

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

проф., д.т.н., доц.

(должность, уч. степень, звание)

С.В. Мичурин

(инициалы, фамилия)



(подпись)

«19» мая 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита информации»
(Наименование дисциплины)

Код направления подготовки/ специальности	09.03.02
Наименование направления подготовки/ специальности	Информационные системы и технологии
Наименование направленности	Информационные системы и технологии в бизнесе
Форма обучения	заочная

Санкт-Петербург – 2021

Лист согласования рабочей программы дисциплины

Программу составил (а)

зав.каф., к.т.н., доц.

(должность, уч. степень, звание)



19.05.2021

(подпись, дата)

А.А. Овчинников

(инициалы, фамилия)

Программа одобрена на заседании кафедры № 51

«19» мая 2021 г, протокол №10

Заведующий кафедрой № 51

к.т.н., доц.

(уч. степень, звание)



19.05.2021

(подпись, дата)

А.А. Овчинников

(инициалы, фамилия)

Ответственный за ОП ВО 09.03.02(03)

доц., к.т.н., доц.

(должность, уч. степень, звание)



19.05.2021

(подпись, дата)

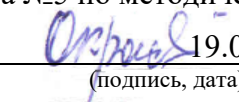
О.И. Красильникова

(инициалы, фамилия)

Заместитель директора института №5 по методической работе

доц., к.т.н., доц.

(должность, уч. степень, звание)



19.05.2021

(подпись, дата)

О.И. Красильникова

(инициалы, фамилия)

Аннотация

Дисциплина «Защита информации» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 09.03.02 «Информационные системы и технологии » направленности «Информационные системы и технологии в бизнесе». Дисциплина реализуется кафедрой «№51».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-2 «Способен выполнять работы по обслуживанию программно-аппаратными средствами сетей и инфокоммуникаций»

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 обучающегося.

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 части, формируемой участниками образовательных отношений, 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
Профессиональные компетенции	ПК-2 Способен выполнять работы по обслуживанию программно-аппаратными средствами сетей и инфокоммуникаций	<p>ПК-2.3.1 знать общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемых сетевых устройств информационно-коммуникационных систем; архитектуру аппаратных, программных и программно-аппаратных средств администрируемых сетевых устройств информационно-коммуникационных систем; базовую эталонную модель взаимодействия открытых систем для управления сетевым трафиком; протоколы канального, сетевого, транспортного и прикладного уровней; модели взаимодействия открытых систем; инструкции по эксплуатации администрируемых сетевых устройств; типовые ошибки, возникающие при работе инфокоммуникационной системы, признаки их проявления при работе и методы устранения; методы и средства восстановления работоспособности программно-аппаратных средств инфокоммуникационной системы и/или ее составляющих после сбоев</p> <p>ПК-2.У.1 уметь анализировать сообщения об ошибках в сетевых устройствах и операционных системах; выявлять и устранять последствия сбоев и отказов сетевых устройств и операционных систем; производить мониторинг администрируемых</p>

		сетевых устройств информационно-коммуникационных систем; документировать изменения в конфигурации администрируемого программного обеспечения сетевых устройств информационно-коммуникационных систем; документировать причины сбоев и результаты восстановления работоспособности программно-аппаратных средств информационно-коммуникационной системы и/или ее составляющих; пользоваться нормативно-технической документацией в области инфокоммуникационных технологий; осуществлять резервное копирование программного обеспечения сетевых устройств ПК-2.В.1 владеть навыками использования современных методов контроля производительности сетевых устройств информационно-коммуникационных систем; обновления программного обеспечения сетевых устройств; настройки сетевого программного обеспечения; обнаружения отклонений от штатного режима работы инфокоммуникационной системы и/или ее составляющих; использования команд и утилит операционной системы для мониторинга ее состояния и трафика; выявления причин возникновения аварийных ситуаций при использовании программно-аппаратных средств инфокоммуникационной системы и/или ее составляющих
--	--	--

2. Место дисциплины в структуре ОП

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

- «Информатика»,
- «Дискретная математика»,
- «Инфокоммуникационные системы и сети».

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

- «Администрирование информационных систем»,
- «Надежность информационных систем».
-

3. Объем и трудоемкость дисциплины

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№7

1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	4/ 144	4/ 144
Из них часов практической подготовки	8	8
Аудиторные занятия, всего час.	16	16
в том числе:		
лекции (Л), (час)	8	8
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	8	8
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)	9	9
Самостоятельная работа, всего (час)	119	119
Вид промежуточной аттестации: зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Экз.	Экз.

Примечание: ** кандидатский экзамен

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий.

Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, 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	1				19
Раздел 2. Симметричные шифры Тема 2.1 Исторические шифры Тема 2.2 Блочные шифры Тема 2.3 Поточковые шифры	2		4		36
Раздел 3. Криптография с открытым ключом Тема 3.1 Математические основы систем с открытым ключом Тема 3.2 Основные алгоритмы с открытым ключом	3		2		36
Раздел 4. Криптографические протоколы Тема 4.1 Основные протоколы с открытым ключом Тема 4.2 Специальные протоколы	2		2		28
Итого в семестре:	8		8		119
Итого	8	0	8	0	119

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

Номер раздела	Название и содержание разделов и тем лекционных занятий
---------------	---

1	<p>Раздел 1. Основные понятия криптографии.</p> <p>Тема 1.1 — Основные определения</p> <p>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.</p> <p>Криптографическая защита информации. Представление информации в цифровом виде.</p> <p>Тема 1.2 — Задачи информационной безопасности</p> <p>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>Раздел 2. Симметричные шифры</p> <p>Тема 2.1 — Исторические шифры</p> <p>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</p> <p>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, CFB, OFB. Режим счетчика. Многократное шифрование.</p> <p>Тема 2.3 — Поточковые шифры</p> <p>Требования к поточным шифрам. Методы построения больших периодов в поточных шифрах. Регистры сдвига с линейной обратной связью (РСЛОС). m-последовательности. Алгоритм Берлекэмп-Мессе. Построение поточковых шифров на основе РСЛОС. Нелинейное комбинирование РСЛОС: генератор Геффе, шифры с контролем тактов. Применение поточного шифрования.</p>
3	<p>Раздел 3. Криптография с открытым ключом</p> <p>Тема 3.1 — Математические основы систем с открытым ключом</p> <p>Модульная арифметика. Алгоритм Евклида и его сложность. Расширенный алгоритм Евклида. Основные теоремы о</p>

	<p>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.</p>
4	<p>Раздел 4. Криптографические протоколы 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.</p>

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено					
Всего					

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 7				
1	Реализация исторического (подстановочного или перестановочного) шифра	2	2	2
2	Реализация симметричного блочного	2	2	2

	шифра			
3	Реализация систем с открытым ключом	2	2	3
4	Реализация криптографического протокола	2	2	4
Всего		8	8	

4.5. Курсовое проектирование/ выполнение курсовой работы
Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся
Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 7, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	47	47
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	36	36
Домашнее задание (ДЗ)	36	36
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)		
Всего:	119	119

5. Перечень учебно-методического обеспечения
для самостоятельной работы обучающихся по дисциплине (модулю)
Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 7-11.

6. Перечень печатных и электронных учебных изданий
Перечень печатных и электронных учебных изданий приведен в таблице 8.
Таблица 8– Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
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
http://znanium.com/catalog.php?bookinfo=523231	Компьютерная математика: Учебное пособие /К.В.Титов - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 261 с.	
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.-Петербург. гос. ун-т аэрокосм. приборостроения. - СПб.: Изд-во ГУАП, 2014. - 178 с.	40
004.056(075) Б70	Блочные шифры: Учебное пособие/ С. В. Беззатеев, Е. А. Крук, А.А. Овчинников, В. Б. Прохорова; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - СПб.: РИО ГУАП, 2003. - 63 с.	49
http://znanium.com/catalog.php?bookinfo=615250	Руководство к решению задач по дискретной математике / Шубович А.А. - Волгоград: Волгоградский ГАУ, 2015. - 88 с.	

7. Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

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

8. Перечень информационных технологий

8.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
1	MS Windows
2	MS Office
3	Инструментальная среда программирования

8.2. Перечень информационно-справочных систем,используемых при осуществлении образовательного процесса по дисциплине

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

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Фонд аудиторий ГУАП для проведения занятий лекционного и семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	
2	Вычислительная лаборатория	

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Экзамен	Список вопросов к экзамену; Экзаменационные билеты; Задачи; Тесты.

10.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 14. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 14 –Критерии оценки уровня сформированности компетенций

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
«отлично» «зачтено»	<ul style="list-style-type: none"> – 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.

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«хорошо» «зачтено»	<ul style="list-style-type: none"> – 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.
«удовлетворительно» «зачтено»	<ul style="list-style-type: none"> – 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.
«неудовлетворительно» «не зачтено»	<ul style="list-style-type: none"> – 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.

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
1	Задача обеспечения секретности.	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1
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-Гамала	
16	Задача обеспечения аутентификации. Цифровая подпись.	
17	Подпись RSA.	
18	Подпись Эль-Гамала.	
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	
----	--	--

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.
Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
	Учебным планом не предусмотрено	

Перечень тем для курсового проектирования/выполнения курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для курсового проектирования/выполнения курсовой работы

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

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
1	Задание 1. Основы модульной арифметики (50 вариантов) Пример задания: Вариант 1. Вычислить: $-17 \bmod 44$ $-31 \bmod 17$ $-49 \bmod 16$ $-76 \bmod 11$ $23 \bmod 50$	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1
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-Гамала (индивидуальные варианты) Пример задания: Построить открытый и секретный ключи, зашифровать и расшифровать сообщение с помощью системы Мак-Элиса, для сообщения $m = 100101$.	
5	Параметр M определяется индивидуальным номером студента, остальные параметры системы выбрать самостоятельно. 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 М определяется индивидуальным номером студента, размер открытого модуля $p > 19$, остальные параметры ЭЦП выбрать самостоятельно.	
--	--	--

Перечень тем контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
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: $19^{220} \bmod 73$
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 М 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 М определяется индивидуальным номером студента, размер открытого модуля $p > 19$, остальные параметры ЭЦП выбрать самостоятельно.

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

11. Методические указания для обучающихся по освоению дисциплины

11.1. 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 обучающимися 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, 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 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

11.2. Методические указания для обучающихся по выполнению 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 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».

11.3. 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-методические материалы 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.

11.4. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины. Форма проведения текущего контроля – защита отчетов по лабораторным работам. Результаты текущего контроля учитываются при проведении промежуточной аттестации в соответствии с требованиями СТО ГУАП. СМК 3.76 «Положение о текущем контроле успеваемости и промежуточной аттестации студентов и аспирантов ГУАП, обучающихся по образовательным программам высшего образования».

11.5. 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 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