

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ  
Декан ФИиВТ

УТВЕРЖДАЮ /А.А. Кречетов/  
(Ф.И.О. декана (директора института))

14.02.2024 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

М.1.2.3 Интеллектуальные системы безопасности

(код и наименование дисциплины по учебному плану)

Направление подготовки  
(специальность)

09.04.04 Программная инженерия

Квалификация выпускника

Магистр

(бакалавр/магистр/специалист)

Программа магистратуры

Программное обеспечение систем искусственного  
интеллекта

Курс 2  
Триместр 5

**Распределение учебного времени**

Трудоемкость по учебному плану	288 / 8	часов/зачетных единиц
Лекции	14	часов
Лабораторные работы	-	часов
Практические занятия	56	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	70	часов
Контактная работа по экзамену	6	часов
Курсовой проект (работа)	-	триместр
Самостоятельная работа обучающихся (без учета экз.)	182	часов
Самостоятельная работа по подготовке к экзамену	30	часов
Экзамен	5	триместр
Зачет	-	триместр
БРК, ДЗ	-	триместр

(год)

Программа составлена в соответствии с требованиями ФГОС ВО направления подготовки (специальности) 09.04.04 Программная инженерия

Программу составили:

заведующий кафедрой с ученой степенью кандидата наук	ИиСП	СОГЛАСОВАНО	А.В. Бородин
(должность)	(кафедра)		(И.О. Фамилия)

РАССМОТРЕНА и ОДОБРЕНА на заседании кафедры, за которой закреплена дисциплина  
Кафедра информатики и системного программирования

07.02.2024	протокол №	6
(дата)		

Заведующий кафедрой	СОГЛАСОВАНО	А.В. Бородин
		(И.О. Фамилия)

Рабочая программа СОГЛАСОВАНА с факультетом (институтом), выпускающей(ими)  
кафедрой(ами).

СООТВЕТСТВУЕТ действующей ОП.

Заведующий кафедрой	СОГЛАСОВАНО	А.В. Бородин
		(И.О. Фамилия)

Председатель методической комиссии факультета (института), в который входит  
выпускающая кафедра

СОГЛАСОВАНО	А.А. Кречетов
	(И.О. Фамилия)

Эксперт(ы): МАЙМИН ВЛАДИСЛАВ РУВИМОВИЧ , Председатель Ассоциации  
разработчиков программного обеспечения «ПС СОФТ», член Совета директоров НКО  
"МОНЕТА.РУ" (ООО), Председатель Правления НКО "МОНЕТА.РУ" (ООО)

Рабочая программа проверена и зарегистрирована в УМЦ 15.03.2024 г.

Специалист учебно-методического центра СОГЛАСОВАНО /Т.А. Смирнова/

## Раздел 1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является достижение планируемых результатов обучения, соответствующих установленным в ОПОП индикаторам достижения компетенций:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения
1. ПК-9 Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях	ПК-9.1. Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности а различных предметных областях	<b>знания:</b> ПК-9.1. З-1. Знает требования информационной безопасности в различных предметных областях <b>умения:</b> ПК-9.1. У-1. Умеет разрабатывать программное и аппаратное обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях <b>навыки:</b> ПК-9.1. В-1. Владеет инструментальными средствами разработки программного и аппаратного обеспечений технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях
	ПК-9.2. Модернизирует программное и аппаратной обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности а различных предметных областях	<b>знания:</b> ПК-9.2. З-1. Знает требования информационной безопасности в различных предметных областях в контексте модернизации программного обеспечения <b>умения:</b> ПК-9.2. У-1. Умеет модернизировать программное и аппаратное обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях <b>навыки:</b> ПК-9.2. В-1. Владеет методами модернизации программного и аппаратного обеспечений технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях

## Раздел 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к части, формируемой участниками образовательных отношений ОПОП.

Дисциплина является обязательной

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих государственной итоговой аттестации в форме: Выполнение и защита выпускной квалификационной работы (ПК-9)

### Раздел 3. ОПИСАНИЕ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

Для формирования заявленных компетенций используются методологические технологии, реализующие деятельностный, личностно-ориентированный, практико-ориентированный подходы.

Основными стратегическими технологиями являются: исследовательские, лекционные занятия, практические занятия

На достижение конкретных целей обучения направлены применяемые тактические технологии: задания, классическая лекция, проблемная лекция

### Раздел 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

#### 5 триместр

Виды и темы занятий	Количество часов	Формируемые компетенции
<b>Интеллектуальные системы безопасности</b>	<b>252</b>	ПК-9
Лекция. Лекция №1. Вводная лекция. Понятие модели угроз. Классификация моделей угроз. Применение технологий искусственного интеллекта при решении задач (физической и) информационной безопасности.	2	
Лекция. Лекция №2. Биометрические системы идентификации. Классификация биометрических систем. Задачи, решаемые биометрическими системами. Примеры биометрических систем.	4	
Лекция. Лекция №3. Методы обнаружения аномалий и вторжений. Классификация методов обнаружения аномалий и вторжений. Сигнатурные методы. Поведенческие методы. Спектральные модели поведения системы. Продукционные методы обнаружения аномалий и вторжений.	4	
Лекция. Лекция №4. Анализ журналов. Парсинг. Интеллектуальные методы анализа синтаксических деревьев на выходе парсеров.	2	
Лекция. Лекция №5. Комплексные системы безопасности. Роль технологий искусственного интеллекта для комплексных систем безопасности. Оценка экономического эффекта от применения технологий искусственного интеллекта в системах безопасности.	2	
Практическое занятие. Практическое занятие №1. Построение модели угроз и модели нарушителя по индивидуальным вариантам	8	
Практическое занятие. Практическое занятие №2. Знакомство с биометрическими системами с открытым кодом.	12	
Практическое занятие. Практическое занятие №3. Методы отбора сигнатур для обнаружения РПВ. Обнаружение РПВ на основе сигнатур.	12	
Практическое занятие. Практическое занятие №4. Анализ журналов. Парсинг. Продукционные методы обнаружения атак.	12	
Практическое занятие. Практическое занятие №5. Анализ журналов. Спектральные методы обнаружения аномалий. Продукционные методы анализа спектров.	12	

Задания для самостоятельной работы, в том числе выполнение Биометрические системы с открытым кодом.	
Проблема обнаружения вторжений.	
Детекторы движения в системах цифрового видео.	
Знакомство с протоколом SYSLOG.	
Использование stunnel, sslwrap, SSL/TLS.	
Стандарты RFC 3164, RFC 3195, RFC 5424, RFC 5425, RFC 5426, RFC 5427, RFC 5674, RFC 5675, RFC 5676, RFC 5848, RFC 6012, RFC 6587.	
Анализ аномалий.	
Общие принципы Фурье-анализа.	
Общие принципы вейвлет-анализа.	
Продукционные системы.	
Проблема обнаружения РПВ.	
Концепция сосуществования.	182
Иная контактная работа:	0
Подготовка к экзамену	30
Проведение экзамена	6

## Раздел 5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение дисциплины рекомендуется начать с ознакомления с рабочей программой, ее структурой и содержанием разделов. Учебный материал структурирован, изучение дисциплины осуществляется в тематической последовательности.

**Занятия лекционного типа** дают систематизированные знания по дисциплине, концентрируют внимание на наиболее сложных и важных вопросах. Во время лекционных занятий рекомендуется вести конспектирование учебного материала; обращать внимание на формулировки и категории, раскрывающие суть проблемы, явления или процесса; зафиксировать выводы и практические рекомендации.

Подготовка к **занятиям семинарского типа** включает ознакомление с планом практического занятия; работу с конспектом лекций, выполнение домашнего задания, работу с учебной и учебно-методической литературой, научными изданиями и электронными образовательными ресурсами, рекомендованными рабочей программой дисциплины.

Содержание **самостоятельной работы** определяется рабочей программой дисциплины, оценочными и методическими материалами, заданиями и указаниями преподавателя. Самостоятельная работа может осуществляться в аудиторной и внеаудиторной формах. Эффективным средством осуществления самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к образовательной программе, рабочей программе дисциплины, к электронным библиотечным системам, профессиональным базам данных и информационным справочным системам.

Изучение дисциплины включает выполнение заданий для самостоятельного выполнения. Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплин представлены в рабочей программе.

Формой промежуточной аттестации по дисциплине является экзамен.

## Раздел 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 6.1. Учебно-методическое обеспечение

№№ п/п	Список используемой литературы	Количество экземпляров печатных изданий, имеющихся в библиотеке, или электронный адрес издания (ресурса) в сети Интернет
<b>УЧЕБНЫЕ, УЧЕБНО-МЕТОДИЧЕСКИЕ И НАУЧНЫЕ ИЗДАНИЯ</b>		
1.	Шумский, Алексей Анатольевич. Системный анализ в защите информации [Текст] : учеб. пособие для вузов по специальностям в обл. информ. безопасности / А. А. Шумский, А. А. Шелупанов. М.: Гелиос АРВ, 2005. - 220 с. ISBN 5-85438-128-1. Экземпляры: всего 20.	20
2.	Станкевич, Лев Александрович. Интеллектуальные системы и технологии [Текст : Электронный ресурс] : Учебник и практикум / Станкевич Л.А. М.: Издательство Юрайт, 2018. - 397 с. ISBN 978-5-534-02126-4.	<a href="https://urait.ru/book/intellektualnye-sistemy-i-tehnologii-413546">https://urait.ru/book/intellektualnye-sistemy-i-tehnologii-413546</a>
3.	Смирнов, В. М. Системы отображения информации. Инженерная психология [Электронный ресурс] : учебник / Смирнов В. М. Санкт-Петербург: Лань, 2020. - 172 с. ISBN 978-5-8114-4288-1.	<a href="https://e.lanbook.com/book/131048">https://e.lanbook.com/book/131048</a>
4.	Петренко, В. И. Защита персональных данных в информационных системах. Практикум [Текст] : Учебное пособие для вузов / Петренко В. И., Мандрица И. В.; Мандрица И. В. 4-е изд., стер. Санкт-Петербург: Лань, 2022. - 108 с. ISBN 978-5-507-45301-6.	<a href="https://e.lanbook.com/book/264242">https://e.lanbook.com/book/264242</a>
5.	Остроух, А. В. Системы искусственного интеллекта [Электронный ресурс] : монография / Остроух А. В., Суркова Н. Е.; Суркова Н. Е. 4-е изд., стер. Санкт-Петербург: Лань, 2024. - 228 с. ISBN 978-5-507-47478-3.	<a href="https://e.lanbook.com/book/379988">https://e.lanbook.com/book/379988</a>

### 6.2. Материально-техническая база и программное обеспечение

№№ п/п	Аудитории для проведения учебных занятий, самостоятельной работы и проведения государственной итоговой аттестации	Перечень основного оборудования	Программное обеспечение
1.	427 (III)	Мобильный телефон Samsung Galaxy A7 (2), Мобильный телефон Samsung Galaxy S9+ (2), Ноутбук Apple MacBook Pro13 with Retina display and Touch Bar Mid2017 (1), Планшет Apple iPad 2018 (1), Проектор мультимедийный Hitachi CP- RX94 (1), Смартфон APPLE iPhone 8 Plus 64 Gb, MQ8L2RU/A, серый (1), Смартфон APPLE iPhone	Microsoft Windows Enterprise, Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ГАРАНТ-Мастер, Microsoft Access, Microsoft Visio Professional, Microsoft

		X 64 Gb,MQAD2RU/A, серебристый (1), Шлем виртуальной реальности HTC Vive (2), Комплект учебной мебели (1)	Project Professional, Microsoft Visual Studio Enterprise, Комплект ПО для решения основных пользовательских задач
2.	429 (III)	ПК RAMEC GALE/i7-3770/B75M2x4DDR3/GTX650/500S ATA3/монит.LCD PHILIPS 23,6" клав.,мышь (8), Принтер HP LaserJet Professional P1102 (1), Проектор VIEWSONIC PJD6550LW белый (1), Комплект учебной мебели (1)	Microsoft Windows Enterprise, Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ГАРАНТ-Мастер, Microsoft Access, Microsoft Visio Professional, Microsoft Project Professional, Microsoft Visual Studio Enterprise, Комплект ПО для решения основных пользовательских задач
3.	430 (III)	ПК RAMEC GALE/i7-3770/B75M2x4DDR3/GTX650/500S ATA3/монит.LCD PHILIPS 23,6" клав.,мышь (8), Проектор VIEWSONIC PJD6550LW белый (1), Шкаф телекоммуникационный напольный ЦМО ШТК-М (1), Комплект учебной мебели (1)	Microsoft Windows Enterprise, Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ГАРАНТ-Мастер, Microsoft Access, Microsoft Visio Professional, Microsoft Project Professional, Microsoft Visual Studio Enterprise, Комплект ПО для решения основных пользовательских задач
4.	521 (I)	Комплект учебной мебели (1)	Microsoft Windows Enterprise, Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ГАРАНТ-Мастер, Microsoft Access, Microsoft Visio Professional, Microsoft Project Professional, Microsoft Visual Studio Enterprise, Комплект ПО для решения основных пользовательских задач
5.	522 (I)	Анализатор спектра NS-30А (1), Антенна M102 в компл. с кабелем	Microsoft Windows Enterprise, Справочная

		<p>ВЧ TNCm-SMAm (1), Блок питания лаборат. НУ 3003 D-3 (1), Внешний HDD WD 2TB 3.0 , 3.5"USB (1), Внешний накопитель 1 Seagate Original USB 3.0 4 Tb (1), Внешний накопитель флешка USB TRANSCEM Jetflash 780 64 Gb (1), Гигабитный управляемый коммутатор на 16 портов (1), Измеритель CN -801 HP (1), Кондиционер AEG ACS-09HR (1), Многофункциональный измерительный прибор (1), Монитор 20 "Beng FP 202W (2), Монитор LCD Samsung 17" SM 713N (1), МФУ Canon i-SENSYS MF 4018 (1), МФУ 1 Лазерный Canon i-Sensys MF226 (1), Набор ВЧ переходников (1), Ноутбук Dell Latitude E6520 Intel Core I5 Processor 2520M 15,6" (2), Ноутбук TOSHIBA Satellite L655-1H2-RU (1), Паяльная станция AOYUE 968 (1), Переключатель ZX80-DR230 (1), Персональный компьютер 3 Atlant A2X4/4G(3)/512Mb/монитор Pyama 2209/3Y (1), ПК RAMEC GALE LCD LG 23"/Intel i5 4590/MSI B85M-E45/2x4DDR3/GT740 2Gb/500Gb/клав,мышь (28), Преобразователь SP-200-24-AC-DC в кожухе 199x99x50мм (1), Приемопередающая программно-конфигурируемая радиоплатформа G32 (1), Принтер Canon LBP 2900 лазерный с кабелем (1), Проектор мультимедийный Hitachi CP-EX250 (1), Проектор мультимедийный Hitachi CP-EX251N (1), Сист. блок Pen D 945 3.4 DDR 2 1024*2/FDD 3.5/250 Gb/DVD-RW/кл+мышь+коврик (1), Системный блок CPU Intel Core i7-6700/ASRod Z-170/32 Gb/GTX 1070/200 Gb/Wi-Fi +клав, мышь (1), Станок сверлильный 350 Вт (1), Универсальная приёмо-передающая платформа для проектирования СВЧ-систем компл.mgx92 (1), Усилитель LZY-22 (1), Усилитель ZHL-3A-S (1), Комплект учебной</p>	<p>правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ГАРАНТ-Мастер, Microsoft Access, Microsoft Visio Professional, Microsoft Project Professional, Microsoft Visual Studio Enterprise, Комплект ПО для решения основных пользовательских задач</p>
--	--	--	--

## Раздел 7. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ/ ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Критерии оценивания индикаторов достижения компетенций направлены на:

- усвоение теоретического материала (объем знаний, глубина усвоения), предусмотренного рабочей программой;
- умение излагать материал (четкость, грамотность изложения материала, точность и полнота воспроизведения учебного материала);
- умение применять теоретические знания при решении практических заданий.

Шкала оценивания представлена ниже.

Уровень сформированности элементов компетенции	Критерии оценивания	Шкала оценивания
Пороговый уровень	Обучающийся имеет знания основного материала, проявляет умение логично его излагать, но может допускать неточности в изложении материала, недостаточно правильные формулировки, испытывает затруднения в выполнении практических заданий.	удовлетворительно
Продвинутый уровень	Обучающийся твердо знает программный материал, излагает его грамотно и по существу, не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения	хорошо
Высокий уровень	Обучающийся глубоко и прочно усвоил программный материал, грамотно и логически стройно его излагает, дает исчерпывающие ответы на поставленные вопросы. В ответе тесно увязывается теория с практикой, при этом обучающийся не затрудняется с ответом при видоизменении задания, свободно справляется с задачами, вопросами и другими видами применения знаний, показывает знакомство с монографической литературой, периодическими изданиями, правильно обосновывает принятые решения, свободно владеет разносторонними навыками, приемами выполнения практических работ	отлично

### 7.1. Текущий контроль успеваемости

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины (модуля) и производится с применением технологии рейтингового контроля в соответствии с технологической картой дисциплины. Порядок составления технологической карты и алгоритм проведения процедуры оценивания видов деятельности обучающихся, направленных на освоение знаний, умений, навыков и/или опыта деятельности, по накопительной системе в баллах устанавливается положением о системе РИТМ в ФГБОУ ВО «ПГТУ»

### 7.2. Промежуточная аттестация обучающихся

Промежуточная аттестация обучающихся направлена на оценивание результатов обучения

по дисциплине (модулю) и проводится с использованием фондов оценочных средств.

Примеры типовых контрольных заданий из базы фонда оценочных средств по образовательной программе.

**1) К правовым методам, обеспечивающим информационную безопасность, относятся:**

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- + Разработка и конкретизация правовых нормативных актов обеспечения безопасности

**2) Основными источниками угроз информационной безопасности являются все указанное в списке:**

- Хищение жестких дисков, подключение к сети, инсайдерство
- + Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

**3) Виды информационной безопасности:**

- + Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

**4) Цели информационной безопасности – своевременное обнаружение, предупреждение:**

- + несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

**5) Основные объекты информационной безопасности:**

- + Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

**6) Основными рисками информационной безопасности являются:**

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- + Потеря, искажение, утечка информации

**7) К основным принципам обеспечения информационной безопасности относится:**

- + Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

**8) Основными субъектами информационной безопасности являются:**

- руководители, менеджеры, администраторы компаний
- + органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

**9) К основным функциям системы безопасности можно отнести все перечисленное:**

- + Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании

- Внедрение аутентификации, проверки контактных данных пользователей

**тест 10) Принципом информационной безопасности является принцип недопущения:**

- + Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

**11) Принципом политики информационной безопасности является принцип:**

- + Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

**12) Принципом политики информационной безопасности является принцип:**

- + Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

**13) Принципом политики информационной безопасности является принцип:**

- + Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

**14) К основным типам средств воздействия на компьютерную сеть относится:**

- Компьютерный сбой
- + Логические закладки («мины»)
- Аварийное отключение питания

**15) Когда получен спам по e-mail с приложенным файлом, следует:**

- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
- + Удалить письмо с приложением, не раскрывая (не читая) его

**16) Принцип Кирхгофа:**

- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
- + Секретность закрытого сообщения определяется секретностью ключа

**17) ЭЦП – это:**

- Электронно-цифровой преобразователь
- + Электронно-цифровая подпись
- Электронно-цифровой процессор

**18) Наиболее распространены угрозы информационной безопасности корпоративной системы:**

- Покупка нелегального ПО
- + Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

**19) Наиболее распространены угрозы информационной безопасности сети:**

- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
- + Сбой (отказ) оборудования, нелегальное копирование данных

**тест\_20) Наиболее распространены средства воздействия на сеть офиса:**

- Слабый трафик, информационный обман, вирусы в интернет
- + Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии

**21) Утечкой информации в системе называется ситуация, характеризующаяся:**

- + Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

**22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:**

- + Целостность
- Доступность
- Актуальность

**23) Угроза информационной системе (компьютерной сети) – это:**

- + Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

**24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:**

- Регламентированной
- Правовой
- + Защищаемой

**25) Разновидностями угроз безопасности (сети, системы) являются все перечисленные в списке:**

- + Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

**26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:**

- + Владелец сети
- Администратор сети
- Пользователь сети

**27) Политика безопасности в системе (сети) – это комплекс:**

- + Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

**28) Наиболее важным при реализации защитных мер политики безопасности является:**

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности

### Перечень вопросов для проведения промежуточной аттестации

1. В чем сходство и отличие модели атак и защиты биометрических систем распознавания диктора от модели для других биометрических систем?
2. Каковы общие и характерные атаки и уязвимости для различных биометрических систем?
3. Какие атаки и уязвимости наиболее критичны с точки зрения безопасности биометрических систем распознавания диктора?
4. Какие методы, средства защиты и предотвращения уязвимостей на биометрические системы распознавания диктора наиболее успешны?
5. Каковы общие и характерные методы защиты от атак и уязвимостей для различных биометрических систем?
6. Что можно предложить для улучшения описанной системы разграничения прав доступа?
7. Какие существуют оценки эффективности системы биометрической аутентификации?
8. Какие существуют требования для тестирования систем биометрической аутентификации в соответствии со стандартами?
9. Сформулируйте понятие информационной безопасности информационной системы (ИС).
10. Что такое конфиденциальность, целостность, доступность применительно к ИС?
11. Что такое лицензирование и что такое сертификация применительно к ИС? Что из них и когда является обязательным.
12. Роль технологий ИИ в защите ИС.
13. Объясните понятие «угроза безопасности ИС».
14. Назовите основные признаки классификации возможных угроз безопасности ИС.
15. Какие Вы знаете предпосылки появления угроз ИБ?
16. Какие возможны подходы к оценке ущерба от реализации угроз ИБ?
17. Что такое модель нарушителя?
18. Что такое политика безопасности?
19. В чем заключается отличие основных видов политик безопасности?
20. Какие ресурсы ИС могут быть защищаемыми объектами при решении проблем НСД?
21. Чем отличаются понятия «защита ИС от НСД» и «защита СВТ» от НСД?
22. Что такое объект доступа и субъект доступа?

23. Что такое контекстное разграничение?

24. В каких системах возможно применение механизма контекстного разграничения доступа?

25. В чем суть дискреционного управления доступом?

26. В чем суть мандатного разграничения доступом?

27. В чем суть спектрального анализа логов?