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

Кафедра № 23

УТВЕРЖДАЮ
Руководитель образовательной программы

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

В.А. Ненашев
(инициалы, фамилия)

(подпись)

«25» февраля 2026 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Обеспечение информационной безопасности в инфокоммуникациях»
(Наименование дисциплины)

Код направления подготовки/ специальности	11.04.03
Наименование направления подготовки/ специальности	Конструирование и технология электронных средств
Наименование направленности/ специализации	Проектирование и технология аэрокосмических приборов и электронных средств
Форма обучения	очная
Год приема	2026

Санкт-Петербург– 2026

Лист согласования рабочей программы дисциплины

Программу составил (а)

проф., д.т.н. _____ О.П. Куркова
(должность, уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Программа одобрена на заседании кафедры № 23
«16» февраля 2026 г, протокол №7/26

Заведующий кафедрой № 23

д.т.н.,проф. _____ А.Р. Бестугин
(уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Заместитель директора института №2 по методической работе

доц.,к.т.н.,доц. _____ Н.В. Марковская
(должность, уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Аннотация

Дисциплина «Обеспечение информационной безопасности в инфокоммуникациях» входит в образовательную программу высшего образования – программу магистратуры по направлению подготовки/ специальности 11.04.03 «Конструирование и технология электронных средств» направленности/специализации «Проектирование и технология аэрокосмических приборов и электронных средств». Дисциплина реализуется кафедрой «№23».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

УК-4 «Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия»

ОПК-3 «Способен приобретать и использовать новую информацию в своей предметной области, предлагать новые идеи и подходы к решению инженерных задач»

ОПК-4 «Способен разрабатывать и применять специализированное программно-математическое обеспечение для проведения исследований и решения инженерных задач»

Содержание дисциплины охватывает круг вопросов, связанных с обеспечением информационной безопасности в инфокоммуникациях при проектировании и эксплуатации электронных аппаратно-программных средств и систем.

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

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме дифференцированного зачета (1 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 преподавания дисциплины внедрение интегративного подхода в образовательную среду программы подготовки магистрантов по специальности 11.04.03 «Конструирование и технология электронных средств»;

– получение обучающимися системных знаний в области обеспечения информационной безопасности в инфокоммуникациях;

– предоставление обучающимся возможности развить системный подход к решению задач создания и эксплуатации инфокоммуникационных систем на базе аппаратно-программных электронных средств для аэрокосмической техники различного назначения;

– получение обучающимися знаний и предоставление обучающимся возможности развития умений и навыков в части формирования и реализации требований по обеспечению информационной безопасности при создании и эксплуатации инфокоммуникационных систем на базе аппаратно-программных электронных средств для аэрокосмической техники, анализа и оценки информационной безопасности инфокоммуникационных систем в соответствии с требованиями, установленными нормативной документацией;

– создание поддерживающей образовательной среды преподавания по программе подготовки магистрантов специальности 11.04.03 «Конструирование и технология электронных средств» с применением современных методов и инструментов моделирования профиля безопасности инфокоммуникационных систем на базе аппаратно-программных электронных средств.

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
Универсальные компетенции	УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.З.2 знать современные технологии, обеспечивающие коммуникацию и кооперацию в цифровой среде УК-4.У.1 уметь применять на практике технологии коммуникации и кооперации для академического и профессионального взаимодействия, в том числе в цифровой среде, для достижения поставленных целей
Общепрофессиональные компетенции	ОПК-3 Способен приобретать и использовать новую информацию в своей предметной области, предлагать новые идеи и подходы к решению	ОПК-3.З.1 знать принципы построения локальных и глобальных компьютерных сетей, основы Интернет-технологий, типовые процедуры применения проблемно-ориентированных прикладных программных средств в дисциплинах профессионального цикла и профессиональной сфере деятельности

	инженерных задач	
Общепрофессиональные компетенции	ОПК-4 Способен разрабатывать и применять специализированное программно-математическое обеспечение для проведения исследований и решения инженерных задач	ОПК-4.З.1 знать методы расчета, проектирования, конструирования и модернизации электронных средств с использованием систем автоматизированного проектирования и компьютерных средств, в том числе с использованием искусственного интеллекта ОПК-4.У.1 уметь осуществлять выбор наиболее оптимальных прикладных программных пакетов для решения соответствующих задач научной и образовательной деятельности, в том числе с использованием искусственного интеллекта ОПК-4.В.1 владеть современными программными средствами (CAD) моделирования, оптимального проектирования и конструирования приборов, схем и электронных устройств различного функционального назначения

2. Место дисциплины в структуре ОП

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

– «Интегрированные производственные системы и ИПИ-технологии»;

– «Коммерциализация результатов научных исследований и разработок».

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

– «Конструирование ЭС аэрокосмических систем и комплексов»;

– «Моделирование конструкций и технологий электронных средств»;

– «Планирование и организация научных исследований и опытно-конструкторских работ».

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
		№1
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)		
Самостоятельная работа, всего (час)	57	57
***Вид промежуточной аттестации*:** зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.)	Дифф. зач.,	Дифф. зач.,

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий. Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 1					
Раздел 1. Введение в курс. Основные положения Тема 1.1. Объект и цели защиты Тема 1.2. Основные характеристики информации: доступность, целостность, конфиденциальность. Тема 1.3. Системное представление инфокоммуникации. Парадигма информационной безопасности. Тема 1.4. Виды и источники угроз Тема 1.5. Уязвимость инфокоммуникационных систем	2	0	0	0	4
Раздел 2. Виды воздействий, создающих угрозы безопасности Тема 2.1. Объективные внутренние факторы Тема 2.2. Объективные внешние факторы Тема 2.3. Субъективные внутренние факторы Тема 2.4. Субъективные внешние факторы	4	0	0	0	4
Раздел 3. Требования и критерии информационной безопасности Тема 3.1. Общий подход к формированию требований и оценке безопасности, определенный международной и национальной нормативной документацией Тема 3.2. Общая модель критериев безопасности Тема 3.3. Последовательность выполнения разработки инфокоммуникационных систем на базе аппаратно-программных электронных средств с учетом реализации требований информационной безопасности Тема 3.4. Последовательность процесса оценки информационной безопасности инфокоммуникационных систем Тема 3.5. Последовательность формирования требований и Спецификаций безопасности при разработке Заданий по безопасности и Профиля защиты. Политика безопасности при создании инфокоммуникационной системы. Тема 3.6. Общая организационная структура Требований безопасности	6	0	4	0	8

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Раздел 4. Функциональные требования безопасности Тема 4.1. Парадигма функциональных требований. Типы данных Тема 4.2. Структура построения функциональных требований безопасности. Класс требований. Семейство требований. Компонент требований. Тема 4.3. Каталог требований. Принципы обозначений требований при разработке Заданий и Спецификаций безопасности, Профиля защиты. Тема 4.4. Характеристики, иерархия и взаимосвязь основных Семейств функциональных требований безопасности. Ранжирование компонентов. Наборы действий и функций.	6	0	4	0	8
Раздел 5. Требования доверия к безопасности Тема 5.1. Парадигма требований доверия. Методы и способы оценки доверия. Шкала оценки доверия. Тема 5.2. Иерархическая структура требований доверия безопасности. Принципы обозначений требований доверия. Тема 5.3 Основные Классы и Семейства требований доверия. Тема 5.4. Элементы требований доверия. Действия Разработчика. Действия Оценщика.	4		4		8
Раздел 6. Защита информации Тема 6.1. Виды защиты информации Тема 6.2. Выбор методов защиты Тема 6.3. Техника защиты информации Тема 6.4. Основные типы моделей безопасности компьютерных систем	4		5		16
Раздел 7. Автоматизированные системы в защищенном исполнении. Тема 7.1. Общие положения о защищенном исполнении автоматизированных систем Тема 7.2. Порядок создания автоматизированных систем в защищенном исполнении	4				4
Раздел 8. Основы защиты открытых систем в соответствии с требованиями ISO/IEC 10181 и ISO/IEC 11181 Тема 8.1 Обзор схем обеспечения безопасности для открытых систем. Тема 8.2. Основы и схемы обеспечения аутентификации. Тема 8.3. Основы и структура системы контроля доступа. Тема 8.4. Основы обеспечения невозможности отказа партнеров по связи от факта передачи или приема сообщений. Тема 8.5. Основы и структура обеспечения конфиденциальности. Тема 8.6. Основы и структура обеспечения целостности. Тема 8.7. Основы контроля защиты и сигналов	4				5

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
о нарушении безопасности. Схема проверки безопасности и сигналы тревоги.					
Итого в семестре:	34	0	17	0	57
Итого	**34**	**0**	**17**	**0**	**57**

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	**Введение в курс. Основные положения** Объект и цели защиты. Основные характеристики информации: доступность, целостность, конфиденциальность. Системное представление инфокоммуникации. Парадигма информационной безопасности. Виды и источники угроз. Уязвимость инфокоммуникационных систем.
2	**Виды воздействий, создающих угрозы безопасности** Объективные внутренние факторы Объективные внешние факторы Субъективные внутренние факторы Субъективные внешние факторы
3	**Требования и критерии информационной безопасности** Общий подход к формированию требований и оценке безопасности, определенный международной и национальной нормативной документацией. Общая модель критериев безопасности. Последовательность выполнения разработки инфокоммуникационных систем на базе аппаратно-программных электронных средств с учетом реализации требований информационной безопасности. Последовательность процесса оценки информационной безопасности инфокоммуникационных систем. Последовательность формирования требований и Спецификаций безопасности при разработке Заданий по безопасности и Профиля защиты. Политика безопасности при создании инфокоммуникационной системы. Общая организационная структура Требований безопасности.
4	**Функциональные требования безопасности** Парадигма функциональных требований. Типы данных. Структура построения функциональных требований безопасности. Класс требований. Семейство требований. Компонент требований. Каталог требований. Принципы обозначений требований при разработке Заданий и Спецификаций безопасности, Профиля защиты. Характеристики, иерархия и взаимосвязь основных Семейств функциональных требований безопасности. Ранжирование компонентов. Наборы действий и функций.

Номер раздела	Название и содержание разделов и тем лекционных занятий
5	**Требования доверия к безопасности** Парадигма требований доверия. Методы и способы оценки доверия. Шкала оценки доверия. Иерархическая структура требований доверия безопасности. Принципы обозначений требований доверия. Основные Классы и Семейства требований доверия. Элементы требований доверия. Действия Разработчика. Действия Оценщика.
6	**Защита информации** Виды защиты информации. Выбор методов защиты. Техника защиты информации. Основные типы моделей безопасности компьютерных систем
7	**Автоматизированные системы в защищенном исполнении.** Общие положения о защищенном исполнении автоматизированных систем. Порядок создания автоматизированных систем в защищенном исполнении.
8	**Основы защиты открытых систем в соответствии с требованиями ISO/IEC 10181 и ISO/IEC 11181** Обзор схем обеспечения безопасности для открытых систем. Основы и схемы обеспечения аутентификации. Основы и структура системы контроля доступа. Основы обеспечения невозможности отказа партнеров по связи от факта передачи или приема сообщений. Основы и структура обеспечения конфиденциальности. Основы и структура обеспечения целостности. Основы контроля защиты и сигналов о нарушении безопасности. Схема проверки безопасности и сигналы тревоги.

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 1				
1	Информационная безопасность	4		3

	информационных потоков			
2	Функциональные требования и требования доверия, предъявляемые к безопасности	8		4, 5
3	Виды и методы защиты информации. Безопасность сетей.	5		6
	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	Семестр1, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	24	24
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	6	6
Домашнее задание (ДЗ)	17	17
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	10	10
Всего:	**57**	**57**

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)
Библиотека ГУАП	Макаренко С. И. Информационная безопасность: учебное пособие. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.: ил.	0

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
Библиотека ГУАП	Макаренко С. И. Информационная безопасность: учебное пособие. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.: ил.	0
Библиотека ГУАП	Макаренко С. И. Аудит безопасности критической информационными воздействиями. Монография. – СПб.: Наукоемкие технологии, 2018 – 122 с.	0
Библиотека ГУАП	Макаренко С. И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки Монография. – СПб.: Наукоемкие технологии, 2020. – 337 с.	0
Библиотека ГУАП	Макаренко С. И., Иванов М.С. Сетецентрическая война – принципы, технологии, примеры и перспективы. Монография. – СПб.: Наукоемкие технологии, 2018. – 898 с	0
Библиотека ГУАП	Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. — СПб.: Наукоемкие технологии, 2017. — 546 с.	0
Библиотека ГУАП	Н.А. Богульская, М.М. Кучеров. Модели безопасности компьютерных систем/Учебное пособие – Красноярск: Сиб. федер. ун-т, 2019. – 206 с.	0
Библиотека ГУАП	О.В. Казарин. Безопасность программного обеспечения компьютерных систем. Монография. – М.: МГУЛ, 2003. – 212 с.	0

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://pro.guap.ru/	Элементы электронного курса по дисциплине[1] размещены внутри ЭИОС ГУАП «Интегрированная среда обучения»

[1] Разработчик может перечислить конкретные элементы электронного курса, например: задания для подготовки к занятиям, методические рекомендации для самостоятельной подготовки, учебно-методические

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	*Электронная информационно-образовательная среда ГУАП «Интегрированная среда обучения» (https://pro.guap.ru/) разработана сотрудниками ГУАП (введена в эксплуатацию приказом ГУАП от 06.06.2017 № 05-215/17), перечень модулей и их функциональное назначение изложены по ссылке https://guap.ru/it/system/iso*
2	*Официальный сайт образовательной организации в сети «Интернет» (https://guap.ru/), разработан сотрудниками ГУАП (введен в эксплуатацию Приказом ГУАП от 23.03.2023 № 05-145/23)*
3	*LibreOffice 5 (Лицензия LGPLv3)*
4	*Microsoft Office 2019 (договор ГУАП, информация о лицензии представлена по ссылке https://guap.ru/it/system/iso/po)*
5	*MozillaFirefox(лицензии GPL/LGPL/MPL)*

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

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
1	*Электронный каталог библиотеки ГУАП с доступом к базе полнотекстовых изданий (https://lib.guap.ru.), доступ через личный кабинет читателя библиотеки ГУАП*
2	*Научная электронная библиотека «eLIBRARY» (https://elibrary.ru/), доступ через личный кабинет читателя библиотеки ГУАП, а также по IP -адресам ГУАП*
3	*ЭБС «Лань» (https://e.lanbook.com/), доступ через личный кабинет читателя библиотеки ГУАП, а также по IP -адресам ГУАП*
4	*ЭБС Консорциума аэрокосмических вузов России (http://elsau.ru/ suai), доступ по IP-адресам ГУАП*
5	*ЭБС Znanium (https://znanium.ru/), доступ через личный кабинет читателя библиотеки ГУАП, а также по IP -адресам ГУАП*
6	*образовательая платформа «Юрайт» (https://urait.ru/), доступ через личный кабинет читателя библиотеки ГУАП, а также по IP -адресам ГУАП*
7	*Научная электронная библиотека «КиберЛенинка» (https://cyberleninka.ru/), свободный доступ*

9. Материально-техническая база

материалы по темам, мультимедийные презентации по темам, извлечения из нормативно-правовых актов и т.п.

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	Мультимедийная лекционная аудитория	14-06Г (ул. Большая Морская, д.67, лит. А)
2	Класс для групповых дискуссий	51-06-03 (ул. Большая Морская, д.67, лит. А)
3	Помещение для самостоятельной работы обучающихся - Читальный зал библиотеки ГУАП: специализированная мебель; персональные компьютеры – 10 шт., обеспечен доступ в электронную информационно-образовательную среду ГУАП по локальной вычислительной сети и точке доступа WiFi, а также к электронно-библиотечным системам, реферативной базе данных Scopus; копировальный аппарат Kyocera KM2035.	22-19 (ул. Большая Морская, д.67, лит. А)

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
Дифференцированный зачёт	Список вопросов; Тесты; Задачи.

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**.

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«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
	Учебным планом не предусмотрено	

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

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

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
1	Что является объектом защиты при реализации информационной безопасности?	УК-4.3.2 ОПК-3.3.1
2	Что является основными характеристиками информации?	УК-4.3.2 ОПК-3.3.1
3	В чем суть парадигмы информационной безопасности?	УК-4.3.2 ОПК-3.3.1
4	Что подразумевается под «угрозой» информационной безопасности?	УК-4.3.2 ОПК-3.3.1
5	В чем состоит уязвимость инфокоммуникационной системы?	УК-4.3.2 ОПК-3.3.1
6	Какие воздействующие факторы могут составлять угрозу для информационной безопасности инфокоммуникационной системы?	УК-4.3.2 ОПК-3.3.1
7	Что представляет собой модель критериев информационной безопасности? Какие виды требований предъявляются к объектам защиты для обеспечения информационной безопасности?	УК-4.3.2 ОПК-3.3.1 ОПК-4.3.1

8	В какой последовательности необходимо выполнять разработки инфокоммуникационных систем на базе аппаратно-программных электронных средств с учетом реализации требований информационной безопасности?	УК-4.З.2 ОПК-3.З.1 УК-4.У.1
9	В какой последовательности необходимо осуществлять процесс оценки информационной безопасности инфокоммуникационных систем?	УК-4.З.2 ОПК-3.З.1 УК-4.У.1
10	В соответствии с какой структурной иерархией должны формироваться требований безопасности?	УК-4.З.2 ОПК-3.З.1 УК-4.У.1
11	В чем суть парадигмы функциональных требований информационной безопасности?	УК-4.З.2 ОПК-3.З.1
12	В соответствии с какой иерархической структурой формируются функциональные требования безопасности?	УК-4.З.2 ОПК-3.З.1 ОПК-4.З.1 ОПК-4.У.1 ОПК-4.В.1
13	Что является основными характеристиками основных Семейств функциональных требований безопасности?	УК-4.З.2 ОПК-3.З.1
14	Какие Классы, Семейства и Компоненты функциональных требований предусмотрены Каталогом? Расскажите об одном из вариантов.	УК-4.З.2 ОПК-3.З.1 УК-4.У.1
15	В чем суть парадигмы требований доверия?	УК-4.З.2 ОПК-3.З.1
16	В соответствии с какой иерархической структурой формируются требования доверия?	УК-4.З.2 ОПК-3.З.1 ОПК-4.З.1 ОПК-4.У.1 ОПК-4.В.1
17	Какие Классы, Семейства и Компоненты требований доверия предусмотрены Каталогом? Расскажите об одном из вариантов.	УК-4.З.2 ОПК-3.З.1
18	Какие существуют виды защиты информации? По какому принципу осуществляется выбор методов защиты?	УК-4.З.2 ОПК-3.З.1
19	Что подразумевается под защищенном исполнении автоматизированных систем?	УК-4.З.2 ОПК-3.З.1 ОПК-4.У.1 ОПК-4.В.1
20	В каком порядке должны осуществляться работы по созданию автоматизированных систем в защищенном исполнении? Чем определяется этот порядок?	УК-4.З.2 ОПК-3.З.1 ОПК-4.З.1 УК-4.У.1 ОПК-4.У.1 ОПК-4.В.1
21	Что подразумевается под «открытой» системой? В чем особенность обеспечения безопасности для открытых систем? Какие существуют типовые схемы обеспечения безопасности для открытых систем?	УК-4.З.2 ОПК-3.З.1 ОПК-4.З.1 УК-4.У.1
22	Как обеспечивается аутентификация в открытых системах?	УК-4.З.2 ОПК-3.З.1
23	Как строятся подсистемы контроля доступа в рамках открытых систем?	УК-4.З.2 ОПК-3.З.1
24	Как обеспечивается невозможность отказа партнеров по связи от факта передачи или приема сообщений?	УК-4.З.2 ОПК-3.З.1
25	Как обеспечивается конфиденциальность информации в открытых системах?	УК-4.З.2 ОПК-3.З.1 УК-4.У.1
26	Как обеспечивается целостность информации в открытых системах?	УК-4.З.2 ОПК-3.З.1

27	Как осуществляется контроль защиты и сигналов о нарушении безопасности?	УК-4.З.2 ОПК-3.З.1 УК-4.У.1

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	**Инструкция. Прочитайте задание и выберите один правильный ответ.** Является ли применение метода «мозговой штурм» при организации научной дискуссии примером использования коммуникативных технологий для профессионального взаимодействия? A) Является B) Не является	УК-4.З.2
2	**Инструкция. Прочитайте задание и выберите один или несколько правильных ответов.** Какие средства могут использоваться в качестве каналов профессиональной коммуникации? A) Личный контакт между людьми B) Публичное выступление C) Компьютерные сети D) Публикации в средствах массовой информации E) Аппаратные каналы связи: телефон, факс	УК-4.З.2
3	**Инструкция. Прочитайте задание и расположите варианты ответа в правильной последовательности.** Расположите этапы проведения патентно-информационного поиска в правильной последовательности: A) Определение предмета и области поиска B) Выбор индексов международной патентной классификации и глубины поиска C) Поиск по российским и зарубежным базам данных D) Анализ и систематизация патентных документов E) Формирование выводов по результатам поиска	УК-4.У.1
4	**Инструкция. Прочитайте задание и дайте свой развернутый вариант ответа.** Опишите не менее трех приемов взаимодействия сторон, используемых в современных коммуникативных технологиях академического и профессионального общения.	УК-4.У.1

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
5	**Инструкция. Прочитайте задание и выберите один правильный ответ.** На каком этапе должно приниматься решение о запрете передачи информации через определенные коммутируемые линии связи? A) При определении контролируемых зон B) При анализе структуры безопасности C) При формировании политики безопасности D) При распределении задач по выбору защитных мер	ОПК-3.З.1
6	**Инструкция. Прочитайте задание и выберите один или несколько правильных ответов.** Какие задачи необходимо решить при разработке сетевой безопасности? A) Анализ сетевой структуры и способов ее применения B) Идентификация типов и характеристик сетевых соединений C) Анализ сетевых доверительных отношений D) Идентификация потенциально контролируемых зон E) Сокращение числа пользователей независимо от их полномочий	ОПК-3.З.1
7	**Инструкция. Прочитайте задание и выберите один правильный ответ.** Какой криптографический режим преобразования используется для проверки целостности информации? A) Гаммирование B) Поразрядное суммирование C) Формирование имитовставки D) Архивирование	ОПК-4.З.1
8	**Инструкция. Прочитайте задание и выберите один или несколько правильных ответов.** К каким видам защитных мер может относиться алгоритм формирования вектора признаков для биометрического распознавания пользователя? A) Управление доступом пользователя к технической системе B) Специальная защита C) Логическое управление и аудит доступа D) Защита от злонамеренного кода	ОПК-4.З.1
9	**Инструкция. Прочитайте задание и расположите варианты ответа в правильной последовательности.** Расположите этапы процесса управления криптографическими ключами в логической последовательности: A) Генерирование и регистрация ключей B) Сертификация и распределение ключей C) Установка и хранение ключей D) Архивирование и отмена ключей E) Извлечение и уничтожение ключей	ОПК-4.У.1
10	**Инструкция. Прочитайте задание и дайте свой развернутый вариант ответа.** Опишите порядок выбора и применения программно-математических средств для решения задачи контроля целостности и защиты информации в инфокоммуникационной системе.	ОПК-4.У.1

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
11	**Инструкция. Прочитайте текст и установите соответствие. К каждой позиции в левом столбце подберите соответствующую позицию в правом столбце.** Установите соответствие между видом злонамеренного программного кода и принципом его действия: A) Вирус — 1) Присоединяется к другим программным модулям и копирует себя в программные файлы B) Троянский конь — 2) Содержит скрытую функцию для получения и передачи данных злоумышленнику C) Червь — 3) Самостоятельно распространяется по сети и использует ресурсы системы D) Зомби — 4) Использует зараженный компьютер для выполнения удаленных команд и сетевых атак Запишите выбранные цифры под соответствующими буквами.	ОПК-4.В.1
12	**Инструкция. Прочитайте задание и дайте свой развернутый вариант ответа.** Опишите принцип действия антивирусных программ типа «сканер», а также укажите их основные ограничения и недостатки.	ОПК-4.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:

1 часть. Введение;

2 часть. Изложение содержания (основная часть раздела/темы);

3 часть. Заключение;

4 часть. Интерактивная часть, *включающая:*

– ответы на вопросы обучающихся;

– краткая дискуссия по теме;

– творческое домашнее задание для самостоятельной работы.

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

В рамках выполнения лабораторных работ обучающийся должен выполнить задания по решению одного из вариантов задач, соответствующих тематикам разделов 3, 4, 5, 6 лекционных занятий. Примеры заданий для выполнения лабораторных работ приведены в таблице 20.

Задания могут выполняться обучающимися с использованием персональной компьютерной техники.

Таблица 20 – Примеры заданий для выполнения лабораторных работ

№ п/п	Примерный перечень лабораторных заданий
1	**Примеры варианта задания по разделу 3:**

№ п/п	Примерный перечень лабораторных заданий
1.1	*Лабораторная работа №1.* ***Информационная безопасность информационных потоков*** *Цель:* изучение свойств информации и получение навыков анализа вероятности их нарушения в информационных потоках *Материалы, оборудование, программное обеспечение:* для выполнения данной лабораторной работы потребуется персональный компьютер с установленным на нем офисным пакетом Microsoft Office и доступ в сеть Интернет *Задание* *Дано:* Организационно-структурная схема объекта исследования *Требуется выполнить:* 1. Провести анализ организационно-структурной схемы объекта и определить наиболее важные информационные потоки 2. Определить возможные последствия нарушений свойств информационной безопасности (конфиденциальность, целостность, доступность информации), для выбранных информационных потоков 3. Определить критичность свойств информационной безопасности для выбранных информационных потоков 4. Определить вероятности нарушения информационной безопасности для выбранных информационных потоков 5. Определить наиболее уязвимые информационные потоки 6. Сформулировать выводы по результатам выполненной работы. 7. подготовить и оформить Отчет в электронном виде, разместить в ЛК АИС ГУАП и защитить у преподавателя
2	**Примеры вариантов задания по разделам 4 и 5:**
2.1	*Лабораторная работа №2.* ***Функциональные требования и требования доверия, предъявляемые к безопасности*** *Цель:* изучение функциональных требования и требования доверия, получение навыка формирования требований для разработки систем безопасности в соответствии с требованиями нормативной документации. *Материалы, оборудование, программное обеспечение:* для выполнения данной лабораторной работы потребуется персональный компьютер с установленным на нем офисным пакетом Microsoft Office и доступ в сеть Интернет *Задание* *Дано:* комплект нормативных документов *(ГОСТ Р ИСО/МЭК 15408-2; ГОСТ Р ИСО/МЭК 15408-3)* *Требуется выполнить:* 1. Изучить требования нормативных документов 2. Руководствуясь требованиями НД ответить на следующие вопросы: • на каком уровне формирования функциональных требований безопасности допускается осуществлять ранжирование; • на каком уровне формирования функциональных требований безопасности можно отследить взаимосвязь между Классами; • какие приемы могут применяться при проведении оценки объекта с целью повышения уровня Доверия; • в соответствии с каким Семейством требований доверия можно оценить безопасность на уровне рассмотрения аппаратных схем; • какое Семейство требований доверия необходимо предусмотреть и обеспечить, если используются функции, определенные с использованием вероятностного метода; • в соответствии с каким классом требований доверия Разработчиком должен формироваться План поддержки доверия; 3. сформулировать выводы по результатам выполненной работы. 4. подготовить и оформить Отчет в электронном виде, разместить в ЛК АИС ГУАП и защитить у преподавателя
3	**Примеры вариантов задания по разделу 6:**
3.1	*Лабораторная работа №3.* ***Виды и методы защиты информации. Безопасность сетей.*** *Цель:* изучение виды и методов защиты информации, получение навыка выбора

№ п/п	Примерный перечень лабораторных заданий
	мер защиты инфокоммуникационной системы в соответствии с требованиями нормативной документации. *Материалы, оборудование, программное обеспечение:* для выполнения данной лабораторной работы потребуется персональный компьютер с установленным на нем офисным пакетом Microsoft Office и доступ в сеть Интернет *Задание* *Дано:* комплект нормативных документов *(ГОСТ Р ИСО/МЭК 13335-4, ГОСТ Р ИСО/МЭК 13335-5)* *Требуется выполнить:* 1. Изучить требования нормативных документов 2. Руководствуясь требованиями НД ответить на следующие вопросы: • необходимо ли перед выбором мер защиты инфокоммуникационной системы по базовому уровню осуществлять идентификацию физических условий и условий окружающей среды ее функционирования; • по какому типу должна (может) идентифицироваться система для выбора мер защиты; • к какому виду защитных мер относится обеспечение функций управления конфигурацией и изменениями системы в процессе ее эксплуатации; • какой криптографический режим преобразований используется для проверки целостности; • какую проблему безопасности может создать угроза в виде направления сообщений по ошибочному маршруту; • является ли разделение сетей одной из мер защиты инфокоммуникационной системы типа «Рабочая станция, подсоединенная к сети, без коллективного пользования»; • какая антивирусна программа позволяет находить и точно идентифицировать конкретный вирус по заранее внесенной в базу «маске вируса»; • что является первоочередной задачей при решении проблемы обеспечения сетевой безопасности; • что должно анализироваться при анализе структуры сети; • необходимо ли при решении проблем сетевой безопасности учитывать возможные к использованию серверные приложения клиента; • можно ли при установлении категории доверительных отношений сети не идентифицировать доверительную среду. 3. сформулировать выводы по результатам выполненной работы. 4. подготовить и оформить Отчет в электронном виде, разместить в ЛК АИС ГУАП и защитить у преподавателя

Структура и форма отчета о лабораторной работе

Отчет должен включать:

- титульный лист;
- описание задания;
-решение задания (задачи);
- необходимые графические материалы;
- выводы

Требования к оформлению отчета о лабораторной работе

Отчет о лабораторной работе должен быть выполнен в письменном виде с указанием на титульном листе номера группы и ФИО обучающегося. Пример оформления титульного листа отчета представлен на сайте ГУАП - https://guap.ru/regdocs/docs/uch.

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 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:

– «Конспект лекций», составляемый обучающимся в процессе лекционных занятий;

– учебно-методические материалы по дисциплине.

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

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

Текущий контроль знаний обучающегося осуществляется по каждому разделу лекционного курса после завершения обучения по соответствующему разделу посредствам текущего промежуточного тестирования.

Тест для текущего тестирования содержит 25 вопросов по соответствующему разделу, на каждый из которых предлагается не менее двух вариантов ответов.

Задачей обучающегося является выбор правильного ответа из предлагаемых вариантов ответов.

Критерием оценки успеваемости обучающегося при текущем контроле являются уровень освоения обучающимся изучаемой дисциплины, оцениваемый по двухуровневой системе:

1 уровень «успевает»: если обучающийся при тестировали дал не менее 15 правильных ответов на вопросы из 25;

2 уровень «не успевает»: если обучающийся при тестировали дал менее 15 правильных ответов на вопросы из 25.

При проведении промежуточной аттестации результаты текущего контроля учитываются следующим образом: к промежуточной аттестации допускаются только обучающиеся, полностью выполнившие задания для оценки текущей успеваемости с результатом «успевает».

11.5. ***Методические указания для обучающихся по прохождению промежуточной аттестации.***

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

– дифференцированный зачет – форма оценки знаний, полученных обучающимся при изучении дисциплины с аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Дифференцированный зачет проводится в форме собеседования по вопросам, представленным в таблице 16.

Промежуточная аттестация может осуществляться посредствам итогового тестирования по всем разделам курса дисциплины.

Тест для тестирования содержит 15 вопросов по соответствующему разделу, на каждый из которых предлагается не менее двух вариантов ответов. Примерный перечень вопросов теста приведен в таблице 21.

Задачей обучающегося при тестировании является выбор правильного ответа (ответов) из предлагаемых вариантов ответов.

Критерии оценки уровня знаний обучающегося при прохождении промежуточной аттестации по изучаемой дисциплины по результатам тестирования оценивается по двухуровневой системе:

1 уровень «зачтено»: если обучающийся при тестировали дал не менее 10 правильных ответов на вопросы из 15;

2 уровень «не зачтено»: если обучающийся при тестировали дал менее 10 правильных ответов на вопросы из 15, что полностью соответствует характеристикам сформированных компетенций, приведенным в таблице 14.

Тест для промежуточной аттестации для проверки у обучающихся формирования универсальных, общепрофессиональных и профессиональных компетенций, предусмотренных программой обучения представлен в таблице 18.

Таблица 21 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
1	Информация – это….? • любые сведения о чем-либо, являющееся результатом неких операций • абстракция, созданная человеком • какие-либо данные, представленные на материальном носителе
2	Инфокоммуникациионная среда – это…? • совокупность системных, структурных, технических, технологических и экономических механизмов, позволяющие Пользователю получать информационные услуги • сетевое распределение информационно-коммуникативных субъектов, удовлетворяющих свои потребности с помощью информационно-телекоммуникационных технологий • сетевое распределение информационно-телекоммуникационных объектов
3	Что относится к информационным услугам? • услуги связи, обеспечивающие обработку информации с использованием средств вычислительной техники • услуги связи, обеспечивающие хранение информации с использованием средств вычислительной техники • услуги связи, обеспечивающие предоставление информации по запросу Заказчика
4	Что является основные характеристиками информации, подлежащими защите? • Целостность • Достоверность • Доступность • Конфиденциальность • Своевременность
5	Для чего Потребитель (Заказчик информационной системы) использует систему критериев безопасности? • для определения требуемого уровня доверия к объекту • для формулирования требований к функциям безопасности • для разработки функциональных Спецификаций безопасности
6	Что является целью сетевой безопасности? • выявление потенциальных видов рисков, связанных с сетевыми соединениями • определение и идентификация потенциальных контролируемых зон • идентификация и анализ факторов, воздействующих на компоненты средств связи
7	Что относится к задачам, которые необходимо решить для обеспечения сетевой безопасности? • анализ сетевой структуры и ее применения • идентификация типов и характеристик сетевых соединений • анализ сетевых доверительных отношений • идентификация потенциально контролируемых зон
8	Решение о запрете передачи информации через определенные коммутируемые линии связи должно приниматься на этапе ….? • Определения контролируемых зон • Анализа структуры безопасности

№ п/п	Примерный перечень вопросов для тестов
	• Формирования Политики безопасности • Распределения задач по выбору защитных мер
9	Что должно анализироваться при анализе структуры сети? • является ли сеть используемой для соединения систем в пределах региона или в более широких масштабах • вся ли информация физически доступна с помощью всех подсоединенных систем • используются ли в структуре сети протоколы коллективного пользования • является ли информация доступной для всех систем вдоль маршрута, который может быть случайно или преднамеренно изменен
10	Необходимо ли при решении проблем сетевой безопасности учитывать возможные к использованию серверные приложения клиента? • Да • НЕТ
11	Алгоритм построения «вектора признаков» для биометрического распознавания пользователя – это защитная мера типа ……? • Управление доступом Пользователя к технической системе • Специальная защита • Логическое управление и аудит доступа
12	ПО, имеющее скрытую функцию, обеспечивающую возможность скопировать данные и переслать их анонимному Получателю – это ….. ? • злонамеренный код • вредоносное ПО • «червь» • «троянский конь» • «вирус»
13	Вредоносное ПО типа «Зомби» - это вирус? • Да • НЕТ
14	Антивирусна программа, которая позволяет находить и точно идентифицировать конкретный вирус по заранее внесенной в базу «маске вируса»– это программа «…..»? • «сканер» • «CRC-сканер» • «блокировщик» • «иммунизатор»
15	Какой криптографический режим преобразований предусматривает при зашифровании информации ввод дополнительного блока набора символов? • гаммирование • простая замена • имитовставка • гаммирование с обратной связью

Дифференцированный зачет, как правило, проводится в период зачетной недели, предшествующей экзаменационной сессии, и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Критерии оценки уровня знаний обучающегося при прохождении промежуточной аттестации в соответствии с таблицей 14.

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