

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 № 2

УТВЕРЖДАЮ
Руководитель образовательной программы

старший преподаватель

(должность, уч. степень, звание)

А.А. Сорокин

(инициалы, фамилия)



(подпись)

«25» февраля 2026 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/ специализации	Программное обеспечение средств вычислительной техники и автоматизированных систем
Форма обучения	очная
Год приема	2026

Ивангород – 2026

Лист согласования рабочей программы дисциплины

Программу составил (а)

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



10.02.2026
(подпись, дата)

А.В. Дагаев
(инициалы, фамилия)

Программа одобрена на заседании кафедры № 2

«10» февраля 2026 г, протокол № 6

И.о. зав. кафедрой № 2

д.ф.-м.н.
(уч. степень, звание)



10.02.2026
(подпись, дата)

Ю.В. Рождественский
(инициалы, фамилия)

Заместитель директора ИФ ГУАП по методической работе

(должность, уч. степень, звание)



10.02.2026
(подпись, дата)

Н.В. Шустер
(инициалы, фамилия)

Аннотация

Дисциплина «Защита информации» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 09.03.01 «Информатика и вычислительная техника» направленности/специализации «Программное обеспечение средств вычислительной техники и автоматизированных систем». Дисциплина реализуется кафедрой «№2».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

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 (7 семестр).

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов.

Язык обучения по дисциплине «русский»

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

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-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-2.3.1 знать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности ОПК-2.У.1 уметь выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности ОПК-2.В.1 владеть навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности
Общепрофессиональные компетенции	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с	ОПК-3.3.1 знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий, включая интеллектуальные технологии, и с учетом основных требований

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

2. Место дисциплины в структуре ОП

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

- Алгоритмы и структуры данных;
- Базы данных;
- Операционные системы;
- Основы программирования.

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

- Web-программирование.

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)	3/ 108	3/ 108
Из них часов практической подготовки		
Аудиторные занятия, всего час.	51	51
в том числе:		
лекции (Л), (час)	34	34
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	17	17
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)	36	36
Самостоятельная работа, всего (час)	21	21
Вид промежуточной аттестации: зачет, 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)	СР (час)
Семестр 7					
Раздел 1. Основные понятия криптографии					
Тема 1.1. Основные определения	10		0		5
Тема 1.2. Задачи информационной безопасности					
Раздел 2. Симметричные шифры					
Тема 2.1. Исторические шифры	8		9		5
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	8		8		5
Тема 3.2. Основные алгоритмы с открытым ключом					
Раздел 4. Криптографические протоколы					
Тема 4.1. Основные протоколы с открытым ключом	8		0		6
Тема 4.2. Специальные протоколы					
Тема 4.3. Генераторы псевдослучайных чисел					
Итого в семестре:	34		17		21
Итого	34	0	17	0	21

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. Блочные шифры Понятие стойкости, предположения об исходных условиях криптоанализа, совершенная стойкость. Одноразовый блокнот. Шифр Вернама. Принципы построения блочных шифров. Свойства смешивания и рассеивания. Составные шифры, итеративные шифры. SP-сети, сети Файстеля. Современные системы шифрования: алгоритмы DES, ГОСТ 28147-89, AES. Режимы блочного шифрования: ECB, CBC, CFB, OFB. Режим счетчика. Многократное шифрование. Тема 2.3. Поточные шифры Требования к поточным шифрам. Методы построения больших периодов в поточных шифрах. Регистры сдвига с линейной обратной связью (РСЛОС). m-последовательности. Алгоритм Берлекэмп-Мессе. Построение поточных 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-Гамала. Система Мак-Элиса. Криптографические хэш-функции. Понятие о цифровой подписи. Подпись RSA. Подпись Эль-Гамала. Подпись DSA. ЭЦП ГОСТ Р 34.10-94 и ГОСТ Р 34.10-01.
4	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					

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	Вводное занятие	1		2
2	Анализ исторических шифров. Шифр Цезаря, Афинский диск, шифр Виженера	4		2
3	Поточное и блочное шифрование	4		2
4	Шифрование с открытым ключом	4		3
5	Генераторы псевдослучайных чисел	4		3
Всего		17		

4.5. Выполнение курсового проекта/ 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)	11	11
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	5	5
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	5	5
Всего:	21	21

5. Перечень учебно-методического обеспечения
для самостоятельной работы обучающихся по дисциплине (модулю)
Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. разделов 6-11.

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.ru/catalog/product/2233509 Режим доступа: для авторизованных пользователей.	Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 5-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2026. — 384 с.	-
https://znanium.ru/catalog/product/2242341 Режим доступа: для авторизованных пользователей.	Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 4-е изд. — Москва : РИОР : ИНФРА-М, 2026. — 398 с.	-
https://znanium.ru/catalog/product/2261229 Режим доступа: для авторизованных пользователей.	Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ИНФРА-М, 2026. — 592 с.	-
https://znanium.ru/catalog/product/2241407 Режим доступа: для авторизованных пользователей.	Криптографическая защита информации : учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.] ; под ред. С.О. Крамарова. — Москва : РИОР : ИНФРА-М, 2026. — 321 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.intuit.ru/	Национальный Открытый Университет "ИНТУИТ"
http://lib.guap.ru/	Библиотека ГУАП
http://pro.guap.ru/	Личный кабинет ГУАП
http://lms.guap.ru/	Система дистанционного образования ГУАП
https://znanium.com/	Электронно-библиотечная система Znanium
https://urait.ru/	Образовательная платформа Юрайт

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
	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	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
4	Помещения для организации самостоятельной работы	111

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; 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 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 связывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий. – правильно выполнил от 90% до 100% тестовых заданий.
«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. – правильно выполнил от 70% до 89% тестовых заданий.
«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. – правильно выполнил от 51% до 69% тестовых заданий.
«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. – правильно выполнил менее 51% тестовых заданий.

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	Цели и принципы защиты информации	ОПК-2.3.1
2	Основные угрозы и опасности в области информационной безопасности	ОПК-2.3.1
3	Классификация методов и средств защиты информации	ОПК-2.3.1
4	Организационные методы защиты информации	ОПК-2.3.1
5	Инженерно-технические методы защиты информации	ОПК-2.3.1

6	Криптографическая защита информации: назначение и область применения	ОПК-2.3.1
7	Представление информации в цифровом виде	ОПК-2.3.1
8	Как выбрать современные программные средства защиты информации	ОПК-2.У.1
9	Как выбрать отечественные средства защиты информации	ОПК-2.У.1
10	Применение современных ИТ при решении задач защиты информации	ОПК-2.В.1
11	Основные задачи информационной безопасности	ОПК-3.3.1
12	Понятие конфиденциальности, целостности и доступности	ОПК-3.3.1
13	Что такое шифр и какие бывают виды шифров	ОПК-3.3.1
14	Что такое электронная цифровая подпись	ОПК-3.3.1
15	Основные задачи управления ключами	ОПК-3.3.1
16	Криптопротоколы: идентификация, разделение секрета, выработка ключа	ОПК-3.3.1
17	Как решать стандартные задачи ИБ с учётом требований безопасности	ОПК-3.У.1
18	Как применять ИКТ и ИИ для решения задач ИБ	ОПК-3.У.1
19	Как оформлять результаты НИР и ОКР с учётом требований ИБ	ОПК-3.В.1
20	Как составлять библиографию и научные обзоры по тематике ИБ	ОПК-3.В.1
21	Исторические шифры: подстановочные и перестановочные	ОПК-3.3.1
22	Шифр Цезаря, аффинный шифр, шифр Виженера	ОПК-3.3.1
23	Роторные машины и их принципы	ОПК-3.3.1
24	Понятие стойкости шифра	ОПК-3.3.1
25	Одноразовый блокнот и шифр Вернама	ОПК-3.3.1
26	Принципы построения блочных шифров	ОПК-3.3.1
27	Сети Файстеля и SP-сети	ОПК-3.3.1
28	Алгоритмы DES, ГОСТ 28147-89, AES	ОПК-3.3.1
29	Режимы блочного шифрования: ECB, CBC, CFB, OFB, CTR	ОПК-3.3.1
30	Требования к поточным шифрам	ОПК-3.3.1
31	РСЛОС и m-последовательности	ОПК-3.3.1
32	Алгоритм Берлекэмп-Мессии	ОПК-3.3.1
33	Математические основы криптографии: модульная арифметика	ОПК-3.3.1
34	Функция Эйлера, теоремы Эйлера и Ферма	ОПК-3.3.1
35	Факторизация и дискретный логарифм	ОПК-3.3.1
36	Быстрое возведение в степень	ОПК-3.3.1
37	Система RSA: принципы и уязвимости	ОПК-3.3.1
38	Схема Эль-Гамала	ОПК-3.3.1
39	Криптографические хэш-функции	ОПК-3.3.1
40	Цифровая подпись: RSA, DSA, ГОСТ	ОПК-3.3.1
41	Протокол Диффи-Хеллмана	ОПК-3.3.1
42	Гибридные системы шифрования	ОПК-3.3.1
43	Доказательства с нулевым разглашением	ОПК-3.3.1
44	Схемы идентификации Фиата-Шамира и Гиллу-Квискуотера	ОПК-3.3.1
45	Инфраструктура открытых ключей и сертификаты	ОПК-3.3.1

46	Слепая подпись	ОПК-3.3.1
47	Протоколы разделения секрета	ОПК-3.3.1
48	Протоколы электронных денег и голосования	ОПК-3.3.1
49	Генераторы псевдослучайных чисел: классификация	ОПК-3.3.1
50	Криптографически стойкие ГПСЧ	ОПК-3.3.1
51	Как анализировать техническую документацию по криптографии	ОПК-7.У.1
52	Как выполнять настройку криптографических модулей	ОПК-7.У.1
53	Как тестировать криптографические системы	ОПК-7.В.1
54	Как выполнять инсталляцию средств защиты информации	ОПК-5.В.1
55	Как выполнять параметрическую настройку систем защиты	ОПК-5.У.1
56	Алгоритмические языки и ОС, применяемые в криптографии	ОПК-8.3.1
57	Как писать и отлаживать программы для криптографических задач	ОПК-8.У.1
58	Как тестировать криптографические программные модули	ОПК-8.В.1
59	Как интегрировать криптографические модули в систему	ОПК-8.У.1
60	Как применять современные ИТ для защиты информации	ОПК-2.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 выполнения курсового проекта/ курсовой работы представлены в таблице 17.

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

№ п/п	Примерный перечень тем для выполнения курсового проекта/ 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 закрытого типа с выбором одного правильного ответа Инструкция: Прочитайте текст и выберите один правильный ответ Какое отечественное программное средство используется для криптографической защиты информации? 1. OpenSSL 2. VeraCrypt 3. КриптоПро CSP 4. TrueCrypt Ключ с правильным ответом: 3	ОПК-2.3.1
2	Задание закрытого типа с выбором нескольких правильных ответов Инструкция: Прочитайте текст и выберите все правильные ответы Какие технологии относятся к современным средствам защиты	ОПК-2.3.1

	информации? 1. Шифрование данных 2. Двухфакторная аутентификация 3. Контроль целостности 4. Ручное копирование файлов Ключ с правильным ответом: 1, 2, 3									
3	Задание закрытого типа на установление соответствия Инструкция: Прочитайте текст и установите соответствие Сопоставьте средство защиты и его назначение. <table><tr><th>Средство</th><th>Назначение</th></tr><tr><td>А. Антивирус</td><td>1. Обнаружение вредоносного ПО</td></tr><tr><td>Б. Межсетевой экран</td><td>2. Фильтрация сетевого трафика</td></tr><tr><td>В. Криптопровайдер</td><td>3. Шифрование и подпись данных</td></tr></table> Ключ с правильным ответом: А1, Б2, В3	Средство	Назначение	А. Антивирус	1. Обнаружение вредоносного ПО	Б. Межсетевой экран	2. Фильтрация сетевого трафика	В. Криптопровайдер	3. Шифрование и подпись данных	ОПК-2.3.1
Средство	Назначение									
А. Антивирус	1. Обнаружение вредоносного ПО									
Б. Межсетевой экран	2. Фильтрация сетевого трафика									
В. Криптопровайдер	3. Шифрование и подпись данных									
4	Задание закрытого типа на установление правильной последовательности Инструкция: Прочитайте текст и установите последовательность Этапы обеспечения защиты информации: 1. Анализ угроз 2. Выбор средств защиты 3. Настройка механизмов безопасности 4. Мониторинг событий 5. Оценка эффективности Запишите последовательность цифр слева направо. Ключ с правильным ответом: 1, 2, 3, 4, 5	ОПК-2.3.1								
5	Задание открытого типа Инструкция: Прочитайте текст и запишите ответ. Как называется процесс преобразования данных в недоступный для чтения вид? Ключ с правильным ответом: шифрование	ОПК-2.3.1								
6	Задание открытого типа с развернутым обоснованным ответом Инструкция: Прочитайте текст и запишите развернутый обоснованный ответ Объясните роль современных информационных технологий в обеспечении защиты информации. Ключ с правильным ответом (эталонный ответ): Современные информационные технологии обеспечивают комплексную защиту данных, включая шифрование, аутентификацию, контроль целостности и мониторинг событий безопасности. Они позволяют предотвращать угрозы, снижать риски утечек и обеспечивать надежную защиту информации в профессиональной деятельности, включая использование отечественных программных средств.	ОПК-2.3.1								
7	Задание закрытого типа с выбором одного правильного ответа Инструкция: Прочитайте текст и выберите один правильный ответ Какое средство используется для выбора криптографических алгоритмов и настройки параметров шифрования в отечественных системах? 1. OpenVPN 2. КриптоПро CSP 3. BitLocker 4. KeePass Ключ с правильным ответом: 2	ОПК-2.У.1								

8	Задание закрытого типа с выбором нескольких правильных ответов Инструкция: Прочитайте текст и выберите все правильные ответы Какие критерии учитываются при выборе средств защиты информации? 1. Соответствие требованиям безопасности 2. Наличие сертификации 3. Совместимость с инфраструктурой 4. Цвет интерфейса программы Ключ с правильным ответом: 1, 2, 3	ОПК-2.У.1								
9	Задание закрытого типа на установление соответствия Инструкция: Прочитайте текст и установите соответствие Сопоставьте средство защиты и его назначение. <table><tr><td>Средство</td><td>Назначение</td></tr><tr><td>А. HSM-модуль</td><td>1. Аппаратное хранение ключей</td></tr><tr><td>Б. IDS/IPS</td><td>2. Обнаружение и предотвращение атак</td></tr><tr><td>В. VPN-шлюз</td><td>3. Защита каналов связи</td></tr></table> Ключ с правильным ответом: А1, В2, В3	Средство	Назначение	А. HSM-модуль	1. Аппаратное хранение ключей	Б. IDS/IPS	2. Обнаружение и предотвращение атак	В. VPN-шлюз	3. Защита каналов связи	ОПК-2.У.1
Средство	Назначение									
А. HSM-модуль	1. Аппаратное хранение ключей									
Б. IDS/IPS	2. Обнаружение и предотвращение атак									
В. VPN-шлюз	3. Защита каналов связи									
10	Задание закрытого типа на установление правильной последовательности Инструкция: Прочитайте текст и установите последовательность Этапы выбора программного средства защиты: 1. Определение требований безопасности 2. Анализ доступных решений 3. Оценка совместимости 4. Тестирование выбранного средства 5. Принятие решения Запишите последовательность цифр слева направо. Ключ с правильным ответом: 1, 2, 3, 4, 5	ОПК-2.У.1								
11	Задание открытого типа Инструкция: Прочитайте текст и запишите ответ. Как называется процесс проверки выбранного средства защиты в условиях, близких к реальной эксплуатации? Ключ с правильным ответом: тестирование	ОПК-2.У.1								
12	Задание открытого типа с развернутым обоснованным ответом Инструкция: Прочитайте текст и запишите развернутый обоснованный ответ Объясните, почему важно учитывать отечественные программные средства при выборе технологий защиты информации. Ключ с правильным ответом (эталонный ответ): Использование отечественных программных средств позволяет обеспечить соответствие требованиям национальной безопасности, снизить зависимость от зарубежных поставщиков и повысить устойчивость инфраструктуры. Это особенно важно при защите критически важных данных и построении доверенной информационной среды.	ОПК-2.У.1								
13	Задание закрытого типа с выбором одного правильного ответа Инструкция: Прочитайте текст и выберите один правильный ответ Какое программное средство используется для проверки целостности файлов? 1. Paint 2. HashCalc 3. Блокнот 4. Калькулятор	ОПК-2.В.1								

	Ключ с правильным ответом: 2									
14	Задание закрытого типа с выбором нескольких правильных ответов Инструкция: Прочитайте текст и выберите все правильные ответы Какие действия относятся к практическому применению технологий защиты информации? 1. Настройка шифрования дисков 2. Управление ключами 3. Настройка политик безопасности 4. Изменение обоев рабочего стола Ключ с правильным ответом: 1, 2, 3	ОПК-2.В.1								
15	Задание закрытого типа на установление соответствия Инструкция: Прочитайте текст и установите соответствие Сопоставьте программное средство и его назначение. <table><tr><td>Средство</td><td>Назначение</td></tr><tr><td>А. КриптоПро CSP</td><td>1. Реализация криптографических алгоритмов</td></tr><tr><td>Б. OpenVPN</td><td>2. Создание защищённых каналов связи</td></tr><tr><td>В. Snort</td><td>3. Обнаружение сетевых атак</td></tr></table> Ключ с правильным ответом: А1, Б2, В3	Средство	Назначение	А. КриптоПро CSP	1. Реализация криптографических алгоритмов	Б. OpenVPN	2. Создание защищённых каналов связи	В. Snort	3. Обнаружение сетевых атак	ОПК-2.В.1
Средство	Назначение									
А. КриптоПро CSP	1. Реализация криптографических алгоритмов									
Б. OpenVPN	2. Создание защищённых каналов связи									
В. Snort	3. Обнаружение сетевых атак									
16	Задание закрытого типа на установление правильной последовательности Инструкция: Прочитайте текст и установите последовательность Этапы применения средств защиты информации: 1. Анализ угроз 2. Выбор подходящих технологий 3. Настройка механизмов защиты 4. Тестирование работоспособности 5. Мониторинг и корректировка Запишите последовательность цифр слева направо. Ключ с правильным ответом: 1, 2, 3, 4, 5	ОПК-2.В.1								
17	Задание открытого типа Инструкция: Прочитайте текст и запишите ответ. Как называется процесс проверки корректности работы настроенных механизмов защиты? Ключ с правильным ответом: тестирование	ОПК-2.В.1								
18	Задание открытого типа с развернутым обоснованным ответом Инструкция: Прочитайте текст и запишите развернутый обоснованный ответ Объясните, почему специалисту важно владеть навыками применения современных технологий защиты информации. Ключ с правильным ответом (эталонный ответ): Владение современными технологиями защиты информации позволяет эффективно предотвращать угрозы, обеспечивать конфиденциальность, целостность и доступность данных. Это повышает устойчивость информационных систем, снижает риски инцидентов и обеспечивает выполнение требований безопасности в профессиональной деятельности, включая использование отечественных решений.	ОПК-2.В.1								
19	Задание закрытого типа с выбором одного правильного ответа Инструкция: Прочитайте текст и выберите один правильный ответ Какой принцип является основополагающим при обеспечении информационной безопасности?	ОПК-3.3.1								

	1. Минимизация интерфейсов 2. Принцип наименьших привилегий 3. Увеличение количества пользователей 4. Максимизация сетевой доступности Ключ с правильным ответом: 2									
20	Задание закрытого типа с выбором нескольких правильных ответов Инструкция: Прочитайте текст и выберите все правильные ответы Какие методы относятся к решению стандартных задач информационной безопасности? 1. Контроль целостности 2. Аутентификация 3. Шифрование 4. Изменение цветовой схемы интерфейса Ключ с правильным ответом: 1, 2, 3	ОПК-3.3.1								
21	Задание закрытого типа на установление соответствия Инструкция: Прочитайте текст и установите соответствие Сопоставьте метод и его назначение. <table><tr><td>Метод</td><td>Назначение</td></tr><tr><td>А. Хэширование</td><td>1. Контроль целостности данных</td></tr><tr><td>Б. Двухфакторная аутентификация</td><td>2. Повышение надёжности идентификации</td></tr><tr><td>В. Шифрование</td><td>3. Защита конфиденциальности информации</td></tr></table> Ключ с правильным ответом: А1, Б2, В3	Метод	Назначение	А. Хэширование	1. Контроль целостности данных	Б. Двухфакторная аутентификация	2. Повышение надёжности идентификации	В. Шифрование	3. Защита конфиденциальности информации	ОПК-3.3.1
Метод	Назначение									
А. Хэширование	1. Контроль целостности данных									
Б. Двухфакторная аутентификация	2. Повышение надёжности идентификации									
В. Шифрование	3. Защита конфиденциальности информации									
22	Задание закрытого типа на установление правильной последовательности Инструкция: Прочитайте текст и установите последовательность Этапы решения стандартной задачи информационной безопасности: 1. Анализ угроз 2. Выбор методов защиты 3. Реализация выбранных средств 4. Тестирование эффективности 5. Документирование результатов Запишите последовательность цифр слева направо. Ключ с правильным ответом: 1, 2, 3, 4, 5	ОПК-3.3.1								
23	Задание открытого типа Инструкция: Прочитайте текст и запишите ответ. Как называется процесс подтверждения подлинности пользователя или системы? Ключ с правильным ответом: аутентификация	ОПК-3.3.1								
24	Задание открытого типа с развернутым обоснованным ответом Инструкция: Прочитайте текст и запишите развернутый обоснованный ответ Объясните, почему важно учитывать требования информационной безопасности при использовании информационно-коммуникационных технологий. Ключ с правильным ответом (эталонный ответ): Учет требований информационной безопасности позволяет обеспечить конфиденциальность, целостность и доступность данных при использовании информационно-коммуникационных технологий. Это снижает риски утечек, несанкционированного доступа и нарушений работы систем, а также обеспечивает корректное и безопасное решение профессиональных задач, включая применение	ОПК-3.3.1								

	интеллектуальных технологий.									
25	Задание закрытого типа с выбором одного правильного ответа Инструкция: Прочитайте текст и выберите один правильный ответ Какой инструмент ИКТ чаще всего используется для поиска научной информации с учётом требований информационной безопасности? 1. Социальные сети 2. Научные электронные библиотеки 3. Развлекательные порталы 4. Форумы Ключ с правильным ответом: 2	ОПК-3.У.1								
26	Задание закрытого типа с выбором нескольких правильных ответов Инструкция: Прочитайте текст и выберите все правильные ответы Какие действия относятся к решению стандартных задач с применением ИКТ и ИБ? 1. Поиск достоверных источников 2. Проверка целостности данных 3. Использование ИИ для анализа информации 4. Изменение темы рабочего стола Ключ с правильным ответом: 1, 2, 3	ОПК-3.У.1								
27	Задание закрытого типа на установление соответствия Инструкция: Прочитайте текст и установите соответствие Сопоставьте инструмент и его назначение. <table><tr><td>Инструмент</td><td>Назначение</td></tr><tr><td>А. Антиплагиат-система</td><td>1. Проверка оригинальности текста</td></tr><tr><td>Б. ИИ-модель анализа данных</td><td>2. Обработка и интерпретация информации</td></tr><tr><td>В. VPN-клиент</td><td>3. Защита сетевого соединения</td></tr></table> Ключ с правильным ответом: А1, Б2, В3	Инструмент	Назначение	А. Антиплагиат-система	1. Проверка оригинальности текста	Б. ИИ-модель анализа данных	2. Обработка и интерпретация информации	В. VPN-клиент	3. Защита сетевого соединения	ОПК-3.У.1
Инструмент	Назначение									
А. Антиплагиат-система	1. Проверка оригинальности текста									
Б. ИИ-модель анализа данных	2. Обработка и интерпретация информации									
В. VPN-клиент	3. Защита сетевого соединения									
28	Задание закрытого типа на установление правильной последовательности Инструкция: Прочитайте текст и установите последовательность Этапы решения стандартной задачи с применением ИКТ и ИБ: 1. Формулирование задачи 2. Поиск и отбор достоверных источников 3. Анализ информации (в том числе с применением ИИ) 4. Проверка соблюдения требований ИБ 5. Подготовка результата Запишите последовательность цифр слева направо. Ключ с правильным ответом: 1, 2, 3, 4, 5	ОПК-3.У.1								
29	Задание открытого типа Инструкция: Прочитайте текст и запишите ответ. Как называется процесс проверки достоверности и корректности найденной информации? Ключ с правильным ответом: верификация	ОПК-3.У.1								
30	Задание открытого типа с развернутым обоснованным ответом Инструкция: Прочитайте текст и запишите развернутый обоснованный ответ Объясните, почему важно учитывать требования информационной безопасности при использовании ИКТ и искусственного интеллекта. Ключ с правильным ответом (эталонный ответ): Учет требований	ОПК-3.У.1								

	информационной безопасности позволяет защитить данные от утечек, подделки и несанкционированного доступа при использовании ИКТ и ИИ. Это обеспечивает корректность анализа, достоверность результатов и безопасное выполнение профессиональных задач. Соблюдение ИБ особенно важно при работе с конфиденциальной информацией и автоматизированными системами обработки данных.									
31	Задание закрытого типа с выбором одного правильного ответа Инструкция: Прочитайте текст и выберите один правильный ответ Какой элемент обязательно должен присутствовать в научной аннотации? 1. Иллюстрации 2. Краткое содержание работы 3. Полный текст исследования 4. Список всех использованных источников Ключ с правильным ответом: 2	ОПК-3.В.1								
32	Задание закрытого типа с выбором нескольких правильных ответов Инструкция: Прочитайте текст и выберите все правильные ответы Какие требования информационной безопасности необходимо учитывать при подготовке научных материалов? 1. Недопущение раскрытия конфиденциальных данных 2. Корректное цитирование источников 3. Проверка оригинальности текста 4. Изменение цветовой схемы документа Ключ с правильным ответом: 1, 2, 3	ОПК-3.В.1								
33	Задание закрытого типа на установление соответствия Инструкция: Прочитайте текст и установите соответствие Сопоставьте элемент научной работы и его назначение. <table><tr><td>Элемент</td><td>Назначение</td></tr><tr><td>А. Обзор литературы</td><td>1. Анализ существующих исследований</td></tr><tr><td>Б. Библиография</td><td>2. Перечень использованных источников</td></tr><tr><td>В. Аннотация</td><td>3. Краткое описание содержания работы</td></tr></table> Ключ с правильным ответом: А1, Б2, В3	Элемент	Назначение	А. Обзор литературы	1. Анализ существующих исследований	Б. Библиография	2. Перечень использованных источников	В. Аннотация	3. Краткое описание содержания работы	ОПК-3.В.1
Элемент	Назначение									
А. Обзор литературы	1. Анализ существующих исследований									
Б. Библиография	2. Перечень использованных источников									
В. Аннотация	3. Краткое описание содержания работы									
34	Задание закрытого типа на установление правильной последовательности Инструкция: Прочитайте текст и установите последовательность Этапы подготовки научного обзора: 1. Поиск источников 2. Отбор релевантных материалов 3. Анализ содержания 4. Формирование структуры обзора 5. Подготовка итогового текста Запишите последовательность цифр слева направо. Ключ с правильным ответом: 1, 2, 3, 4, 5	ОПК-3.В.1								
35	Задание открытого типа Инструкция: Прочитайте текст и запишите ответ. Как называется список использованных источников, оформленный по установленным правилам? Ключ с правильным ответом: библиография	ОПК-3.В.1								
36	Задание открытого типа с развернутым обоснованным ответом Инструкция: Прочитайте текст и запишите развернутый обоснованный ответ	ОПК-3.В.1								

	Объясните, почему важно учитывать требования информационной безопасности при подготовке научных материалов. Ключ с правильным ответом (эталонный ответ): Учет требований информационной безопасности позволяет избежать раскрытия конфиденциальных данных, защитить результаты исследований и обеспечить корректное использование источников. Это повышает достоверность научной работы, предотвращает нарушения авторских прав и способствует безопасному распространению научной информации.									
37	Задание закрытого типа с выбором одного правильного ответа Инструкция: Прочитайте текст и выберите один правильный ответ Какой язык программирования чаще всего используется для реализации криптографических алгоритмов? 1. HTML 2. Python 3. CSS 4. Markdown Ключ с правильным ответом: 2	ОПК-8.3.1								
38	Задание закрытого типа с выбором нескольких правильных ответов Инструкция: Прочитайте текст и выберите все правильные ответы Какие среды разработки подходят для разработки программных средств защиты информации? 1. Visual Studio Code 2. PyCharm 3. IntelliJ IDEA 4. Code V Ключ с правильным ответом: 1, 2, 3	ОПК-8.3.1								
39	Задание закрытого типа на установление соответствия Инструкция: Прочитайте текст и установите соответствие Сопоставьте инструмент и его назначение. <table><tr><td>Инструмент</td><td>Назначение</td></tr><tr><td>А. OpenSSL</td><td>1. Реализация криптографических операций</td></tr><tr><td>Б. Linux</td><td>2. ОС с развитой системой безопасности</td></tr><tr><td>В. Python</td><td>3. Язык для разработки криптографических модулей</td></tr></table> Ключ с правильным ответом: А1, Б2, В3	Инструмент	Назначение	А. OpenSSL	1. Реализация криптографических операций	Б. Linux	2. ОС с развитой системой безопасности	В. Python	3. Язык для разработки криптографических модулей	ОПК-8.3.1
Инструмент	Назначение									
А. OpenSSL	1. Реализация криптографических операций									
Б. Linux	2. ОС с развитой системой безопасности									
В. Python	3. Язык для разработки криптографических модулей									
40	Задание закрытого типа на установление правильной последовательности Инструкция: Прочитайте текст и установите последовательность Этапы разработки криптографического модуля: 1. Выбор алгоритма 2. Проектирование структуры программы 3. Реализация кода 4. Тестирование корректности 5. Документирование Запишите последовательность цифр слева направо. Ключ с правильным ответом: 1, 2, 3, 4, 5	ОПК-8.3.1								
41	Задание открытого типа Инструкция: Прочитайте текст и запишите ответ. Как называется программа, обеспечивающая взаимодействие пользователя с операционной системой? Ключ с правильным ответом: оболочка	ОПК-8.3.1								

42	Задание открытого типа с развернутым обоснованным ответом Инструкция: Прочитайте текст и запишите развернутый обоснованный ответ Объясните, почему знание языков программирования важно при разработке средств защиты информации. Ключ с правильным ответом (эталонный ответ): Знание языков программирования позволяет разрабатывать, анализировать и модифицировать криптографические алгоритмы и средства защиты информации. Это обеспечивает возможность создания безопасных приложений, реализации протоколов шифрования, проверки корректности алгоритмов и адаптации программных решений под требования информационной безопасности.	ОПК-8.3.1								
43	Задание закрытого типа с выбором одного правильного ответа Инструкция: Прочитайте текст и выберите один правильный ответ Какой этап разработки криптографической программы выполняется сразу после составления алгоритма? 1. Тестирование 2. Написание кода 3. Документирование 4. Анализ угроз Ключ с правильным ответом: 2	ОПК-8.У.1								
44	Задание закрытого типа с выбором нескольких правильных ответов Инструкция: Прочитайте текст и выберите все правильные ответы Какие действия относятся к отладке криптографического модуля? 1. Проверка корректности реализации математических операций 2. Анализ промежуточных значений 3. Поиск ошибок в логике алгоритма 4. Изменение цветовой темы IDE Ключ с правильным ответом: 1, 2, 3	ОПК-8.У.1								
45	Задание закрытого типа на установление соответствия Инструкция: Прочитайте текст и установите соответствие Сопоставьте этап разработки и его назначение. <table><tr><td>Этап</td><td>Назначение</td></tr><tr><td>А. Составление алгоритма</td><td>1. Определение логики криптографического преобразования</td></tr><tr><td>Б. Реализация кода</td><td>2. Программная реализация алгоритма</td></tr><tr><td>В. Интеграция модулей</td><td>3. Объединение криптографических функций в систему</td></tr></table> Ключ с правильным ответом: А1, Б2, В3	Этап	Назначение	А. Составление алгоритма	1. Определение логики криптографического преобразования	Б. Реализация кода	2. Программная реализация алгоритма	В. Интеграция модулей	3. Объединение криптографических функций в систему	ОПК-8.У.1
Этап	Назначение									
А. Составление алгоритма	1. Определение логики криптографического преобразования									
Б. Реализация кода	2. Программная реализация алгоритма									
В. Интеграция модулей	3. Объединение криптографических функций в систему									
46	Задание закрытого типа на установление правильной последовательности Инструкция: Прочитайте текст и установите последовательность Этапы разработки криптографического программного модуля: 1. Постановка задачи 2. Разработка алгоритма 3. Реализация кода 4. Отладка 5. Тестирование стойкости Запишите последовательность цифр слева направо. Ключ с правильным ответом: 1, 2, 3, 4, 5	ОПК-8.У.1								
47	Задание открытого типа	ОПК-8.У.1								

	Инструкция: Прочитайте текст и запишите ответ. Как называется процесс объединения нескольких программных компонентов в единое приложение? Ключ с правильным ответом: интеграция									
48	Задание открытого типа с развернутым обоснованным ответом Инструкция: Прочитайте текст и запишите развернутый обоснованный ответ Объясните, почему важно уметь составлять алгоритмы перед реализацией криптографической программы. Ключ с правильным ответом (эталонный ответ): Составление алгоритма позволяет заранее определить структуру криптографического преобразования, выявить возможные ошибки и обеспечить корректность математических операций. Это ускоряет разработку, повышает безопасность реализации, облегчает отладку и гарантирует правильную интеграцию криптографических модулей в программную систему.	ОПК-8.У.1								
49	Задание закрытого типа с выбором одного правильного ответа Инструкция: Прочитайте текст и выберите один правильный ответ Какой инструмент чаще всего используется для пошаговой отладки криптографических программ? 1. Текстовый редактор 2. Отладчик (debugger) 3. Графический редактор 4. Архиватор Ключ с правильным ответом: 2	ОПК-8.В.1								
50	Задание закрытого типа с выбором нескольких правильных ответов Инструкция: Прочитайте текст и выберите все правильные ответы Какие действия относятся к тестированию криптографического модуля? 1. Проверка корректности входных данных 2. Сравнение результатов с эталонными значениями 3. Анализ устойчивости к атакам 4. Изменение цветовой схемы IDE Ключ с правильным ответом: 1, 2, 3	ОПК-8.В.1								
51	Задание закрытого типа на установление соответствия Инструкция: Прочитайте текст и установите соответствие Сопоставьте тип тестирования и его назначение. <table><tr><td>Тип тестирования</td><td>Назначение</td></tr><tr><td>А. Модульное тестирование</td><td>1. Проверка отдельных функций шифрования</td></tr><tr><td>Б. Интеграционное тестирование</td><td>2. Проверка взаимодействия криптографических модулей</td></tr><tr><td>В. Системное тестирование</td><td>3. Проверка работы всей программы защиты</td></tr></table> Ключ с правильным ответом: А1, Б2, В3	Тип тестирования	Назначение	А. Модульное тестирование	1. Проверка отдельных функций шифрования	Б. Интеграционное тестирование	2. Проверка взаимодействия криптографических модулей	В. Системное тестирование	3. Проверка работы всей программы защиты	ОПК-8.В.1
Тип тестирования	Назначение									
А. Модульное тестирование	1. Проверка отдельных функций шифрования									
Б. Интеграционное тестирование	2. Проверка взаимодействия криптографических модулей									
В. Системное тестирование	3. Проверка работы всей программы защиты									
52	Задание закрытого типа на установление правильной последовательности Инструкция: Прочитайте текст и установите последовательность Этапы отладки криптографической программы: 1. Запуск программы 2. Обнаружение ошибки 3. Анализ причины	ОПК-8.В.1								

	4. Исправление кода 5. Повторное тестирование Запишите последовательность цифр слева направо. Ключ с правильным ответом: 1, 2, 3, 4, 5	
53	Задание открытого типа Инструкция: Прочитайте текст и запишите ответ. Как называется процесс поиска и исправления ошибок в программе? Ключ с правильным ответом: отладка	ОПК-8.В.1
54	Задание открытого типа с развернутым обоснованным ответом Инструкция: Прочитайте текст и запишите развернутый обоснованный ответ Объясните, почему навыки отладки и тестирования особенно важны при разработке криптографических программ. Ключ с правильным ответом (эталонный ответ): Навыки отладки и тестирования особенно важны при разработке криптографических программ, поскольку даже небольшие ошибки могут привести к снижению стойкости алгоритма и уязвимости системы. Корректная отладка обеспечивает правильность математических операций, а тестирование позволяет проверить устойчивость к атакам и соответствие требованиям безопасности. Это гарантирует надежность и защищенность программных средств.	ОПК-8.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
	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.

Структура предоставления лекционного материала:

- постановка задачи;
- основные сведения по теме лекции;
- результаты и выводы.

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

Задания и требования к проведению лабораторных работ размещаются в личном кабинете обучающегося <https://pro.guap.ru/>.

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;
- решение;
- выводы.

Требования к оформлению отчета о лабораторной работе

Общие требования и рекомендации по выполнению письменных работ : методические указания (с изменениями от 09.01.2019) [Электронный ресурс] / Ивановгородский филиал С.-Петерб. гос. ун-т аэрокосм. приборостроения ; сост. А. А.

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.

В процессе выполнения самостоятельной работы у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет ему развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Основными методическими материалами, направляющими самостоятельную работу обучающихся, являются источники из перечня печатных и электронных учебных изданий, указанных в таблице 8. Кроме этого, обучающийся может пользоваться электронными ресурсами, указанными в таблицах 9 и 11.

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 студентов или в виде беседы в форме "ответ-вопрос".

Консультация со слабоуспевающими студентами - 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 к 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;
- контроль курсового проектирования;
- контроль выполнения курсовых работ;
- доклад на научной конференции;
- написание научной статьи.

Контроль осуществляется путем проведения опросов, проверки выполнения заданий на практических занятиях / лабораторных работах. Преподавателем осуществляется текущая оценка сформированности индикаторов ОПК-2.В.1, ОПК-2.3.1, ОПК-2.У.1, ОПК-3.В.1, ОПК-3.3.1, ОПК-3.У.1, ОПК-5.В.1, ОПК-5.У.1, ОПК-7.В.1, ОПК-7.У.1, ОПК-8.В.1, ОПК-8.3.1, ОПК-8.У.1. Даты проведения текущего контроля по указанным заданиям сообщаются обучающимся заранее. Студент должен выполнить все предусмотренные контрольные мероприятия не позднее указанного срока. Результаты текущего контроля учитываются при проведении промежуточной аттестации.

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 Таблице 14:

- менее 51 - "не зачтено" или "неудовлетворительно" (2);
- от 51 до 69 - "зачтено" или "удовлетворительно" (3);
- от 70 до 89 - "зачтено" или "хорошо" (4);
- от 90 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:

- экзамен проводится в устной форме в виде ответа на вопросы;
- экзамен проводится в письменной форме в виде теста;
- экзамен проводится с применением средств электронного обучения (СДО

ГУАП).

В случае дистанционной формы промежуточной аттестации экзамен проводится в виде теста с применением средств электронного обучения.

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