

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ  
Декан ФИиВТ

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

02.02.2023 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

**С.1.1.45 Программно-аппаратные средства защиты информации**

*(код и наименование дисциплины по учебному плану)*

Направление подготовки (специальность)	10.05.03 Информационная безопасность автоматизированных систем
Квалификация выпускника	Специалист (бакалавр/магистр/специалист)
Специализация	Безопасность автоматизированных систем критически важных объектов

Курс	5
Семестр	9, 10

**Распределение учебного времени**

Трудоемкость по учебному плану	288 / 8	часов/зачетных единиц
Лекции	50	часов
Лабораторные работы	84	часов
Практические занятия	-	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	134	часов
Контактная работа по экзамену	6	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	118	часов
Самостоятельная работа по подготовке к экзамену	30	часов
Экзамен	10	семестр
Зачет	9	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:

доцент	ИБ	СОГЛАСОВАНО	А.А. Пекунов
(должность)	(кафедра)		(И.О. Фамилия)

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

(наименование кафедры)		
31.01.2023	протокол №	10/1
(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 08.02.2023 г.

Специалист учебно-методического центра СОГЛАСОВАНО /М.Л. Бойкова/

## 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-14 Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	ОПК-14.1 знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	<b>знания:</b> знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах <b>умения:</b> <b>навыки:</b>
	ОПК-14.2 умеет определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем	<b>знания:</b> <b>умения:</b> умеет определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем <b>навыки:</b>
	ОПК-14.3 Проведение технико-экономической оценки целесообразности создания системы защиты информации автоматизированной системы	<b>знания:</b> Знает технико-экономические оценки целесообразности создания системы защиты информации автоматизированной системы <b>умения:</b> Умеет проводить технико-экономические оценки целесообразности создания системы защиты информации автоматизированной системы <b>навыки:</b> Проведение технико-экономической оценки целесообразности создания системы защиты информации автоматизированной системы
2. ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг	ОПК-15.1 знает программные средства, позволяющие вести автоматизированный аудит	<b>знания:</b> знает программные средства, позволяющие вести автоматизированный аудит <b>умения:</b> <b>навыки:</b>
	ОПК-15.2 умеет разрабатывать предложения по	<b>знания:</b> <b>умения:</b> умеет разрабатывать предложения по совершенствованию

защищенности автоматизированных систем	совершенствованию системы управления информационной безопасностью автоматизированной системы	системы управления информационной безопасностью автоматизированной системы <b>навыки:</b>
	ОПК-15.3 Анализировать программные, архитектурно- технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах	<b>знания:</b> Знает программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах <b>умения:</b> Умеет анализировать программные, архитектурно- технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах <b>навыки:</b> Анализировать программные, архитектурно- технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах

## 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: Анализ рисков информационной безопасности (ОПК-15)

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих дисциплинах: Техническая защита информации (ОПК-15); государственной итоговой аттестации в форме: Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-14), Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-15)

## 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 и лабораторные занятия

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

Раздел 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

10 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
<b>Программно-аппаратные средства</b>	<b>144</b>	ОПК-14, ОПК-15
Лекция. Криптографические средства обеспечения безопасности информации	8	
Лекция. Программно-аппаратные средства обеспечения безопасности межсетевого взаимодействия	8	
Лекция. Программно-аппаратные средства, применяемые при оценке эффективности СЗИ	8	
Лекция. Сертификация программно-аппаратных средств обеспечения ИБ	8	
Лабораторная работа. Установка и настройка системы разграничения доступа АМЛЗ «Криптон-замок»	3	
Лабораторная работа. Настройка системы контроля входа и регистрации событий программного комплекса СЗИ от НСД «Secret-Net»	3	
Лабораторная работа. Настройка дискреционного и мандатного механизмов управления доступом программного комплекса СЗИ от НСД «Secret-Net»	3	
Лабораторная работа. Настройка подсистемы замкнутой программной среды и подсистемы контроля целостности на основании модели данных программного комплекса СЗИ от НСД «Secret-Net»	3	
Лабораторная работа. Настройка системы контроля входа и регистрации событий программного комплекса СЗИ от НСД «Dallas-Lock»	3	
Лабораторная работа. Настройка дискреционного и мандатного механизмов управления доступом программного комплекса СЗИ от НСД «Dallas-Lock»	3	
Лабораторная работа. Настройка подсистемы замкнутой программной среды и подсистемы контроля целостности на основании модели данных программного комплекса СЗИ от НСД «Dallas-Lock»	3	
Лабораторная работа. Установка и настройка системы разграничения доступа программного комплекса "Аккорд-РАУ"	3	
Лабораторная работа. Настройка дискреционного и мандатного механизмов управления доступом программного комплекса "Аккорд-РАУ"	3	
Лабораторная работа. Настройка подсистемы замкнутой программной среды и подсистемы контроля целостности на основании модели данных программного комплекса "Аккорд-РАУ"	3	
Лабораторная работа. Установка и настройка системы разграничения доступа программного комплекса СЗИ от НСД «Secret-Net» - сетевой вариант	3	
Лабораторная работа. Настройка дискреционного и мандатного механизмов управления доступом программного комплекса СЗИ от НСД «Secret-Net» - сетевой вариант	3	

Лабораторная работа. Настройка подсистемы замкнутой программной среды и подсистемы контроля целостности программного комплекса СЗИ от НСД «Secret-Net» - сетевой вариант	3
Лабораторная работа. Установка и настройка системы разграничения доступа программного комплекса СЗИ от НСД «Dallas-Lock» - сетевой вариант	3
Лабораторная работа. Настройка дискреционного и мандатного механизмов управления доступом программного комплекса СЗИ от НСД «Dallas-Lock» - сетевой вариант	3
Лабораторная работа. Настройка подсистемы замкнутой программной среды и подсистемы контроля целостности программного комплекса СЗИ от НСД «Dallas-Lock»- сетевой вариант	3
Задания для самостоятельной работы, в том числе выполнение КР	
Изучение литературы	64
Иная контактная работа:	0
Подготовка к экзамену	30
Проведение экзамена	6

### 9 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
<b>Программно-аппаратные средства</b>	<b>108</b>	ОПК-14, ОПК-15
Лекция. Методы обеспечения ИБ. Типовая структура и типовые функции ПАСОИБ	3	
Лекция. Принципы разработки и функционирования программно-аппаратных средств обеспечения ИБ	3	
Лекция. Классификация автоматизированных систем и требований по защите информации	4	
Лекция. Программно-аппаратные средства защиты от несанкционированного доступа	4	
Лекция. Программно-аппаратные средства доверенной	4	
Лабораторная работа. Установка и настройка системы разграничения доступа АМЛЗ «Аккорд»	5	
Лабораторная работа. Настройка подсистем контроля целостности и регистрации событий АМЛЗ «Аккорд»	5	
Лабораторная работа. Настройка системы разграничения доступа программного комплекса «Аккорд-64»	5	
Лабораторная работа. Настройка системы контроля входа и регистрации событий программного комплекса «Аккорд-64»	5	
Лабораторная работа. Настройка дискреционного и мандатного механизмов управления доступом программного комплекса «Аккорд-64»	5	
Лабораторная работа. Установка и настройка системы разграниченного доступа АМДЗ «Соболь»	5	
Лабораторная работа. Настройка подсистем контроля целостности и регистрации событий на основе модели данных АМДЗ «Соболь»	6	

Задания для самостоятельной работы, в том числе выполнение Изучение литературы	54
Иная контактная работа:	0

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

Изучение модуля 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 модулю, 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 лабораторного занятия; работу с конспектом лекций, выполнение домашнего задания, работу с учебной и учебно-методической литературой, научными изданиями и электронными образовательными ресурсами, рекомендованными рабочей программой модуля.

Содержание **самостоятельной работы** определяется рабочей программой модуля, 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 модуля, к электронным библиотечным системам, профессиональным базам данных и информационным справочным системам. Изучение модуля включает выполнение контрольной работы, лабораторной работы. Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплин представлены в рабочей программе.

## 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
<b>УЧЕБНЫЕ, УЧЕБНО-МЕТОДИЧЕСКИЕ И НАУЧНЫЕ ИЗДАНИЯ</b>		
1.	Прохорова, О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник для вузов / Прохорова О. В. 5-е изд., стер. Санкт-Петербург: Лань, 2023. - 124 с. ISBN 978-5-507-46010-6.	<a href="https://e.lanbook.com/book/293009">https://e.lanbook.com/book/293009</a>
2.	Мельников, Владимир Павлович. Методы и средства хранения и защиты компьютерной информации [Текст] : учебник : [по направлениям "Автоматизация технологических процессов и производств", "Конструкторско-технологическое обеспечение машиностроительных производств"] / В. П. Мельников, А. Г. Схиртладзе ; под ред. В. П. Мельникова. Старый	10

	ТНТ, 2017. - 399 с. ISBN 978-5-94178-403-5. Экземпляры: всего 10.	
3.	Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных [Текст] : Учеб.пособ.для студ-ов вузов,обуч.по спец."Защищен.телекоммуникац.системы","Комплекс.обеспечение инф.безопасности автоматизирован.систем" / [П.Ю.Белкин,О.О.Михальский,А.С.Першаков и др.]. М.: Радио и связь, 1999. - 168 с. ISBN 5-256-01416-1. Экземпляры: всего 5.	5
4.	Платонов, Владимир Владимирович. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей [Текст] : [учеб. пособие для студентов вузов по специальности 090102 "Компьютерная безопасность" и др.] / В. В. Платонов. М.: Академия, 2006. - 238 с. ISBN 5-7695-2706-4. Экземпляры: всего 10.	10
ЭЛЕКТРОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ		
1.	Научная электронная библиотека eLIBRARY.RU	<a href="http://elibrary.ru">http://elibrary.ru</a>
2.	Научная электронная библиотека «Киберленинка»	<a href="http://cyberleninka.ru">http://cyberleninka.ru</a>
ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ		
1.	Справочно-правовая система Консультант+	<a href="http://www.consultant.ru">http://www.consultant.ru</a>
2.	Информационно-правовой портал Гарант	<a href="http://www.garant.ru">http://www.garant.ru</a>
3.	Профессиональные справочные системы Техэксперт	<a href="http://www.cntd.ru">http://www.cntd.ru</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.	107 (III)	Анализатор линейных коммуникаций УЛАН-2 (1), Генератор шума Соната -P2 (1), Доска маркерная 100*200см (1), ИБП UPS 1100VA (7), Коммутатор D-Link DES-3200-28 (8), Коммутатор D-Link DES-3810-28 (2), Комплекс защиты информации Secret Disk 4.0 (1), Комплекс защиты информации Secret Net 5.0 (2), Компьютер RAMEC STORM Custom i7-3770K/8ГБ/ монитор LCD 21.5", клавиат.,мышь (15), Нелинейный локатор SEL SP-61/М "Катран" (1), Ноутбук Acer Aspire 3 A315-42 (1), ПК Intel Core i7/GA-Z77-D3H/DDR3 8Gb/500Gb SATA II/INWIN ATX-450, Монитор BenQ	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



		G2450NM,клав,мышь (3), ПК Intel Core i7/GA-Z77-D3H/DDRIII 8Gb/500Gb SATAIII/INWIN EAR003, Монитор 24" BenQ G2450NM,клав,мышь (2), Проектор мультимедийный Hitachi CP-X1250+разветвитель видеосигнала (1), Система виброакустической защиты "Соната-AB" (1), Система виброакустической.защиты "Соната-PC2" (1), Средства ограничения доступа к компьютеру АПМДЗ "КРИПТОН-ЗАМОК/Е" (2), Экран настенный 200*200см Braun Roll Vision (1), Комплект учебной мебели (1)	
--	--	--	--

## 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	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.

#### **МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

### **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1**

По модулю: «Программно-аппаратные средства информационной безопасности»

#### **1. Дискреционное управление доступом. Определение, задачи и функции.**

#### **2. Механизмы журналирования и регистрации событий**

Зав. кафедрой ИБ \_\_\_\_\_ И.Г. Сидоркина

«\_\_\_» \_\_\_\_\_ 20\_\_ г.

## **Примеры типовых заданий**

1. Основные принципы создания средств защиты информации;
2. Концепция построения ПАСОИБ;
3. Структура, функции и задачи ПАСОИБ;
4. Методы ограничения и управления доступом. Идентификация и аутентификация. Парольные системы;
5. Методы ограничения и управления доступом. Дискреционное управление доступом;
6. Методы ограничения и управления доступом. Мандатное управление доступом;

7. Методы ограничения и управление доступом. Ролевое управление доступом.
8. Цели и задачи диспетчера доступа;
9. Сравнительные характеристики основных подходов к разработке ПАСОИБ;
10. Количественные характеристики парольных систем. Правила выбора стойких паролей;
11. Назначение, задачи и принципы создания механизма замкнутой программной среды.
12. Концепция распространения прав доступа;

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

**БИЛЕТ № 1**

По модулю: «Программно-аппаратные средства информационной безопасности»

1. Анализаторы уязвимостей подсистемы разграничения доступа;
2. Дели и задачи системы анализа контроля целостности данных, средств их фиксации и журналирования изменений;

Зав. кафедрой ИБ \_\_\_\_\_ И.Г. Сидоркина

«\_\_\_» \_\_\_\_\_ 20\_\_ г.

**Перечень вопросов для проведения промежуточной аттестации**

Вопросы для зачета:

1. Основные принципы создания средств защиты информации;
2. Концепция построения ПАСОИБ;
3. Структура, функции и задачи ПАСОИБ;
4. Методы ограничения и управления доступом. Идентификация и аутентификация. Парольные системы;
5. Методы ограничения и управления доступом. Дискреционное управление доступом;
6. Методы ограничения и управления доступом. Мандатное управление доступом;
7. Методы ограничения и управление доступом. Ролевое управление доступом.
8. Цели и задачи диспетчера доступа;
9. Сравнительные характеристики основных подходов к разработке ПАСОИБ;
10. Количественные характеристики парольных систем. Правила выбора стойких паролей;
11. Назначение, задачи и принципы создания механизма замкнутой программной среды.
12. Концепция распространения прав доступа;

Вопросы для экзамена:

1. Контроль и управление потоками данных посредством мандатного механизма управления доступом;
2. Основные руководящие документы, определяющие структуру и функции СЗИ.
3. Назначение и принципы функционирования программно-аппаратных комплексов защиты информации;
4. Варианты применения программно-аппаратных комплексов защиты информации;
5. Механизмы блокирования загрузки ОС со съёмных носителей;
6. Механизмы контроля целостности защищаемых данных;
7. Механизмы журналирования и регистрации событий.
8. Функциональные возможности различных комплексов ПАСОИБ;
9. Функционирование механизмов идентификации и аутентификации различных комплексов ПАСОИБ;
10. Организация замкнутой программной среды в различных комплексах ПАСОИБ;
11. Контроль доступа к устройствам и протоколам обмена данными в различных комплексах ПАСОИБ;
12. Управление крипто-потоками в различных комплексах ПАСОИБ.
13. Принципы и способы развёртывания сетевых решений различных комплексов ПАСОИБ;
14. Механизмы администрирования локальных рабочих станций в сетевых реализациях различных комплексов ПАСОИБ;
15. Внутрисетевое взаимодействие в защищенных локальных сетях;
16. Принципы организации защиты информации с применением «тонкого клиента».
17. Оценка эффективности СЗИ. Основные оцениваемые защитные механизмы СЗИ от НСД;
18. Оценка эффективности СЗИ от НСД. Задача контроля эффективности:
19. Порядок оценки механизма управления доступом при проведении контроля эффективности СЗИ от НСД;
20. Порядок оценки механизмов гарантированного удаления информации и затирания памяти.
21. Анализаторы уязвимостей подсистемы разграничения доступа;
22. Дели и задачи системы анализа контроля целостности данных, средств их фиксации и журналирования изменений;
23. Контроль функционирования подсистем регистрации и учёта. Состав, структура и назначение журналов ПАСОИБ;
24. Антивирусная подсистема СЗИ от НСД. Задачи, назначение, порядок её применения, установки и эксплуатации.
25. Назначение и принципы работы межсетевых экранов;
26. Защита локальных сетей с помощью аппаратно-программных комплексов шифрования;
27. Централизованное управление сетевыми устройствами с применением сценариев автоматической настройки;
28. Тестирование защищенных сетей на «проникновение» и качество обмена информацией.