи;</li> <li>- делает выводы и обобщения;</li> <li>- свободно владеет системой специализированных понятий.</li> </ul>
$70 \leq K \leq 84$	«хорошо» «зачтено»	<ul style="list-style-type: none"> <li>- обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы;</li> <li>- не допускает существенных неточностей;</li> <li>- увязывает усвоенные знания с практической деятельностью направления;</li> <li>- аргументирует научные положения;</li> <li>- делает выводы и обобщения;</li> <li>- владеет системой специализированных понятий.</li> </ul>
$55 \leq K \leq 69$	«удовлетворительно» «зачтено»	<ul style="list-style-type: none"> <li>- обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы;</li> <li>- допускает несущественные ошибки и неточности;</li> <li>- испытывает затруднения в практическом применении знаний направления;</li> <li>- слабо аргументирует научные положения;</li> <li>- затрудняется в формулировании выводов и обобщений;</li> <li>- частично владеет системой специализированных понятий.</li> </ul>
$K \leq 54$	«неудовлетворительно» «не зачтено»	<ul style="list-style-type: none"> <li>- обучающийся не усвоил значительной части программного материала;</li> <li>- допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении;</li> <li>- испытывает трудности в практическом применении знаний;</li> <li>- не может аргументировать научные положения;</li> <li>- не формулирует выводов и обобщений.</li> </ul>

### 10.3. Типовые контрольные задания или иные материалы:

#### 1. Вопросы (задачи) для экзамена (таблица 15).

Таблица 15 – 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 блочные шифры. Сети Файстеля. Примеры.
7	Шифр DES.
8	Шифр FEAL
9	Шифр ГОСТ 28147-89.
10	Шифр AES
11	Режимы блочного 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

2. Вопросы (задачи) для зачета / дифференцированного зачета (таблица 16).

Таблица 16 – 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 17).

Таблица 17 – 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 блочного шифра перебором по ключу
20	Количество раундов шифров-стандартов
21	Множественное 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:  $-17 \bmod 44$ $-31 \bmod 17$ $-49 \bmod 16$ $-76 \bmod 11$ $23 \bmod 50$
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: $19^{20} \bmod 73$
4	Задание 4. Системы с открытым ключом: системы RSA, Мак-Элиса, Эль-Гамала (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-Гамала (индивидуальные варианты)
	Пример задания: Построить открытый и секретный ключи, подписать и проверить подпись сообщения с помощью системы Эль-Гамала. Сообщение $M$ определяется индивидуальным номером студента, размер открытого модуля $p > 19$ , остальные параметры ЭЦП выбрать самостоятельно.

10.4. 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.

#### 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;
- научиться методически обрабатывать материал (выделять главные мысли и положения, приходиться 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 Блочные шифры

Тема 2.3 Поточковые 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 работ 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](http://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](http://www.guap.ru)) в разделе «Сектор нормативной документации».

#### Методические указания по прохождению лабораторных работ:

1. [004.056(075) Т 33] Беззатеев С. В. Теория информационной безопасности и методология защиты информации: методические указания к выполнению лабораторных работ № 1. - СПб.: ГОУ ВПО "СПбГУАП", 2007. Кол-во экз. в библ. - 88.
2. [519.7 М 34] И. Л. Ерош, М. Ю. Литвинов, Н. В. Соловьев. Математические основы защиты информации: методические указания к выполнению лабораторных работ. СПб.: ГОУ ВПО "СПбГУАП", 2008. - 31 с.. Кол-во экз. в библ. – 74.

### **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