

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ
Декан ФИиВТ

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

30.06.2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

С.1.1.42 Теоретические основы компьютерной безопасности

(код и наименование дисциплины по учебному плану)

Направление подготовки (специальность) 10.05.03 Информационная безопасность автоматизированных систем

Квалификация выпускника Специалист
(бакалавр/магистр/специалист)

Специализация Анализ безопасности информационных систем

Курс 5
Семестр 9

Распределение учебного времени

Трудоемкость по учебному плану	144 / 4	часов/зачетных единиц
Лекции	18	часов
Лабораторные работы	-	часов
Практические занятия	36	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	54	часов
Контактная работа по экзамену	6	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	54	часов
Самостоятельная работа по подготовке к экзамену	30	часов
Экзамен	9	семестр
Зачет	-	семестр
БРК, ДЗ	-	семестр

(год)

Программа составлена в соответствии с требованиями ФГОС ВО направления подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем

Программу составили:

старший преподаватель	ИБ	СОГЛАСОВАНО	В.И. Смирнов
(должность)	(кафедра)		(И.О. Фамилия)

РАССМОТРЕНА и ОДОБРЕНА на заседании кафедры, за которой закреплена дисциплина
Кафедра информационной безопасности

(наименование кафедры)		
30.04.2021	протокол №	17
(дата)		

Заведующий кафедрой	СОГЛАСОВАНО	И.Г. Сидоркина
		(И.О. Фамилия)

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

СООТВЕТСТВУЕТ действующей ОП.

Заведующий кафедрой	СОГЛАСОВАНО	И.Г. Сидоркина
		(И.О. Фамилия)

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

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

Эксперт(ы): Зверева Екатерина Васильевна, Начальник отдела ПД ИТР ОАО ММЗ

Рабочая программа проверена и зарегистрирована в УМЦ 01.07.2021 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. ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1 знает основные угрозы безопасности информации и модели нарушителя объекта информатизации	знания: знает основные угрозы безопасности информации и модели нарушителя объекта информатизации умения: навыки:
	ОПК-6.2 умеет разрабатывать модели угроз и модели нарушителя объекта информатизации	знания: умения: умеет разрабатывать модели угроз и модели нарушителя объекта информатизации навыки:
	ОПК-6.3 Определение комплекса мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем	знания: знает правила, процедуры, практические приемы, руководящие принципы, методы и средства для защиты информации автоматизированных систем умения: умеет применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем навыки: Определение комплекса мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем

Раздел 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к обязательной части ОПОП.

Дисциплина является обязательной

Для продолжения формирования заявленных компетенций необходимы знания предшествующих дисциплин: Основы информационной безопасности (ОПК-6), Организационное и правовое обеспечение ИБ (ОПК-6)

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих государственной итоговой аттестации в форме: Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-6)

Раздел 3. ОПИСАНИЕ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

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

Основными стратегическими технологиями являются: лекционные занятия, практические занятия, процедуры самообучения, исследовательские, дискуссионные

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

Раздел 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

9 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
Основные положения теории компьютерной безопасности. Методология построения систем защиты информации	36	ОПК-6
Лекция. Введение в теорию компьютерной безопасности. Построение систем защиты от угрозы нарушения конфиденциальности информации	2	
Лекция. Построение систем защиты от угроз нарушения конфиденциальности и целостности информации	2	
Лекция. Построение систем защиты от угроз отказа доступа к информации и раскрытия параметров компьютерной системы	2	
Практическое занятие. Практическая работа № 1. Идентификация и аутентификация в обеспечении компьютерной безопасности	4	
Практическое занятие. Практическая работа № 2. Криптография и стеганография в обеспечении компьютерной безопасности	4	
Практическое занятие. Практическая работа № 3. Технологии машинного обучения в обеспечении компьютерной безопасности	4	
Задания для самостоятельной работы, в том числе выполнение реферата Подготовка к лекциям, повторение учебного материала прошлых лекций. Подготовка к практическим работам. Реферат	18	
Модели безопасности компьютерных систем	36	ОПК-6
Лекция. Модели компьютерных систем с дискреционным управлением доступом	2	
Лекция. Модели компьютерных систем с мандатным управлением доступом	2	
Лекция. Модели компьютерных систем с ролевым управлением доступом. Модели безопасности информационных потоков	2	
Практическое занятие. Практическая работа № 4. Дискреционная политика управления доступом и модели безопасности	4	
Практическое занятие. Практическая работа № 5. Мандатная (полномочная) политика управления доступом и модели безопасности	4	
Практическое занятие. Практическая работа № 6. Политики ролевого управления доступом, безопасности информационных потоков и ИПС	4	

Задания для самостоятельной работы, в том числе выполнение реферата Подготовка к лекциям, повторение учебного материала прошлых лекций. Подготовка к практическим работам. Реферат	18	ОПК-6
Нормативные документы для решения задач компьютерной безопасности	36	
Лекция. Современные нормативы обеспечения информационной безопасности. Пакет документов ФСТЭК по профилям защиты	2	
Лекция. Современные стандарты по идентификации, аутентификации и защите персональных данных	2	
Лекция. Аудит компьютерной безопасности. Нормативная база аудита	2	
Практическое занятие. Практическая работа № 7. Стандарты в области защиты информации в компьютерных системах	4	
Практическое занятие. Практическая работа № 8. Стандарты по идентификации, аутентификации и защите персональных данных	4	
Практическое занятие. Практическая работа № 9. Система внутреннего аудита и управления информационной безопасностью предприятия	4	
Задания для самостоятельной работы, в том числе выполнение КР, реферата Подготовка к лекциям, повторение учебного материала прошлых лекций. Подготовка к практическим работам. Реферат	18	
Контрольная работа	18	
Иная контактная работа:	0	
Подготовка к экзамену	30	
Проведение экзамена	6	

Раздел 5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение дисциплины "Теоретические основы компьютерной безопасности" 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 "Теоретические основы компьютерной безопасности", 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 "Теоретические основы компьютерной безопасности". Содержание **самостоятельной работы** определяется рабочей программой дисциплины

"Теоретические основы компьютерной безопасности", 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 "Теоретические основы компьютерной безопасности", к электронным библиотечным системам, профессиональным базам данных и информационным справочным системам.

Изучение дисциплины "Теоретические основы компьютерной безопасности" включает выполнение контрольной работы, практической работы и подготовку реферата.

Краткие требования к написанию реферата:

- Реферат состоит из введения, основного текста, заключения и списка литературы. Реферат при необходимости может содержать приложение. Каждая из частей начинается с новой страницы. Первой страницей реферата является титульный лист.
- Заголовки должны четко и кратко отражать содержание разделов. Заголовки следует печатать с прописной буквы. Переносы слов не допускаются. Если заголовок состоит из двух предложений, их разделяют точкой. В конце заголовка точку не ставят.
- Во введении реферата указываются актуальность темы реферата, цель реферата, задачи, которые необходимо решить, чтобы достигнуть указанной цели. Кроме того, во введении реферата дается краткая характеристика структуры работы и использованной литературы. Объем введения для реферата – 1-1,5 страницы.
- Основной текст разделён на главы. Главы и параграфы реферата нумеруются. Точка после номера не ставится. Обычно в реферате 3-4 главы. Каждая новая глава начинается с новой страницы. На основную часть реферата приходится до 16 страниц.
- В заключении формируются выводы. В заключении должны быть представлены ответы на поставленные во введении задачи, сформулирован общий вывод и дано заключение о достижении цели реферата. Заключение должно быть кратким, четким.
- При составлении списка литературы следует придерживаться общепринятых стандартов. Список литературы должен включать от 4 до 12 позиций. Работы, указанные в списке литературы, должны быть относительно новыми (за последние 5-10 лет). Более старые источники можно использовать лишь при условии их уникальности. Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплин представлены в рабочей программе. Формой промежуточной аттестации по дисциплине "Теоретические основы компьютерной безопасности" 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, имеющих в библиотеке, или электронный адрес издания (ресурса) в сети Интернет
УЧЕБНЫЕ, УЧЕБНО-МЕТОДИЧЕСКИЕ И НАУЧНЫЕ ИЗДАНИЯ		
1.	Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : учебное пособие / П. Н. Девянин. 2-е изд., испр. и доп. Москва: Горячая линия-Телеком, 2017. - 338 с. ISBN 978-5-9912-0328-9.	https://e.lanbook.com/book/111049
2.	Барабанов, А. В. Семь безопасных информационных	

	технологий [Электронный ресурс] : монография / А. В. Барабанов, А. В. Дорофеев, А. С. Марков, В. Л. Цирлов: ДМК Пресс, 2017. - 224 с. ISBN 978-5-97060-494-6.	https://e.lanbook.com/book/97352
3.	Грушо, Александр Александрович. Теоретические основы компьютерной безопасности [Текст] : [учеб. пособие для вузов по специальностям группы 090100 "Информ. безопасность"] / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. М.: Академия, 2009. - 267, [1] с. ISBN 978-5-7695-4242-8. Экземпляры: всего 11.	11
4.	Корт, Семен Станиславович. Теоретические основы защиты информации [Текст] : [учеб. пособие для студентов вузов по группе специальностей в обл. информ. безопасности] / С. С. Корт. М.: Гелиос АРВ, 2004. - 233 с. ISBN 5-85438-010-2. Экземпляры: всего 29.	29
5.	Щербаков, А. Ю. Введение в теорию и практику компьютерной безопасности [Текст] : [Учеб. пособие] / Щербаков А. Ю. М.: Издатель Молгачева С. В., 2001. - 351 с. ISBN 5-89251-098-0. Экземпляры: всего 5.	5
6.	Зегжда, Дмитрий Петрович. Основы безопасности информационных систем [Текст] : Учеб. пособие для вузов по спец. "Компьютерная безопасность" и "Комплексное обеспечение информационной безопасности автоматизир.систем" / Д. П. Зегжда, А. М. Ивашко. М.: Горячая линия - Телеком, 2000. - 449 с. ISBN 5-93517-018-3. Экземпляры: всего 9.	9
7.	Щеглов, Андрей Юрьевич. Защита компьютерной информации от несанкционированного доступа [Текст] : научное издание / А. Ю. Щеглов. СПб.: Наука и техника, 2004. - 384 с. ISBN 5-94387-123-3. Экземпляры: всего 10.	10
ЭЛЕКТРОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ		
1.	Научная электронная библиотека eLIBRARY.RU	http://elibrary.ru
2.	Научная электронная библиотека «Киберленинка»	http://cyberleninka.ru
3.	ЭБС ПГТУ	https://www.volgatech.net/electronic-library-system-of-volgatech/
4.	Электронно-библиотечная система Лань	https://e.lanbook.com/
5.	Электронно-библиотечная система IPRBooks	http://www.iprbookshop.ru/
6.	ФСТЭК России	http://fstec.ru/
7.	Федеральное агентство по техническому регулированию и метрологии (Росстандарт)	https://www.rst.gov.ru/portal/gost
ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ		
1.	Справочно-правовая система Консультант+	http://www.consultant.ru
2.	Информационно-правовой портал Гарант	http://www.garant.ru
3.	Профессиональные справочные системы Техэксперт	http://www.cntd.ru

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.	535 (III)	Мультимедийный комплект 4 (1), Ноутбук Acer (1), Персональный компьютер в сборе PowerCool(Core i3-8100/H310/16GbDDR4/HDD 0.5Tb/23"6 АОС/кл.мышь/пач-корд 3м) (20), Комплект учебной мебели (1)	Microsoft Windows Enterprise, Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ГАРАНТ-Мастер, Комплект ПО для решения основных пользовательских задач
2.	107 (III)	Доска маркерная 100*200см (1), ИБП UPS 1100VA (7), Компьютер RAMEC STORM Custom i7-3770K/8ГБ/ монитор LCD 21.5", клавиат.,мышь (15), ПК Intel Core i7/GA-Z77-D3H/DDRIII 8Gb/500Gb SATA II/INWIN ATX-450, Монитор BenQ G2450HM,клав,мышь (3), ПК Intel Core i7/GA-Z77-D3H/DDRIII 8Gb/500Gb SATAIII/INWIN EAR003, Монитор 24" BenQ G2450HM,клав,мышь (2), Проектор мультимедийный Hitachi CP-X1250+разветвитель видеосигнала (1), Экран настенный 200*200см Braun Roll Vision (1), Комплект учебной мебели (1)	Microsoft Windows Enterprise, Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ГАРАНТ-Мастер, Комплект ПО для решения основных пользовательских задач

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. Одной из наиболее известных работ конца 70-х годов XX века, представившей обобщенный анализ теоретических и практических аспектов защиты компьютерной информации того периода, стала книга "Современные методы защиты информации". Её автором является

- a) Хартсон
- b) Хоффман
- c) Хэмминг
- d) Харрисон

2. Любое умышленное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую, является

- a) угрозой отказа служб
- b) угрозой нарушения целостности
- c) угрозой раскрытия параметров КС
- d) угрозой нарушения конфиденциальности

3. Определению «дискреционная защита» согласно Оранжевой Книге удовлетворяет группа безопасности:

- a) А
- b) В

- c) C
d) D
4. Какие свойства информации были нарушены, если известно, что злоумышленник получил доступ к некоторой секретной информации, хранящейся в вычислительной системе, и произошло умышленное изменение информации?
- a) доступность и конфиденциальность
b) целостность и доступность
c) адекватность и репрезентативность
d) конфиденциальность и целостность
5. Для автоматизированных систем было предложено рассматривать основные виды угроз:
- a) угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб, угроза раскрытия параметров АС, включающей в себя систему защиты
b) угроза нарушения конфиденциальности, угроза нарушения целостности
c) угроза нарушения целостности, угроза отказа служб
d) угроза отказа служб, угроза раскрытия параметров АС, включающей в себя систему защиты
6. Законом предусмотрены два типа электронных подписей:
- a) простая и усиленная
b) простая и сложная
c) адаптивная и квалифицированная
d) адаптивная и неквалифицированная
7. Криптографическая подсистема включает в себя
- a) использование сертифицированных средств защиты
b) обеспечение целостности программных средств и обработки информации
c) контроль доступа, управление потоками информации
d) использование сертифицированных криптографических средств
8. Какая парадигма исторически была первой в теории защиты компьютерных систем?
- a) парадигма, которая строится на понятии доверия
b) парадигма, которая строится на идее контроля действий пользователей и субъектов от их имени
c) парадигма, которая строится на ограничении доступов к информации
d) парадигма, которая строится на идее контроля пассивных сущностей (объектов и контейнеров)
9. Предоставление легальным пользователем дифференцированных прав доступа к ресурсам системы — это
- a) авторизация
b) аутентификация
c) валидация
d) верификация
10. Основными компонентами парольной системы являются
- a) интерфейс пользователя; интерфейс администратора; модуль сопряжения с другими подсистемами безопасности
b) интерфейс пользователя; интерфейс администратора; модуль сопряжения с другими подсистемами безопасности; база знаний неформализованного опыта
c) интерфейс пользователя; интерфейс администратора; модуль сопряжения с другими подсистемами безопасности; база данных учетных записей
d) база данных учетных записей; модуль сопряжения с другими подсистемами безопасности
11. Вторая группа классов защищенности АС согласно Руководящим документам Гостехкомиссии России включает в себя
- a) многопользовательские АС, пользователи имеют одинаковые полномочия доступа ко всей информации на носителях различного уровня конфиденциальности
b) многопользовательские АС, одновременно обрабатывается или хранится информация разных уровней конфиденциальности, не все пользователи имеют равные права доступа
c) АС, в которых работают фиксированное количество пользователей, с равными правами доступа к

информации

d) АС, в которых работает один пользователь

12. Этапы по проведению аудита безопасности информационных систем определены в следующем порядке:

a) сбор информации аудита; анализ данных аудита; инициирование процедуры аудита; выработка рекомендаций; подготовка аудиторского отчета

b) сбор информации аудита; инициирование процедуры аудита; анализ данных аудита; выработка рекомендаций; подготовка аудиторского отчета

c) инициирование процедуры аудита; сбор информации аудита; анализ данных аудита; выработка рекомендаций; подготовка аудиторского отчета

d) инициирование процедуры аудита; сбор информации аудита; анализ данных аудита; подготовка аудиторского отчета; выработка рекомендаций

13. Требования к средствам защиты АС от НСД не реализует подсистема защиты

a) подсистема управления доступом

b) подсистема обеспечения целостности

c) подсистема обеспечения корректности

d) подсистема регистрации и учета

14. В формальных моделях безопасности КС часто используется понятие автомата (например, для описания свойств системы защиты). Автоматом называется совокупность из

a) двух элементов $A(X,Y)$

b) трёх элементов $A(X,Y,f)$

c) четырёх элементов $A(X,S,Y,f)$

d) пяти элементов $A(X,S,Y,h,f)$

15. Минимальный набор компонентов, составляющий доверенную вычислительную среду, обеспечивает следующие функциональные возможности:

a) взаимодействие с аппаратным обеспечением АС; защиту памяти

b) функции файлового ввода-вывода; управление процессами

c) взаимодействие с аппаратным обеспечением АС; защиту памяти; функции файлового ввода-вывода; управление процессами

d) все компоненты и механизмы защищенной автоматизированной системы, отвечающие за реализацию политики безопасности

16. В модели Харрисона-Руззо-Ульмана используется понятие монотонной системы. Такая система не содержит операций

a) destroy object o' и delete r from $M[s,o]$

b) delete r from $M[s,o]$ и enter r into $M[s,o]$

c) enter r into $M[s,o]$ и create object o'

d) create object o' и destroy object o'

17. Какой из мониторов разрешает к выполнению только поток, принадлежащий множеству легального доступа?

a) монитор безопасности объектов

b) монитор обращений

c) монитор безопасности субъектов

d) монитор порождения субъектов

18. Документом, содержащим требования безопасности для конкретного объекта оценки и специфицирующим функции безопасности и меры доверия, предлагаемые объектом оценки для выполнения установленных требований, является

a) профиль защиты

b) политика функции безопасности

c) задание по безопасности

d) политика безопасности организации

19. В АС, для которых реализуются программные или программно-аппаратные СКЗИ, при хранении и

обработке информации должны быть предусмотрены следующие основные механизмы защиты от НСД

- a) идентификация и аутентификации пользователей и субъектов доступа; управление доступом; обеспечение целостности; регистрация и учет
 - b) обеспечение целостности; идентификация и аутентификации пользователей и субъектов доступа
 - c) управление доступом; регистрация и учет
 - d) обеспечение целостности; регистрация и учет
20. Что не определяет границы проведения обследования?
- a) организационные, физические, программно-технические и прочие аспекты обеспечения безопасности, которые необходимо учесть в ходе проведения обследования, и их приоритеты
 - b) список обследуемых физических, программных и информационных ресурсов, а также площадки (помещения), попадающие в границы обследования
 - c) права и обязанности аудиторов, руководства компании и руководителей структурных подразделений
 - d) основные виды угроз безопасности, рассматриваемые при проведении аудита

Перечень вопросов для проведения промежуточной аттестации

Вопросы на экзамен

1. Основные научные направления теории информационной безопасности. Этапы развития теории информационной безопасности в рамках субъект-сущностного подхода. Характеристика. Основные события.
2. Основные аксиомы, общие принципы, понятия и определения теории информационной безопасности в рамках субъект-сущностного подхода. Стандарт СТО.ФСБ.КК 1-2018. "Компьютерная экспертиза. Термины и определения".
3. Классическая классификация угроз безопасности информации. Основные методы реализации угроз. Причины, виды и каналы утечки информации.
4. Структура системы защиты от угроз нарушения конфиденциальности информации. Организационные меры и меры обеспечения физической безопасности.
5. Место идентификации и аутентификации в структуре системы защиты от угроз нарушения конфиденциальности информации. Основные понятия и определения. Роль и задачи аутентификации. Факторы аутентификации.
6. Место идентификации и аутентификации в структуре системы защиты от угроз нарушения конфиденциальности информации. Парольная аутентификация.
7. Место идентификации и аутентификации в структуре системы защиты от угроз нарушения конфиденциальности информации. Аутентификация с помощью биометрических характеристик.
8. Место идентификации и аутентификации в структуре системы защиты от угроз нарушения конфиденциальности информации. Аутентификация с помощью одноразовых паролей.
9. Структура системы защиты от угроз нарушения конфиденциальности информации. Разграничение доступа. Виды политик управления доступом.
10. Криптографические методы обеспечения конфиденциальности информации. Требования к средствам криптографической защиты информации. Способы и особенности реализации криптографических подсистем.
11. Конфиденциальность данных при использовании облачных технологий. Протоколы гомоморфной криптографии. Частично гомоморфные криптосистемы.
12. Конфиденциальность данных при использовании облачных технологий. Протоколы гомоморфной криптографии. Почти гомоморфные криптосистемы.
13. Конфиденциальность данных при использовании облачных технологий. Протоколы гомоморфной криптографии. Полностью гомоморфные криптосистемы.
14. Защита от угрозы нарушения конфиденциальности на уровне содержания информации. Методы

скрытой передачи и хранения информации. Защита текстовой информации.

15. Защита от угрозы нарушения конфиденциальности на уровне содержания информации. Методы скрытой передачи и хранения информации. Защита мультимедийных контейнеров.

16. Защита от угрозы нарушения конфиденциальности на уровне содержания информации. Методы скрытой передачи и хранения информации. Сетевая стеганография.

17. Защита от угрозы нарушения конфиденциальности на уровне содержания информации. Методы скрытой передачи и хранения информации. Стеганография в помехоустойчивых кодах.

18. Структура системы защиты от угроз нарушения конфиденциальности информации. Защита внешнего периметра. Межсетевой экран как средство фильтрации сетевого трафика. Основные функциональные подсистемы.

19. Структура системы защиты от угроз нарушения конфиденциальности информации. Защита внешнего периметра. Классификации межсетевых экранов. Основные виды межсетевых экранов.

20. Технологии машинного обучения в обеспечении компьютерной безопасности. Методы обнаружения и классификации компьютерных атак и сетевых аномалий методами искусственного интеллекта.

21. Технологии машинного обучения в обеспечении компьютерной безопасности. Системы и инструменты обнаружения сетевых атак.

22. Технологии машинного обучения в обеспечении компьютерной безопасности. Обнаружение компьютерных атак с применением нейронных сетей. Обнаружение и классификация сетевых аномалий с использованием гибридных искусственных нейронных сетей.

23. Технологии машинного обучения в обеспечении компьютерной безопасности. Нечёткая логика в задачах информационной безопасности.

24. Технологии машинного обучения в обеспечении компьютерной безопасности. Искусственные иммунные системы в информационной безопасности.

25. Структура системы защиты от угроз нарушения конфиденциальности информации. Протоколирование и аудит.

26. Структура системы защиты от угроз нарушения целостности информации. Принципы обеспечения целостности. Модель контроля целостности Кларка-Вилсона.

27. Построение систем защиты от угрозы нарушения целостности информации. Защита памяти. Барьерные адреса. Динамические области памяти. Адресные регистры. Страницы и сегменты памяти.

28. Криптографические методы обеспечения целостности информации. Электронная подпись. Криптографические хэш-функции. Коды проверки подлинности.

29. Особенности аутентификации в распределённых системах. Групповая подпись. Классификация схем групповой подписи. Применение групповой подписи для аутентификации субъектов в распределённых системах.

30. Особенности аутентификации в распределённых системах. Криптографические протоколы в условиях ограниченных вычислительных ресурсов. Концепция аутсорс-вычислений.

31. Защита от угрозы нарушения целостности информации на уровне содержания. Защита семантического анализа и актуальности информации.

32. Структура системы защиты от угроз нарушения доступности. Резервное копирование информации. Использование RAID-массивов.

33. Построение систем защиты от угрозы отказа доступа к информации. Защита от сбоев программно-аппаратной среды. Обеспечение отказоустойчивости программного обеспечения. Предотвращение неисправностей в программном обеспечении.

34. Построение систем защиты от угрозы раскрытия параметров компьютерной системы. Способы изучения кода программного обеспечения. Способы защиты программного обеспечения от изучения кода.

35. Разработка безопасного программного обеспечения. Модели жизненного цикла программного обеспечения. Безопасный жизненный цикл. Способы встраивания средств защиты в программное обеспечение.

36. Разработка безопасного программного обеспечения. Меры по разработке безопасного программного обеспечения (анализ требований, проектирование архитектуры, кодирование и тестирование).
37. Математические основы моделей безопасности. Понятие автомата. Элементы теории графов. Алгоритмически разрешимые/неразрешимые проблемы. Модель решетки. MLS-решетка.
38. Классические подходы по заданию логики работы системы разграничения доступа. Вербальная модель разграничения доступа. Модель Хартсона. Модель Лэмпсона, Грэхема, Деннинга.
39. Основные виды формальных моделей безопасности. Проблема адекватности реализации модели безопасности в реальной компьютерной системе.
40. Модели компьютерных систем с дискреционным управлением доступом. Модель матрицы доступов Харрисона-Руззо-Ульмана. Модель типизированной матрицы доступов.
41. Модели компьютерных систем с дискреционным управлением доступом. Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant.
42. Модели компьютерных систем с мандатным управлением доступом. Модель Белла-ЛаПадулы. Политика low-watermark в модели Белла-ЛаПадулы. Модель мандатного контроля целостности информации Биба.
43. Модели компьютерных систем с мандатным управлением доступом. Модель систем военных сообщений.
44. Модели компьютерных систем с ролевым управлением доступом. Базовая модель ролевого управления доступом. Модель администрирования ролевого управления доступом.
45. Модели компьютерных систем с ролевым управлением доступом. Модель мандатного ролевого управления доступом. Базовая модель атрибутивного управления доступом.
46. Модели безопасности информационных потоков (автоматная, вероятностная и др.). Субъект-ориентированная модель изолированной программной среды.
47. Модели безопасности управления доступом и информационными потоками (ДП-модели).
48. Современные нормативы обеспечения информационной безопасности. Пакет документов ФСТЭК по профилям защиты.
49. Современные национальные стандарты по идентификации, аутентификации и защите персональных данных.
50. Аудит компьютерной безопасности (внутренний и внешний).