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

Кафедра № 14

УТВЕРЖДАЮ
Руководитель направления

д.т.н.,проф.
(должность, уч. степень, звание)

М.Б. Сергеев
(инициалы, фамилия)

(подпись)
«25» мая 2022г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Безопасность и защита информации в информационных системах (на английском языке)»
(Наименование дисциплины)

Код направления подготовки/ специальности	09.04.01
Наименование направления подготовки/ специальности	Информатика и вычислительная техника
Наименование направленности	Встроенные системы обработки информации и управления (Embedded Systems)
Форма обучения	очная

Санкт-Петербург– 2022

Лист согласования рабочей программы дисциплины

Программу составил (а)

проф., к.т.н.,доц.		Н.А. Шехунова
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Программа одобрена на заседании кафедры № 14
«25» мая 2022г, протокол №11

Заведующий кафедрой № 14

к.т.н.,доц.		В.Л. Оленев
(уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Ответственный за ОП ВО 09.04.01(32)

к.т.н.,доц.		В.Л. Оленев
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Заместитель директора института №1 по методической работе

ст.преп.		В.Е. Таратун
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Аннотация

Дисциплина «Безопасность и защита информации в информационных системах (на английском языке)» входит в образовательную программу высшего образования – программу магистратуры по направлению подготовки/ специальности 09.04.01 «Информатика и вычислительная техника» направленности «Встроенные системы обработки информации и управления (Embedded Systems)». Дисциплина реализуется кафедрой «№14».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ОПК-5 «Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем»

ОПК-6 «Способен разрабатывать компоненты программно-аппаратных комплексов обработки информации и автоматизированного проектирования»

ОПК-7 «Способен адаптировать зарубежные комплексы обработки информации и автоматизированного проектирования к нуждам отечественных предприятий»

Содержание дисциплины охватывает круг вопросов, связанных с областью проблем защиты информации и информационной безопасности.

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

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

Общая трудоемкость освоения дисциплины составляет 6 зачетных единиц, 216 часов.

Язык обучения по дисциплине «английский»

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Целью преподавания дисциплины является получение теоретических и практических знаний для формирования навыков в области разработки и сопровождения средств защиты информации. Теоретическая часть включает изучение основ информационной безопасности автоматизированных систем обработки информации и управления (АСОИУ). Практическая часть предполагает освоение основных принципов информационных и коммуникационных технологий информационной безопасности АСОИУ.

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-5 Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем	ОПК-5.З.1 знать современное программное и аппаратное обеспечение информационных и автоматизированных систем ОПК-5.У.1 уметь модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач ОПК-5.В.1 владеть навыками разработки программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач
Общепрофессиональные компетенции	ОПК-6 Способен разрабатывать компоненты программно-аппаратных комплексов обработки информации и автоматизированного проектирования	ОПК-6.З.1 знать аппаратные средства и платформы инфраструктуры информационных технологий, виды, назначение, архитектуру, методы разработки и администрирования программно-аппаратных комплексов объекта профессиональной деятельности ОПК-6.У.1 уметь анализировать техническое задание, разрабатывать и оптимизировать программный код для решения задач обработки информации и автоматизированного проектирования ОПК-6.В.1 владеть навыками составления технической документации по использованию и настройке компонентов программно-аппаратного комплекса

Общепрофессиональные компетенции	ОПК-7 Способен адаптировать зарубежные комплексы обработки информации и автоматизированного проектирования к нуждам отечественных предприятий	ОПК-7.З.1 знать функциональные требования к прикладному программному обеспечению для решения актуальных задач предприятий отрасли, национальные стандарты обработки информации и автоматизированного проектирования ОПК-7.У.1 уметь приводить зарубежные комплексы обработки информации в соответствие с национальными стандартами, интегрировать с отраслевыми информационными системами ОПК-7.В.1 владеть навыками настройки интерфейса, разработки пользовательских шаблонов, подключения библиотек, добавления новых функций

2. Место дисциплины в структуре ОП

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

– «Информатика»

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и могут использоваться при выполнении выпускной квалификационной работы

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
		№3
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	6/ 216	6/ 216
Из них часов практической подготовки		
Аудиторные занятия, всего час.	34	34
в том числе:		
лекции (Л), (час)	17	17
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	17	17
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)	54	54
Самостоятельная работа, всего (час)	128	128
***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 2					
Раздел 1.	3		2		30
Раздел 2.	3		8		30
Раздел 3.	3		7		30
Раздел 4.	4				30
Раздел 5.	4				8
Итого в семестре:	17		17		128
Итого	17	0	17	0	128

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	Раздел 1. Введение. Тема 1.1.Цели, задачи и актуальные вопросы защиты информации в АСОИУ и компьютерных сетях. Тема 1.2. Задачи анализа и классификации угроз.
2	Раздел 2. Защита от НСД. Тема 2.1.Система управления доступом. Тема 2.2. Математические модели систем управления доступом. Тема 2.3. Идентификация и аутентификация. Тема 2.4. Скрытые каналы НСД.
3	Раздел 3. Криптографические методы защиты информации; Тема 3.1Основные понятия криптологии. Классификация шифров.. Тема 3.2.Симметричные шифры. Тема 3.3. Системы с открытыми ключами. Системы ЭЦП.
4	Раздел 4. Защита информации в глобальных сетях. Тема 4.1.Защита от удаленных атак
5	Раздел 5.Заключение. Тема 5.1.Тенденции развития методов и средств защиты информации. Актуальные задачи для исследования.

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)	№ раздела дисцип

				лины
Учебным планом не предусмотрено				

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)	№ раздела дисциплины
Семестр 2			
1	Методы и алгоритмы симметричного шифрования. Базовые симметричные шифры. Криптографические стандарты.	3	3
2	Исследование систем с открытыми ключами : система РСА (RSA), система ЭльГамаля (El Gamale)	3	3
3	Исследование систем ЭЦП, ГОСТ Р34.10-2001	3	3
4	Исследование основных типов криптоатак на информацию, хранимую в памяти и методов противодействия им.	4	1
5	Исследование эффективности помехоустойчивости кодов для защиты информации в памяти встроенных систем обработки информации и управления	4	2
Всего		17	

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 2, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	60	60
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	60	60
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	8	8
Всего:	128	128

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 Ш 22	Шаньгин В.Ф. Информационная безопасность: научно-популярная литература / В. Ф. Шаньгин. - М. : ДМК Пресс, 2014. - 702 с.	8
004.9(075) С59	Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. Учебное пособие. СПб:БХВ-Петербург, 2010 304 с.	4
004.7(075) И 74 004	Информационная безопасность открытых систем: учебник: в 2 т./ С. В. Запечников [и др.]. - М.: Горячая линия - Телеком. – 2008 Т. 2: Средства защиты в сетях. - М., 2008. - 558 с.	25
004 Р 69	Романьков В.А. Введение в криптографию: курс лекций / В. А. Романьков. - 2-е изд., испр. и доп. - М. : ФОРУМ, 2012. - 240 с	10
004 Р 98	Рябко Б.Я. Криптографические методы защиты информации : учебное пособие / Б. Я. Рябко, А. Н. Фионов. - 2-е изд., стер. - М. : Горячая линия - Телеком, 2014. - 229 с.	10
	Ожиганов А.А. Криптография: учебное пособие. СПб: Университет ИТМО, 2016. – 140с.	
004 Ш76	Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си: монография / Б. Шнайер; Ред. П. В. Семьянов. - М. : Триумф, 2003. - 815 с	14
	Тарасюк М.В., Шехунова Н.А. Защищенное программное обеспечение. Учебное пособие СПб. ИТМО. 2012	На каф. 14 ГУАП (18)
004 М 36	Маховенко Е.Б. Теоретико-числовые методы в криптографии. Учебное пособие. М.:Гелиос-АРВ.2006. систем.	2
004.4 Ш 22	Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства: учебное пособие/ В. Ф. Шаньгин. - М.: ДМК Пресс, 2008. - 544 с.	1
004(075) О-75	Основы криптографии : учебное пособие / А. П. Алферов [и др.]. - 3-е изд. испр. и доп. - М. : Гелиос АРВ, 2005. - 480 с	8
004 З-62	Зима В.М. Безопасность глобальных сетевых технологий / В. М. Зима, А. А. Молдовян, Н. А. Молдовян. - 2-е изд. - СПб. : БХВ - Петербург, 2003. - 368 с.	3

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
http://dokipedia.ru/document/5182727	Руководящий документ Гостехкомиссии РФ. Автоматизированные системы. Защита информации от НСД. Классификация автоматизированных систем и требования по защите информации
www.cacr.math.uwaterloo.ca/hac,	Математические основы криптографии
www.ma.iup.edu/MAA/proceedings/vol	Международный образовательный ресурс по защите информации
http://books.ifmo.ru/file/pdf/1989.pdf	Криптография. Учебное пособие

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
	Не предусмотрено

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
	Не предусмотрено

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	Лекционная аудитория	
2	Компьютерный класс	

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средствдля 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

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 5-балльная шкала	Характеристика сформированных компетенций
«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.
«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.
«удовлетворительно» «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.
«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.

10.3. 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

	Классификация методов и средств защиты информации
	Функциональная схема архитектуры защищенной АСОИУ
	Цели, задачи и актуальные вопросы защиты информации в АСОИУ и компьютерных сетях.
	Задачи анализа и классификации информационных угроз
	Классификация угроз информации. Модели угроз
	Криптология: определение, основные понятия, классификация основных задач
	Криптографические методы защиты информации
	Классификация шифров. Теорема о совершенной секретности
	Теория информации, как математическая база для анализа симметричных криптографических систем
	Теория сложности, как математическая основа современной криптографии
	Формальное описание криптографических систем. Классификация. Требования.
	Системы электронной цифровой подписи: определение, реализация
	Симметричные шифры.
	Блоковые шифры. Вычислительно секретные шифры. Основные методы криптоанализа блоковых шифров
	Поточные шифры. Криптоанализ поточных шифров
	Системы с открытыми ключами. Математические задачи, лежащие в основе построения систем с открытыми ключами
	Коды, обнаруживающие подлог
	Хэш- функции в криптографии: требования, методы реализации, области использования.
	Стандарты ЭЦП.
	Управление ключами. Протоколы распределения ключей
	Математические модели управления доступом.
	Методы реализации матрицы доступа
	Модели нарушителя замкнутой и открытой программной среды
	Модель скрытого канала. Ликвидация скрытого канала
	Методы защиты от удаленных атак из Internet
	Межсетевые экраны: классификация, функции, уровни ЭМВОС, на которых устанавливают МЭ.
	Функциональные возможности нарушителя доверенной программной среды
	Требования к межсетевым экранам второго класса РД МЭ
	Обеспечение целостности открытой программной среды
	Безопасность облачных технологий
	Функциональная архитектура безопасности системы
	Технологическая архитектура безопасности системы
	Системная архитектура безопасности системы
	Требования к системам класса С1 и С2
	Требования к системам класса С2 и В1
	Требования к системам класса В1 и В2
	Общие требования к системам класса В2 и В3
	Требования к системам В3 и А1
	Основные характеристики дискреционного управления
	Основные характеристики мандатного управления
	Основные характеристики транзитивного управления доступом
	Модель нарушителя замкнутой программной среды
	Модель нарушителя открытой программной среды
	Модель нарушителя доверенной программной среды

	Цели механизмов и функций идентификации
	Цели механизмов и функций аутентификации
	Назначение систем обнаружения компьютерных угроз
	Задачи обеспечения целостности данных
	Методы обеспечения целостности данных
	Область применения компьютерных угроз
	Общие требования к Межсетевым экранам 3 и 2-го уровня
	Средства и технологии криптографической защиты на сетевом уровне ЭМВОС
	Средства и технологии дискреционного управления доступом к защищаемым ресурсам
	Средства и технологии реализации ролевого управления
	Стеганографические каналы скрытого обмена данными
	Правила обработки входящих пакетов на сетевом интерфейсе
	Минимальные требования по ЗИ при обработке конфиденциальной информации
	Минимальные требования по ЗИ при обработке секретной информации
	Минимальные требования к АСОИУ по классу 1В
	Вычислить функцию Эйлера от чисел **567 и 1280.** Вывести формулу **f(p**a) = [p**(a – 1)] (p – 1)**, где **f –** функция Эйлера**.** **С**троится последовательность целых чисел a2 = [a0 –a1] , a3 = [a1 –a2], a4 = [a2 – a3] ,… Докажите, что, начиная с некоторого места, эта последовательность имеет вид d,d,0,d,d,0,..., где d = НОД(a0,a1)
	С помощью теоремы о свертке вычислите произведение по модулю **7** двух полиномов: 3x**7 + 4x**5 + x**2 + 1, x**7 + 5x**6 + 6xs + 1
	Найти значение числа **20000001** по модулям **5,7,11,13,17,19,23** алгоритмом вычисления вычетов.
	Найти все представления числа n в виде суммы квадратов двух целых чисел, **n = 35,41, 221**. Установить связь полученных результатов с числом точек плоской квадратной 1 единичной решетки, лежащих на окружности радиуса sqrt(n).
	Решить задачу об укладке рюкзака рюкзак **{17,24,11,12,3,21,15,18,1,5}, C =100.**
	Сравните избыточность программ, написанных на PASCAL, VC,VB. Delphi Укажите пути сокращения избыточности.
	Приведите решение уравнения **13x mod 70 = 1**
	Найти Укажите корни уравнения $\mathbf{1 + x^2 + x^4 + x^6 + x^8 + x^{10} = 0}$ **в GF(31)**.
	Для к Для каких простых **p** числа –**3, 6, 21** будут квадратичными вычетами?
	Указать метод распараллеливания вычислений при умножении больших чисел.
	Пусть X’ означает битовое представление блока X. Показать, что ,если C = DES (M), тогда C’ = DES (M’). Объясните, как это свойство может быть использовано для атаки по выбранному тексту для сокращения усилий криптоаналитика на 50%.
	Показать, что над $\mathbf{GF(2^m)}$, уравнение $\mathbf{x^2 + a = 0}$, всегда имеет единственный корень.
	Показ Показать, что элементы кольца дискретного нормирования,

	обладающие нормой **k > 1**, о образуют идеал.
	Показать, что **sqrt (2) + sqrt (5)** - целое алгебраическое число.
	Предл Предложить модификацию бинарного алгоритма Евклида для вычисления **НОД** многочленов из **R[x] над GF(p)**.
	Указать все представления числа n в виде суммы квадратов двух целых **чисел n = 35,**
	Предл Предложить алгоритм извлечения кубического корня в **GF(3)**. Установить связь получ полученных результатов с числом точек плоской квадратной единичной решетки, лежа на окружности радиуса sqrt (n).
	Постройте систему разделения секрета без помощи Трента.
	Организуйте скрытый канал в ЭЦП на базе алгоритма Эль-Гамаля
	Как ликвидировать скрытый канал в DSA?
	Постройте систему разделения секретов без раскрытия долей.
	Предложить эффективную атаку на хэш-функцию $\mathbf{h^i = ((g^{h(i-1)})^{Mi} \bmod p) \bmod q}$
	Нарушитель, получив подписьS1 к подготовленному им значению хэш-функции **h1**, сформировал «несанкционированную» подпись **S** к значению хэш-функции **h.** Каким образом он это сделал, если уравнение проверки подписи**;** $\mathbf{g = S^h \bmod n,}$ где **(n,g)** – открытый ключ. $\mathbf{n = p*q}$.
	Предложить схему слепой подписи с уравнением проверки $\mathbf{S^3 = h \bmod n.}$ **h = h (M)**, где $\mathbf{n = p*q}$
	Найти произвольную тройку чисел **M,a,b,** таких что **(a,b)** является правильной подписью к сообщению **M** для системы ЦП со следующим уравнением проверки подписи; $\mathbf{g^M*f(a) = (y^b)*a^b \bmod p,}$ где $\mathbf{a = g^k.}$
	Укажите способ подделки подписи в системе ЦП с уравнением проверки подписи $\mathbf{g^M*b = y^a*a^b \pmod p}$.
	Двуключевая криптосистема Рабина шифрует сообщение **M** как **C = M(M + b) mod n** **b и n** – параметры открытого ключа, **p и q (pq = n)** – параметры закрытого ключа. Указать алгоритм дешифрования для случая, когда ***(p + 1) и (q + 1) делятся на 4*** ***(Вычисляйте d так, что 2d mod n =b, тогда (M +d)**2 mod n = (C + d**2) mod n)***
	Пусть открытый ключ в системе Меркле-Хеллмана задан вектором ***A =(17,34,2,21,41)***,шифрограмма ***C = 72.*** Параметры секретного ключа ***и =50, , w =17.*** Найти зашифрованное сообщение ***M***.
	Составить уравнение подписи в схеме ЦП с уравнением проверки подписи $\mathbf{(b + h)^h = g \bmod n,}$ **где n = p*q**. Обосновать переход от исходного уравнения проверки подписи $\mathbf{s^h = g \bmod n}$ к указанному выше.
	Пусть n = pq, где **p,q** – простые. Дано **a, 0<a<n**, пусть **x и y** – квадратные корни из **a** по **mod n** , такие, что **y /= x и y /= n - x.** Показать, что **НОД (x + y, n) + p** или **q**

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
	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

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

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

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.

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 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

- каждая ЛР выполняется по индивидуальному заданию, выданному студенту преподавателем;
- в задании должно быть четко сформулирована задача, выполняемая в ЛР;
- описаны входные и выходные данные для проведения ЛР;
- ЛР должна выполняться на основе полученных теоретических знаний;
- выполнение ЛР должно осуществляться на основе методических указаний, предоставляемых преподавателем;
- ЛР должна выполняться в специализированном компьютерном классе и может быть доработана студентом в домашних условиях, если позволяет ПО;
- итогом выполнения ЛР является отчет или демонстрация результатов работы преподавателю в электронном виде (на усмотрение преподавателя).

Структура и форма отчета о лабораторной работе

- постановка задачи;
- особенности решения и используемые методы (если они потребовались);
- программа на языке программирования с комментариями;
- список литературы.

Требования к оформлению отчета о лабораторной работе:

- ЛР представляется в печатном и электронном виде;
- ЛР должна соответствовать структуре и форме отчета, представленной выше;
- ЛР должна иметь титульный лист (ГОСТ 7,32-2001 издания 2008 года) с названием и подписью студента, который ее сделал и оформил;

Студент должен защитить ЛР. Отметка о защите должна находиться на титульном листе вместе с подписью преподавателя.

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 обучающихсяявляются:

– учебно-методический материал по дисциплине;

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

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.

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 – 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».

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