МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ивангородский гуманитарно-технический институт (филиал)
федерального государственного автономного образовательного учреждения высшего образования
"Санкт-Петербургский государственный университет аэрокосмического приборостроения"

Кафедра прикладной математики, информатики и информационных таможенных технологий
(Кафедра 2)

УТВЕРЖДАЮ
Руководитель направления
д.т.н., проф.
(должность, уч. степень, звание)
М.Б. Сергеев
(инициалы, фамилия)
(подпись)
" 24 " 03 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

"Защита информации"

(Наименование дисциплины)

Код направления подготовки/специальности	09.03.01
Наименование направления подготовки/ специальности	Информатика и вычислительная техника
Наименование направленности	Программное обеспечение средств вычислительной техники и автоматизированных систем
Форма обучения	заочная

Ивангород - 2022

Лист согласования рабочей программы дисциплины

Программу составил(а)

доц., к.т.н.	24.03.2022	А.В. Дагаев
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Программа одобрена на заседании Кафедры 2

" 24 " 03 2022 г., протокол № 9

Заведующий Кафедрой 2

к.ф.-м.н., доцент	24.03.2022	Е.А. Яковлева
(уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Ответственный за ОП ВО 09.03.01(05)

зав.каф., к.ф.-м.н., доц.	24.03.2022	Е.А. Яковлева
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Заместитель Директора ИФ ГУАП по методической работе

	24.03.2022	Н.В. Жданова
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Аннотация

Дисциплина "Защита информации" входит в образовательную программу высшего образования по направлению подготовки/ специальности 09.03.01 "Информатика и вычислительная техника" направленности "Программное обеспечение средств вычислительной техники и автоматизированных систем". Дисциплина реализуется Кафедрой прикладной математики, информатики и информационных таможенных технологий (Кафедрой 2).

Дисциплина нацелена на формирование у выпускника следующих компетенций:

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

ОПК-2 "Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их 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 сущностью и значением информации в развитии современного информационного общества, опасностями и угрозами, возникающими в этом процессе, соблюдением требований информационной безопасности.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа обучающегося, консультации.

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

Цели дисциплины: - Формирование у студентов представления о сущности и значении информации в развитии современного информационного общества; - Знакомство студентов с опасностями и угрозами информации; - Ознакомление с требованиями информационной безопасности; - Обучение методам защиты информации; - Освоение методов шифрования информации; - Изучение алгоритмов генерации псевдослучайных чисел; - Воспитание у студентов необходимого уровня культуры разработки программных продуктов, отвечающим требованиям по защите хранимой, передаваемой и обрабатываемой информации.

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.З.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 понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	ОПК-2.З.1. Знать современные информационные технологии и программные средства, в том числе отечественного производства ОПК-2.У.1. Уметь выбирать современные информационные технологии и программные средства, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности ОПК-2.В.1. Владеть навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, и применять их при решении задач профессиональной деятельности

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Общепрофессиональные компетенции	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-3.З.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 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.З.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 может базироваться на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- Математика. Теория вероятностей и математическая статистика
- Основы программирования

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и могут оказать влияние на практики, государственную итоговую аттестацию и выполнение 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
		7
Общая трудоемкость дисциплины, ЗЕ/час.	4/144	4/144
из них часов практической подготовки	0	0
Аудиторные занятия, всего час.	12	12
в том числе:		
- лекции (Л), час.	6	6
- практические/семинарские занятия (ПЗ, СЗ), час.		
- лабораторные работы (ЛР), час.	6	6
- курсовой проект/работа (КП, КР), час.		
Экзамен, час.	9	9
Самостоятельная работа (СРС), всего час.	123	123
Вид промежуточной аттестации: зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.)	Экз.	Экз.

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/КР час.	СРС час.
Семестр 7					
Раздел 1. Основные понятия криптографии Тема 1.1. Основные определения Тема 1.2. Задачи информационной безопасности	1	0	0	0	20
Раздел 2. Симметричные шифры Тема 2.1. Исторические шифры Тема 2.2. Блоковые шифры Тема 2.3. Потоковые шифры	1	0	2	0	40
Раздел 3. Криптография с открытым ключом Тема 3.1. Математические основы систем с открытым ключом Тема 3.2. Основные алгоритмы с открытым ключом	2	0	4	0	40
Раздел 4. Криптографические протоколы Тема 4.1. Основные протоколы с открытым ключом Тема 4.2. Специальные протоколы Тема 4.3. Генераторы псевдослучайных чисел	2	0	0	0	23
Итого в семестре:	6	0	6	0	123
Итого:	6	0	6	0	123

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	Основные понятия криптографии Тема 1.1. Основные определения Определение целей и принципов защиты информации; установление, факторов, влияющих на защиту информации; основные опасности и угрозы в области информационной безопасности. Классификации видов, методов и средств защиты информации. Организационная защита информации. Инженерно-техническая защита информации. Криптографическая защита информации. Представление информации в цифровом виде. Тема 1.2. Задачи информационной безопасности Задача обеспечения конфиденциальности. Определение шифра. Задача обеспечения аутентификации, понятия об электронной цифровой подписи (ЭЦП). Основные задачи в области управления ключами. Криптопротоколы: обеспечение идентификации, разделение секрета, выработка ключа, цифровые деньги.
2	Симметричные шифры Тема 2.1. Исторические шифры Подстановочные шифры и перестановочные шифры. Шифр Цезаря, аффинный шифр, шифр моноалфавитной замены. Шифр Виженера. Цилиндр Джефферсона. Полиалфавитные шифры. Роторные машины. Тема 2.2. Блоковые шифры Понятие стойкости, предположения об исходных условиях криптоанализа, совершенная стойкость. Одноразовый блокнот. Шифр Вернама. Принципы построения блоковых шифров. Свойства смешивания и рассеивания. Составные шифры, итеративные шифры. SP-сети, сети Файстеля. Современные системы шифрования: алгоритмы DES, ГОСТ 28147-89, AES. Режимы блокового шифрования: ECB, CBC, CFB, OFB. Режим счетчика. Многократное шифрование. Тема 2.3. Потоковые шифры Требования к поточным шифрам. Методы построения больших периодов в поточных шифрах. Регистры сдвига с линейной обратной связью (РСЛОС). m-последовательности. Алгоритм Берлекэмпа-Месси. Построение потоковых шифров на основе РСЛОС. Нелинейное комбинирование РСЛОС: генератор Геффе, шифры с контролем тактов. Применение поточного шифрования.
3	Криптография с открытым ключом Тема 3.1. Математические основы систем с открытым ключом Модульная арифметика. Алгоритм Евклида и его сложность. Расширенный алгоритм Евклида. Основные теоремы о вычетах. Функция Эйлера. Теоремы Эйлера, Ферма. Факторизация. Логарифмирование в конечных полях. Оценки сложности “трудных” проблем, на которых строятся системы с открытым ключом. Быстрое возведение в степень. Тема 3.2. Основные алгоритмы с открытым ключом Система Меркли-Хеллмана. Схема RSA. Атаки на RSA. Схема шифрования Эль-Гамаля. Система Мак-Элиса. Криптографические хэш-функции. Понятие о цифровой подписи. Подпись RSA. Подпись Эль-Гамаля. Подпись DSA. ЭЦП ГОСТ Р 34.10-94 и ГОСТ Р 34.10-01.
4	Криптографические протоколы Тема 4.1. Основные протоколы с открытым ключом Выработка ключа. Протокол Диффи-Хелмана. Гибридные системы шифрования: цифровой конверт. Доказательство с нулевым разглашением. Схема идентификации Фиата-Шамира. Схема идентификации Гиллу-Квискуотера. Инфраструктура открытых ключей. Сертификаты открытых ключей. Тема 4.2. Специальные протоколы Слепая подпись. Протоколы разделения секрета и вручения бит. Протоколы цифровых денег и электронного голосования. Защищенные распределенные вычисления. Тема 4.3. Генераторы псевдослучайных чисел Виды и классификация генераторов. Структура генераторов. Криптографически стойкие ГПСЧ. Периодичность и апериодичность.

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	0	0	

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	Анализ исторических шифров. Шифр Цезаря, Афинский диск, шифр Виженера	2	0	2
2	Шифрование с открытым ключом	4	0	3
	Всего	6	0	

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.
Изучение теоретического материала дисциплины (ТО)	30	30
Курсовое проектирование (КП, КР)	0	0
Расчетно-графические задания (РГЗ)	0	0
Выполнение реферата (Р)	0	0
Подготовка к текущему контролю успеваемости (ТКУ)	30	30
Домашнее задание (ДЗ)	0	0
Контрольные работы заочников (КРЗ)	40	40
Подготовка к промежуточной аттестации (ПА)	23	23
Всего	123	123

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)
https://znanium.com/catalog/product/1861657	Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1861657. – Режим доступа: по подписке.	-
https://znanium.com/catalog/product/405000	Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/405000. – Режим доступа: по подписке.	-
https://znanium.com/catalog/product/1088209	Пилиди, В. С. Математические основы зашиты информации : учебное пособие / В. С. Пилиди ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2019. - 308 с. - ISBN 978-5-9275-3363-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1088209. – Режим доступа: по подписке.	-
https://znanium.com/catalog/product/1210523	Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523. – Режим доступа: по подписке.	-

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://window.edu.ru/	Бесплатная электронная библиотека онлайн "Единое окно к образовательным ресурсам"
https://www.intuit.ru/	Национальный Открытый Университет "ИНТУИТ"
https://elibrary.ru/	eLIBRARY.RU - Научная электронная библиотека
http://lib.guap.ru/	Библиотека ГУАП

URL адрес	Наименование
https://znanium.com/	Электронно-библиотечная система Znanium
https://e.lanbook.com/	ЭБС Лань
https://www.book.ru/	BOOK.RU - современная электронная библиотека для вузов и ссузов от правообладателя
https://urait.ru/	Образовательная платформа Юрайт
http://www.iprbookshop.ru/	Электронно-библиотечная система IPR BOOKS

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	CrypTool 2
2	Embarcadero RAD Studio XE7 Professional
3	Microsoft Office Professional Plus
4	Microsoft Visual Studio Community
5	Visual Studio Code

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
Учебным планом не предусмотрено	

9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Фонд аудиторий ИФ ГУАП для проведения лекционных и практических (семинарских) занятий	
2	Лаборатория прикладной математики и информационных технологий	206
3	Кабинет информационных технологий и программных систем	212

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 - Тесты - Экзаменационные билеты

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	Код индикатора
1	Понятие информация. Понятие криптографии. Принципы защиты информации.	ОПК-3.З.1
2	Опасности и угрозы в области информационной безопасности.	ОПК-3.З.1
3	Классификация методов защиты информации.	ОПК-3.З.1
4	Организационная защита информации.	ОПК-3.У.1

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
5	Инженерно-техническая защита информации.	ОПК-3.У.1
6	Криптографическая защита информации.	ОПК-3.У.1
7	Представление информации в цифровом виде.	ОПК-3.З.1
8	Конфиденциальность.	ОПК-3.З.1
9	Понятие аутентификация.	ОПК-3.З.1
10	Понятие авторизация.	ОПК-3.З.1
11	Понятие идентификация.	ОПК-3.З.1
12	Задачи управления ключами.	ОПК-3.В.1
13	Криптопротоколы	ОПК-3.В.1
14	Определение шифр.	ОПК-8.З.1
15	Симметричные шифры.	ОПК-8.У.1
16	Шифр Цезаря, аффинный шифр, шифр моноалфавитной замены.	ОПК-1.З.1
17	Шифр Виженера.	ОПК-1.З.1
18	Цилиндр Джефферсона.	ОПК-1.З.1
19	Полиалфавитные шифры.	ОПК-1.У.1
20	Роторные машины.	ОПК-1.У.1
21	Стойкость шифра.	ОПК-8.З.1
22	Одноразовый блокнот.	ОПК-8.У.1
23	Шифр Вернама.	ОПК-8.У.1
24	Принципы построения блоковых шифров.	ОПК-2.З.1
25	Составные шифры, итеративные шифры.	ОПК-2.З.1
26	SP-сети, сети Файстеля.	ОПК-2.У.1
27	DES, ГОСТ 28147-89, AES.	ОПК-2.У.1
28	Режимы блокового шифрования: ECB, CBC, CFB, OFB.	ОПК-2.В.1
29	Потоковые шифры.	ОПК-2.В.1
30	Понятие открытый ключ. Понятие закрытый ключ.	ОПК-8.В.1
31	Алгоритм Евклида и его сложность.	ОПК-1.В.1

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 выполнения курсовой работы

№ п/п	Примерный перечень тем для 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	К правовым методам, обеспечивающим информационную безопасность, относятся...	ОПК-3.З.1
2	Основными источниками угроз информационной безопасности являются все указанное в списке...	ОПК-3.З.1
3	Виды информационной безопасности..	ОПК-3.З.1
4	Цели информационной безопасности...	ОПК-3.З.1
5	Чем симметричные шифры отличаются от несимметричных?	ОПК-8.З.1
6	Опишите характеристики потоковых шифров	ОПК-8.З.1
7	Чем потоковые шифры отличаются от блочных	ОПК-8.У.1
8	Какие исторические шифры являются наиболее криптостойкие	ОПК-3.З.1
9	Что такое открытый ключ	ОПК-8.В.1
10	Что такое закрытый ключ	ОПК-8.В.1
11	Какие информационные системы используют ЭЦП?	ОПК-2.З.1
12	Приведите пример основных алгоритмов с открытым ключом	ОПК-8.В.1
13	Что такое ЭЦП?	ОПК-2.З.1
14	Опишите основные протоколы для работы с открытым ключом	ОПК-8.У.1
15	Опишите специальные протоколы	ОПК-8.У.1
16	Опишите протокол Диффи-Хелмана.	ОПК-8.У.1
17	Опишите схему идентификации Фиата-Шамира	ОПК-8.У.1
18	Что такое случайное число?	ОПК-1.З.1
19	Где используется генератор псевдослучайных чисел?	ОПК-1.В.1
20	Что такое периодичность и апериодичность?	ОПК-1.У.1
21	Приведите классификацию генераторов псевдослучайных чисел	ОПК-3.У.1
22	Какие уровни информационной защиты существуют, их основные составляющие?	ОПК-3.У.1
23	Что включает в себя защита информации от несанкционированного доступа?	ОПК-3.У.1
24	Какие виды механизмов защиты могут быть реализованы для обеспечения конфиденциальности данных и сообщений?	ОПК-3.В.1
25	Какие требования необходимо выполнять при экранировании помещений, предназначенных для размещения вычислительной техники?	ОПК-3.В.1
26	Какой процесс называется аутентификацией пользователя?	ОПК-8.У.1
27	Какие виды симметричных криптосистем существуют?	ОПК-8.В.1
28	Какие требования предъявляются к межсетевым экранам?	ОПК-8.В.1
29	Какие вирусы называются паразитическими?	ОПК-8.В.1
30	Как осуществляется защита при помощи ACL -списков?	ОПК-2.У.1
31	Какие пути защиты информации в локальной сети существуют?	ОПК-2.У.1
32	Что такое дифференциальный криптоанализ?	ОПК-2.В.1

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	Поточное и блочное шифрование
2	Генераторы псевдослучайных чисел

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.

Выделяются следующие виды лекций:

- Вводная лекция

  Вводная лекция к дисциплине знакомит обучающихся с целью и назначением курса, его ролью и местом в системе дисциплин. В ходе такой лекции связывается теоретический и практический материал с практикой будущей работы, рассказывается общая методика работы над курсом, предлагаются литературные источники, помогающие усвоению материала дисциплины и освоению компетенций, ставятся научные проблемы, выдвигаются гипотезы, определяется форма текущего контроля и промежуточной аттестации.

  Вводная лекция к разделу. Аналогично вводной лекции к дисциплине раскрывает ряд вопросов, но связанных не с дисциплиной в целом, а с тематикой конкретного раздела.

- Обзорная лекция

  Проводится с целью систематизации знаний на более высоком уровне, рассмотрения особо трудных вопросов дисциплины.

- Проблемная лекция

  На данной лекции новое знание вводится как неизвестное, которое необходимо "открыть". В рамках лекции создается проблемная ситуация, которую обучающие решают поэтапно с подсказками и помощью преподавателя.

- Лекция вдвоем

  Эта разновидность лекции является продолжением и развитием проблемного изложения материала в диалоге двух преподавателей. Здесь моделируются реальные ситуации обсуждения теоретических и практических вопросов двумя специалистами.

- Лекция с заранее запланированными ошибками

Данная лекция призвана активизировать внимание обучающихся, развивать их мыслительную деятельность, формировать умение выступать в роли экспертов.

Задача преподавателя состоит в том, чтобы заложить в лекцию определенное количество ошибок содержательного, методического, поведенческого характера. Подбираются наиболее типичные ошибки, которые обычно не выпячиваются, а как бы затушевываются. Задача обучающихся состоит в том, чтобы по ходу лекции отмечать ошибки, фиксировать и называть их в конце.

- Лекция-пресс-конференция

Преподаватель просит обучающихся задавать письменно вопросы по данной теме. В течение двух-трех минут обучающиеся формулируют наиболее интересующие их вопросы и передают преподавателю, который в течение трех-пяти минут сортирует вопросы по их содержанию и начинает лекцию. Лекция излагается не как ответы на вопросы, а как связный текст, в процессе изложения которого формируются ответы.

- Лекция-консультация

Материал излагается в виде вопросов и ответов или вопросов, ответов и дискуссий.

Структура предоставления лекционного материала:

- Вводная часть лекции

Первое представление о лекции содержится уже в формулировке темы. Она должна быть краткой, выражать суть основной идеи, быть привлекательной по форме. Целесообразно здесь сказать на значение этой темы для последующего усвоения знаний и развития личности обучающихся, для будущей профессиональной деятельности. Далее можно сообщить цели лекции и ее план. Желательно сориентировать слушателей на последующий контроль знаний, полезно указать на связь нового материала с пройденным и предыдущим. Темп изложения этой части лекции, как правило, должен быть выше темпа изложения основного, что заставляет обучающихся психологически собраться и сосредоточиться. Вводная часть лекции обычно занимает 5-7 минут.

- Основная часть лекции

Переходу к изложению первого вопроса, как правило, должна предшествовать пауза. В это время лектор может проверить, все ли слушатели готовы к восприятию лекции (позы, выражения лиц, разговоры). Заметив обучающихся, не готовых к восприятию, опытные преподаватели произносят краткую мобилизующую фразу, останавливают взгляд на нерадивых, реже - называют фамилию, имя и не тратят время на длительные замечания.

Для того чтобы преодолеть потенциальную пассивность слушателей, необходимо всеми возможными способами придать лекции проблемный характер, побуждая слушателей к самостоятельной познавательной активности и творчеству.

К таким активным средствам можно отнести:

◦ обращение к обучающимся с вопросами, уточняющими понимание основных идей и фактов темы;

◦ организацию мини-столкновений различных точек зрения по выдвинутым преподавателем положениям;

◦ постановку вопросов, задач с множественностью решений и др.;

◦ индивидуальный стиль изложения материала;

◦ обеспечение обратной связи.

- Заключение

В процессе чтения лекции преподаватель должен позаботиться о ее завершении. Рассчитать время, а не прерывать лекцию на полуслове. Обычно для заключения материала бывает достаточно 5-7 минут. Завершая лекцию, преподаватель отвечает на вопросы слушателей, подводит итог, дает методические указания к самостоятельной работе, комментирует предлагаемую литературу. Заканчивать лекцию нужно конструктивно по содержанию и положительно по эмоциональному настрою. Обучающиеся должны уйти заинтересованными, заинтригованными, желающими опробовать завтра же предложения лектора, а также в хорошем настроении и активном тонусе.

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.

Выполнение обучающимся лабораторных работ не в полном объеме может привести к понижению оценки за дисциплину из-за низкого уровня освоения компетенций:

- выполнение менее 75% лабораторных работ - понижение максимальной оценки на 1 балл;
- выполнение менее 50% лабораторных работ - понижение максимальной оценки на 2 балла;
- невыполнение лабораторных работ - понижение максимальной оценки на 3 балла.

Задание и требования к проведению лабораторных работ.

Задания и требования к лабораторным работам размещены в Личном кабинете ГУАП в разделе дисциплины.

Структура и форма отчета о лабораторной работе.

Отчет о лабораторной работе сдается в электронном виде (документ Word, документ PDF) через Личный кабинет ГУАП. Отчет к лабораторной работе содержит следующие элементы:

- титульный лист с названием дисциплины, номером и названием лабораторной работы;
- цели и задачи работы;
- задание;
- ход работы;
- математическая модель;
- схема алгоритма;
- текст программы;
- контрольные примеры;
- выводы;
- список использованных источников (при необходимости).

Требования к оформлению отчета о лабораторной работе.

- Общие требования и рекомендации по выполнению письменных работ : методические указания / С.-Петерб. гос. ун-т аэрокосм. приборостроения ; сост. А. А. Сорокин. - СПб. : Изд-во ГУАП, 2017. - 32 с.

- Общие требования и рекомендации по выполнению письменных работ : методические указания *(с изменениями от 09.01.2019)* [Электронный ресурс] / Ивангородский филиал С.-Петерб. гос. ун-т аэрокосм. приборостроения ; сост. А. А. Сорокин. - Ивангород : 2019. - 37 с. URL: http://ifguap.ru/rp/ReportsFormattingRules.pdf, Личный кабинет ГУАП

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:

- методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения);
- учебно-методический материал по дисциплине.

11.4. Методические указания для обучающихся по прохождению консультаций.

По изучаемой дисциплине проводятся следующие виды консультаций:

- Консультация перед экзаменом - проводится с целью:
  - уточнения организационных моментов;
  - систематизации знаний;
  - ответы на вопросы, вызывающие трудности при подготовке к экзамену.

  Консультация имеет форму лекции, после которой преподаватель отвечает на вопросы обучающихся или в виде беседы в форме "ответ-вопрос".
- Консультация со слабоуспевающими обучающимися - предназначена для:
  - ликвидации пробелов при изучении дисциплины;
  - разъяснения спорных вопросов и вопросов, наиболее сложных для изучения;
  - закрепления пройденного материала;
  - ликвидации академических задолженностей.

  Проводится регулярно согласно графику консультаций преподавателя (не реже 1 раза в 2 недели).

- Консультация по проектной и научно-исследовательской деятельности обучающихся - проводится с целью:
  - расширения научного кругозора обучающихся;
  - рассмотрения вопросов, не включенных в программу изучаемой дисциплины;
  - углубленного изучения материала курса;
  - помощи обучающимся в подготовке научных статей и докладов на конференции;
  - подготовки в участию в конкурсах и олимпиадах.

Проводится регулярно согласно графику консультаций преподавателя или по устной договоренности между обучающимся и преподавателем.

11.5. 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. Невыполнение требований или их части по прохождению текущего контроля успеваемости при успешном прохождении промежуточной аттестации может привести к понижению итоговой оценки.

Возможные методы текущего контроля:

- устный опрос на занятиях;
- систематическая проверка выполнения индивидуальных и домашних заданий;
- защита отчетов по лабораторным работам;
- проведение контрольных работ;
- тестирование;
- контроль самостоятельных работ;
- проведение контрольных работ;
- выполнения контрольной работы заочников;
- доклад на научной конференции;
- написание научной статьи.

11.6. Методические указания для обучающихся по прохождению тестирования.

Использование тестовых заданий возможно как при текущем контроле, так и при проведении промежуточной аттестации. Тесты могут проводиться как в письменной форме, так и с использованием электронных средств обучения.

Можно выделить основные уровни теста, в которых проверка возрастает от контроля знаний (индикатор достижения компетенции - "знать") до применения навыков при решении типовых и нетиповых задач ((индикаторы достижения компетенции - "уметь" и "владеть"):

- Первый уровень - узнавание ранее изученного материала;
- Второй уровень - репродуктивный - в заданиях не содержится материала для ответа или же его извлечение требует не только запоминания материала, но и его понимания (подстановка, конструктивный тест, типовая задача);
- Третий уровень - нетиповые задачи повышенной сложности, для которых требуется самостоятельное нахождение методов решения;
- Смешанный - использование элементов всех трех уровней для проверки разных индикаторов достижения компетенций.

Критерии оценки тестовых работ базируются на 100-бальной шкале согласно МДО ГУАП. СМК 2.77 "Положение о модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП" (допустимо применение любого количественного показателя оценки с приведением его к 100-процентной шкале):

- менее 55 - "не зачтено" или "неудовлетворительно" (2);
- от 55 до 69 - "зачтено" или "удовлетворительно" (3);
- от 70 до 84 - "зачтено" или "хорошо" (4);
- от 85 до 100 - "зачтено" или "отлично" (5).

11.7. 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".

Экзамен проводится в одной из следующих форм:

- в устной форме в виде ответа на вопросы экзаменационного билета
- в письменной форме в виде теста
- с применением средств электронного обучения (LMS ГУАП)

В случае дистанционной формы обучения по данной программе предусмотрено использование с применением средств

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