



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГЕОДЕЗИИ И КАРТОГРАФИИ
(МИИГАиК)

Факультет геоинформатики и информационной безопасности
Кафедра информационно-измерительных систем



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 5387FD2AF5B17FED816FDE9A1D4973B1
Владелец: Степанченко Алексей Леонидович
Действителен: с 21.07.2025 по 14.10.2026

«УТВЕРЖДАЮ»

Проректор
А. Л. Степанченко
16 февраля 2024 г.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)
«Б1.В.06 АРХИТЕКТУРА ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»**

Уровень высшего образования: магистратура

Направление подготовки: 10.04.01 Информационная безопасность

Направленность(профиль) подготовки: Защита информации в геоинформационных системах
и системах сбора пространственных данных

Квалификация (степень) выпускника: магистр

Форма обучения: очная

Год набора (приема на обучение): 2024

Срок получения образования: 2 года

Объем:
в зачетных единицах: 5 з.е.
в академических часах: 180 ак.ч.

Москва, 2024

Разработчики:

Доцент кафедры Информационно-измерительных систем, к.т.н.
Тележников В. Ю.

Фонд оценочных средств по дисциплине (модулю) составлен в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки от 26.11.2020 № 1455

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Геоинформатики и информационной безопасности	Председатель ученого совета факультета	Матерухин А. В.	Рассмотрено	14.12.2023, № 7-23

1. Планируемые результаты обучения, соотнесенные с планируемыми результатами освоения образовательной программы

ПК-3 Способен разрабатывать проектные решения по защите информации автоматизированных систем (в том числе в геоинформационных системах)

ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности

Знать:

ПК-3.1/Зн1 нормативно-правовые документы в области защиты информации, определяющие виды тайн и устанавливающие степени конфиденциальности

Уметь:

ПК-3.1/Ум1 классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности

Владеть:

ПК-3.1/Нв1 методами анализа и оценки информации на предмет ее соответствия критериям отнесения к различным видам тайны и степеням конфиденциальности

ПК-3.2 Определяет типы субъектов доступа и объектов доступа, являющихся объектами защиты

Знать:

ПК-3.2/Зн1 нормативные и методические документы, регламентирующие классификацию субъектов и объектов доступа

ПК-3.2/Зн2 принципы и методы организационной защиты информации

Уметь:

ПК-3.2/Ум1 определять объекты доступа, которые подлежат защите, на основании их функционального назначения и чувствительности информации

Владеть:

ПК-3.2/Нв1 навыками работы с системами управления доступом и средствами контроля доступа

ПК-3.3 Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации

Знать:

ПК-3.3/Зн1 регламенты работ по обеспечению информационной безопасности автоматизированных систем

Уметь:

ПК-3.3/Ум1 разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности распределенных информационных систем

Владеть:

ПК-3.3/Нв1 навыками разработки проектов нормативных документов, регламентирующих работу по защите информации в организации

ПК-3.4 Понимает принципы построения и функционирования современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем)

Знать:

ПК-3.4/Зн1 принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем)

ПК-3.4/Зн3 технологии проектирования и построения защищенных информационных систем

Уметь:

ПК-3.4/Ум1 анализировать и выбирать оптимальную топологию и архитектуру сети с учетом требований и условий эксплуатации

Владеть:

ПК-3.4/Нв1 навыками проектирования и построения локальных и глобальных компьютерных сетей с использованием современных технологий и оборудования

2. Показатели и критерии оценивания компетенций

Планируемые результаты освоения программы	Уровень овладения	Критерии оценивания (перечень сформированных ИДК/ЗУВ по уровням освоения)
ПК-3 Способен разрабатывать проектные решения по защите информации автоматизированных систем (в том числе в геоинформационных системах)	Повышенный	ИДК ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности Знать: ПК-3.1/Зн1 нормативно-правовые документы в области защиты информации, определяющие виды тайн и устанавливающие степени конфиденциальности Уметь: ПК-3.1/Ум1 классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности Владеть: ПК-3.1/Нв1 методами анализа и оценки информации на предмет ее соответствия критериям отнесения к различным видам тайны и степеням конфиденциальности
ПК-3 Способен разрабатывать проектные решения по защите информации автоматизированных систем (в том числе в геоинформационных системах)	Повышенный	ИДК ПК-3.2 Определяет типы субъектов доступа и объектов доступа, являющихся объектами защиты Знать: ПК-3.2/Зн1 нормативные и методические документы, регламентирующие классификацию субъектов и объектов доступа ПК-3.2/Зн2 принципы и методы организационной защиты информации Уметь: ПК-3.2/Ум1 определять объекты доступа, которые подлежат защите, на основании их функционального назначения и чувствительности информации Владеть: ПК-3.2/Нв1 навыками работы с системами управления доступом и средствами контроля доступа

	ИДК ПК-3.3 Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации Знать: ПК-3.3/Зн1 регламенты работ по обеспечению информационной безопасности автоматизированных систем автоматизированных систем Уметь: ПК-3.3/Ум1 разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности распределенных информационных систем Владеть: ПК-3.3/Нв1 навыками разработки проектов нормативных документов, регламентирующих работу по защите информации в организации ИДК ПК-3.4 Понимает принципы построения и функционирования современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) Знать: ПК-3.4/Зн1 принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) ПК-3.4/Зн3 технологии проектирования и построения защищенных информационных систем Уметь: ПК-3.4/Ум1 анализировать и выбирать оптимальную топологию и архитектуру сети с учетом требований и условий эксплуатации Владеть: ПК-3.4/Нв1 навыками проектирования и построения локальных и глобальных компьютерных сетей с использованием современных технологий и оборудования
Базовый	ИДК ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности Знать: ПК-3.1/Зн1 нормативно-правовые документы в области защиты информации, определяющие виды тайн и устанавливающие степени конфиденциальности Уметь: ПК-3.1/Ум1 классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности

Базовый	ИДК ПК-3.2 Определяет типы субъектов доступа и объектов доступа, являющихся объектами защиты Знать: ПК-3.2/Зн2 принципы и методы организационной защиты информации ПК-3.2/Зн1 нормативные и методические документы, регламентирующие классификацию субъектов и объектов доступа Уметь: ПК-3.2/Ум1 определять объекты доступа, которые подлежат защите, на основании их функционального назначения и чувствительности информации ИДК ПК-3.3 Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации Знать: ПК-3.3/Зн1 регламенты работ по обеспечению информационной безопасности автоматизированных систем автоматизированных систем Уметь: ПК-3.3/Ум1 разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности распределенных информационных систем ИДК ПК-3.4 Понимает принципы построения и функционирования современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) Знать: ПК-3.4/Зн3 технологии проектирования и построения защищенных информационных систем ПК-3.4/Зн1 принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) Уметь: ПК-3.4/Ум1 анализировать и выбирать оптимальную топологию и архитектуру сети с учетом требований и условий эксплуатации
---------	--

	Пороговый	ИДК ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности Знать: ПК-3.1/Зн1 нормативно-правовые документы в области защиты информации, определяющие виды тайн и устанавливающие степени конфиденциальности
	Пороговый	ИДК ПК-3.2 Определяет типы субъектов доступа и объектов доступа, являющихся объектами защиты Знать: ПК-3.2/Зн2 принципы и методы организационной защиты информации ПК-3.2/Зн1 нормативные и методические документы, регламентирующие классификацию субъектов и объектов доступа ИДК ПК-3.3 Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации Знать: ПК-3.3/Зн1 регламенты работ по обеспечению информационной безопасности автоматизированных систем автоматизированных систем ИДК ПК-3.4 Понимает принципы построения и функционирования современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) Знать: ПК-3.4/Зн3 технологии проектирования и построения защищенных информационных систем ПК-3.4/Зн1 принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем)

3. Шкала оценивания

Оценка	Критерии оценивания (перечень сформированных ИДК/ЗУВ)
--------	---

Отлично	ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности ПК-3.1/Зн1 нормативно-правовые документы в области защиты информации, определяющие виды тайн и устанавливающие степени конфиденциальности ПК-3.1/Ум1 классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности ПК-3.1/Нв1 методами анализа и оценки информации на предмет ее соответствия критериям отнесения к различным видам тайны и степеням конфиденциальности ПК-3.2 Определяет типы субъектов доступа и объектов доступа, являющихся объектами защиты ПК-3.2/Зн1 нормативные и методические документы, регламентирующие классификацию субъектов и объектов доступа ПК-3.2/Зн2 принципы и методы организационной защиты информации ПК-3.2/Ум1 определять объекты доступа, которые подлежат защите, на основании их функционального назначения и чувствительности информации ПК-3.2/Нв1 навыками работы с системами управления доступом и средствами контроля доступа ПК-3.3 Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации ПК-3.3/Зн1 регламенты работ по обеспечению информационной безопасности автоматизированных систем автоматизированных систем ПК-3.3/Ум1 разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности распределенных информационных систем ПК-3.3/Нв1 навыками разработки проектов нормативных документов, регламентирующих работу по защите информации в организации ПК-3.4 Понимает принципы построения и функционирования современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) ПК-3.4/Зн1 принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) ПК-3.4/Зн3 технологии проектирования и построения защищенных информационных систем ПК-3.4/Ум1 анализировать и выбирать оптимальную топологию и архитектуру сети с учетом требований и условий эксплуатации ПК-3.4/Нв1 навыками проектирования и построения локальных и глобальных компьютерных сетей с использованием современных технологий и оборудования
Хорошо	ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности ПК-3.1/Зн1 нормативно-правовые документы в области защиты информации, определяющие виды тайн и устанавливающие степени конфиденциальности ПК-3.1/Ум1 классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности ПК-3.2 Определяет типы субъектов доступа и объектов доступа, являющихся объектами защиты ПК-3.2/Зн1 нормативные и методические документы, регламентирующие классификацию субъектов и объектов доступа ПК-3.2/Зн2 принципы и методы организационной защиты информации ПК-3.2/Ум1 определять объекты доступа, которые подлежат защите, на основании их функционального назначения и чувствительности информации

	ПК-3.3 Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации ПК-3.3/Зн1 регламенты работ по обеспечению информационной безопасности автоматизированных систем автоматизированных систем ПК-3.3/Ум1 разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности распределенных информационных систем ПК-3.4 Понимает принципы построения и функционирования современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) ПК-3.4/Зн1 принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) ПК-3.4/Зн3 технологии проектирования и построения защищенных информационных систем ПК-3.4/Ум1 анализировать и выбирать оптимальную топологию и архитектуру сети с учетом требований и условий эксплуатации
Удовлетворительно	ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности ПК-3.1/Зн1 нормативно-правовые документы в области защиты информации, определяющие виды тайн и устанавливающие степени конфиденциальности ПК-3.2 Определяет типы субъектов доступа и объектов доступа, являющихся объектами защиты ПК-3.2/Зн1 нормативные и методические документы, регламентирующие классификацию субъектов и объектов доступа ПК-3.2/Зн2 принципы и методы организационной защиты информации ПК-3.3 Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации ПК-3.3/Зн1 регламенты работ по обеспечению информационной безопасности автоматизированных систем автоматизированных систем ПК-3.4 Понимает принципы построения и функционирования современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) ПК-3.4/Зн1 принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) ПК-3.4/Зн3 технологии проектирования и построения защищенных информационных систем
Неудовлетворительно	Результаты обучения не сформированы на достаточном уровне

4. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	Коллоквиум
Промежуточная аттестация	Экзамен

№ п/п	Наименование раздела	Контролируемые ИДК	Вид контроля/ используемые оценочные материалы	
			Текущий	Промежут. аттестация

1	Основные понятия и классификация защищенных автоматизированных систем	ПК-3.1 ПК-3.2		Экзамен
2	Основы защиты информации в защищенных автоматизированных системах	ПК-3.1 ПК-3.2 ПК-3.3		Экзамен
3	Основы организации разработки защищенных АС	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4		Экзамен
4	Общие принципы проектирования защищенных АС	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4		Экзамен
5	Работа с данными в автоматизированных информационных системах	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4	Коллоквиум	Экзамен

5. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

- Положением о формах, периодичности, порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.6 «Организация и проведение промежуточной аттестации».
- Положением о порядке осуществления образовательного процесса, проведения текущего контроля успеваемости и промежуточной аттестации обучающихся с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.8 «Проведение промежуточной аттестации с применением ЭО и ДОТ».

Промежуточная аттестация: Экзамен, 4 семестр.

Экзамен оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется, если обучающийся имеет глубокие, исчерпывающие знания в объеме освоенной программы; знание основной (обязательной) литературы; дает правильные и уверенные ответы, свидетельствующие о наличии твердых знаний и навыков в использовании технических средств; полное, четкое, грамотное и логически стройное изложение материала; демонстрирует свободное применение теоретических знаний при анализе практических вопросов;
- зачтено с оценкой «хорошо» выставляется обучающемуся в случае соблюдения тех же требований, но наличия в ответе обучающегося по некоторым перечисленным показателям недостатков принципиального характера, что вызывает замечания или поправки преподавателя;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся в случае соблюдения тех же требований, но в случае наличия в ответе ошибок, необходимости существенной помощи в виде поправок и наводящих вопросов преподавателя;
- не зачтено («не удовлетворительно») – обучающийся не смог ответить на 2/3 вопросов; не справился с практическим заданием или выполнено менее 50 % практических заданий.

6. Оценочные материалы текущего контроля

Раздел 5. Работа с данными в автоматизированных информационных системах

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 5.1. Работа с данными в автоматизированных информационных системах

Форма контроля/оценочное средство: Коллоквиум

Вопросы/Задания:

1. Дайте определение автоматизированной системы согласно ГОСТ Р 59853-2021.
2. Дайте определение жизненного цикла автоматизированной системы ГОСТ Р 59853-2021.
3. Дайте определение интероперабельности согласно ГОСТ Р 59853-2021.
4. Перечислите основные виды испытаний автоматизированной системы согласно ГОСТ Р 59792-2021.
5. Какие этапы работ включает в себя стадия формирования требований к автоматизированной системе согласно ГОСТ Р 59793-2021?
6. Что включает в себя схема функциональной инфраструктуры автоматизированной системы согласно ГОСТ Р 59795-2021?
7. Что подлежит проверке на этапе проверки полноты и качества выполнения функций автоматизированной системы согласно ГОСТ 59792-2021?
8. Дайте определение верификации формальной модели управления доступом согласно ГОСТ Р 59453.2-2021.
9. Приведите примеры формальных методов, языки которых позволяют строить абстрактные автоматные модели управления доступом согласно ГОСТ Р 59453.2-2021.
10. Дайте определение «скрытого канала» согласно ГОСТ Р 59453.1-2021.
11. Что не входит в состав автономных испытаний автоматизированной системы согласно ГОСТ Р 59792-2021?
 - а) перечень и комплектность объектов автономных испытаний;
 - б) описание взаимодействия пользователей с комплексами программных и технических средств;
 - в) порядок устранения недостатков, выявленных в процессе опытной эксплуатации.
12. Что не входит в стадию технического проекта создания автоматизированной системы согласно ГОСТ 59793-2021?
 - а) Разработка проектных решений по АС и ее частям;
 - б) Разработка рабочей документации на АС и ее части;
 - в) Разработка и оформление документации на поставку изделий для комплектования АС и (или) технических требований (технических заданий) на их разработку.
13. Что не относится к разделу «Входная информация» при подготовке документации на автоматизированную систему согласно ГОСТ 59795-2021?
 - а) описание массива информации;
 - б) перечень и описание входных сообщений (идентификатор, форму представления, сроки и частоту поступления, допустимые форматы данных);
 - в) перечень и описание структурных единиц информации входных сообщений или ссылку на документы, содержащие эти данные.
14. Какой подраздел не должен содержать раздел «Описание внутримашинной информационной базы» при подготовке документации на автоматизированную систему согласно ГОСТ 59795-2021?
 - а) логическая структура;
 - б) физическая структура;
 - в) описание используемых методов классификации и кодирования.
15. Какие разделы входят в состав требований к содержанию документов с решениями по программному обеспечению автоматизированной системы согласно ГОСТ 59795-2021?
 - а) операционная система;
 - б) ограничения на возможность и условия применения алгоритма и характеристики качества решения (точность, время решения и т. д.);
 - в) функции частей программного обеспечения АС.

16. Что должно быть последовательно описано при переводе математического описания в формализованное (машиночитаемое) описание формальной модели управления доступом должны согласно ГОСТ Р 59453.2-2021?

- а) правила перехода абстрактного автомата из состояний в состояния, при этом допустимо объединение нескольких правил в одно или разбиение некоторого правила на несколько с сохранением его свойств;
- б) условия выполнения политик управления доступом в состояниях абстрактного автомата и при переходах из состояний в состояния абстрактного автомата (условия безопасности);
- в) возможности по подключению и комбинированного использования библиотек (пруверов - инструментов для доказательства теорем, солверов - инструментов для решения систем уравнений).

17. Выберите правильное определение политики мандатного контроля целостности со-гласно ГОСТ Р 59453.1-2021.

- а) политика управления доступом, при реализации которой задается матрица доступов, строки которой соответствуют субъектам доступа (учетным записям пользователей), столбцы - объектам или субъектам доступа, ячейки - множеству прав доступа соответствующего строке субъекта доступа к соответствующему столбцу объекту или другому субъекту доступа;
- б) политика управления доступом, при реализации которой задаются классификационные метки (уровни целостности): каждому объекту и субъекту доступа присваивается уровень целостности;
- в) политика управления доступом, при реализации которой задаются классификационные метки (уровни конфиденциальности, уровни доступа): каждому объекту доступа присваивается уровень конфиденциальности, каждому субъекту доступа присваивается уровень доступа (являющийся элементом множества уровней конфиденциальности).

7. Оценочные материалы промежуточной аттестации

4 семестр, Экзамен

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Вопросы/Задания:

1. Классификация автоматизированных систем (АС).
2. Информационные технологии, используемые в АС.
3. Жизненный цикл АС.
4. Основные угрозы безопасности информации в автоматизированных системах.
5. Отказоустойчивость АС.
6. Понятия информации и информационных ресурсов.
7. Предмет защиты информации.
8. Объект защиты информации.
9. Понятие информационной безопасности.
10. Понятие политики информационной безопасности.

11. Понятие системы защиты информации.
12. Основные положения безопасности автоматизированных систем.
13. Трехэтапная разработка мер по обеспечению безопасности автоматизированных систем.
14. Стадия выработки требований.
15. Стадия определения способов защиты.
16. Стадия определения функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты.
17. Основные принципы обеспечения информационной безопасности в автоматизированной системе (АС).
18. Принципы, позволяющие реализовать положения по защите АС.
19. Принцип системности.
20. Принцип комплексности.
21. Принцип непрерывной защиты.
22. Последовательность и содержание этапов разработки АС.
23. Методы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем.
24. Методы и средства обеспечения отказоустойчивости автоматизированных систем.
25. Критерии оценки защищенности АС.
26. Методы обеспечения информационной безопасности АС.
27. Организация коллективной разработки программного обеспечения АС.
28. Проектирование защищенных АС.
29. Методы проектирования.
30. Содержание этапов проектирования.
31. Основы ведения конструкторской документации.
32. Структура и содержание технического задания.
33. Построение комплексной защиты АС.

НСД.

34. Основы проектирования комплексной защиты информационной безопасности от

35. Средства обеспечения надежности защищенных АС.

36. Организация хранения информации в защищенных АС.

37. Жизненный цикл АС.

38. Порядок создания изделий ИТ, удовлетворяющих требованиям безопасности.

39. Архитектура построения защищенных АС.

40. Содержание угроз безопасности АС.

41. Классификация угроз безопасности информации АС.

42. Реальные и мнимые угрозы безопасности защищаемой информации в АС.

43. Методы анализа угроз безопасности АС.

44. Политика безопасности АС.

45. Защита информации в АС обработки данных.

46. Объекты защиты информации в АС.

47. Жизненный цикл защищенных АС.

48. Концепция комплексной защиты информации.

49. Принципы построения распределенных АС.

50. Принципы функционирования распределенных АС.

51. Состав и основные характеристики методов защиты информации в АС.