



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

«МИРЭА – Российский технологический университет»

**РТУ МИРЭА**

---

---

**УТВЕРЖДАЮ**

Первый проректор

\_\_\_\_\_ Н.И. Прокопов  
« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

## **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

### **2.1.6 «Методы и системы защиты информации, информационная безопасность»**

Научная специальность

### **2.3.6 «Методы и системы защиты информации, информационная безопасность»**

Форма обучения

**Очная**

Москва 2025

### **1. Цели освоения дисциплины**

Целями освоения дисциплины «Методы и системы защиты информации, информационная безопасность» являются:

1. Формирование систематических знаний в области теоретических основ информационной безопасности.
2. Овладение базовыми знаниями методов защиты информации и информационной безопасности, основами построения моделей противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющих получать оценки показателей информационной безопасности.
3. Изучение основных принципов и решений (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

### **2. Место дисциплины в структуре программы аспирантуры**

Дисциплина «Методы и системы защиты информации, информационная безопасность» является обязательной дисциплиной образовательного компонента блока «Дисциплины (модули)» учебного плана научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

### **3. Требования к результатам освоения дисциплины «Методы и системы защиты информации, информационная безопасность»**

В ходе освоения дисциплины «Методы и системы защиты информации, информационная безопасность» идет дальнейшее формирование элементов (знаний, умений, навыков и (или) опыта деятельности) аспиранта:

- способность к самостоятельному обучению новым методам исследования;
- способность к пониманию основных проблем в своей предметной области, выбору методов и средств их решения;
- способность самостоятельно приобретать и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой своих исследований;
- способность анализировать состояние научно-технической проблемы, систематизировать и обобщать научно-техническую информацию по теме исследований;
- способность оценивать научную значимость и перспективы прикладного использования результатов исследований.

В результате освоения дисциплины аспирант должен:

Знать:

общие проблемы и задачи информационной безопасности;

модели и методы управления информационной безопасностью, непрерывным функционированием и восстановлением систем, противодействия отказам в обслуживании средств идентификации, классификации и анализа угроз нарушения информационной безопасности;

методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов информатизации;

методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет;

методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия деструктивным воздействиям различного генеза (происхождения);

методы оценки эффективности функционирования систем защиты информации.

Уметь:

использовать реферативные базы журнальных и патентных публикаций;

обосновывать актуальность поставленной исследовательской задачи и решать её с помощью современных технологий и достижений;

использовать разработанные методы и подходы для решения возникающих задач в ходе профессиональной деятельности.

Владеть:

понятийным аппаратом, необходимым для решения профессиональных и исследовательских задач;

методами математического моделирования для постановки и решения основных видов задач исследовательской деятельности;

методами анализа и систематизации результатов научно-исследовательской работы, подготовки презентаций, научных отчетов.

#### 4. Содержание дисциплины

Общая трудоемкость дисциплины «Методы и системы защиты информации, информационная безопасность» составляет 3 зачетных единицы (108 акад. часов).

**4.1. Распределение объема дисциплины по разделам (темам), семестрам, видам учебной работы и формам контроля.**

№ раздела	Семестр	Неделя семестра	Объем (в акад. час.)						Формы текущего контроля успеваемости (по неделям семестра)	
			Всего	Контактная работа (по видам учебных занятий)			СР	Контроль		
				Всего	ЛК	ПР			СР под рук.	Формы промежуточной аттестации (по семестрам)
1	4	1	8	4	4			4		Устное собеседование
1	4	4	6	2		2		2	2	Выполнение практических

№ раздела	Семестр	Неделя семестра	Объем (в акад. час.)							Формы текущего контроля успеваемости (по неделям семестра)  Формы промежуточной аттестации (по семестрам)	
			Всего	Контактная работа (по видам учебных занятий)				СР	Контроль		
				Всего	ЛК	ПР	СР под рук.				
										заданий	
2	4	5	8	4	4			4		Устное собеседование	
2	4	8	6	2		2		2	2	Выполнение практических заданий	
3	4	9	8	4	4			4		Устное собеседование	
3	4	10	8	2		2		2	4	Выполнение практических заданий	
4	4	11	8	4	4			4		Устное собеседование	
4	4	12	8	2		2		2	4	Выполнение практических заданий	
5	4	13	8	4	4			4		Устное собеседование	
5	4	14	8	2		2		2	4	Выполнение практических заданий	
6	4	17	8	4	4			4		Устное собеседование	
6	4	18	8	2		2		2	4	Выполнение практических заданий	
По материалам курса			16						16	Экзамен	
Всего в 4 семестре:			108	36	24	12	0	36	36		
Всего:			108	36	24	12	0	36	36		

#### 4.2. Наименование и содержание разделов дисциплины

Номер темы	Наименование темы	Содержание темы
1	Задачи информационной безопасности.	Предметная область теории информационной безопасности. Основные понятия в области защиты информации. Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Основные принципы построения систем защиты информации. Концепция комплексной защиты информации. Задачи защиты информации. Средства реализации комплексной защиты информации. Информация как объект защиты. Уровни представления информации. Основные свойства защищаемой информации. Виды и формы представления информации. Информационные ресурсы.
2	Построение систем защиты информации.	Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз информационной

Номер темы	Наименование темы	Содержание темы
		безопасности. Разработка моделей угроз и злоумышленника информационной безопасности. Моделирование деструктивных злоумышленных воздействий на систему. Оценка уязвимости системы. Разработка политики информационной безопасности. Модели разграничения доступа к данным.
3	Средства идентификации, классификации и анализа угроз информационной безопасности.	Обеспечение целостности информации при обработке данных. Виды угроз нарушения целостности данных. Методы и средства предупреждения и предотвращения угроз нарушения целостности информации на уровне содержания. Методы и средства предупреждения и предотвращения угрозы отказа доступа к информации. Защита семантического анализа и актуальности информации. Определение и основные способы предотвращения несанкционированного доступа к данным. Методы защиты от НСД. Методы и средства защиты информации от угрозы утечки по техническим каналам связи. Идентификация и аутентификация пользователей в системе. Основные направления и цели использования криптографических методов защиты информации. Методы и средства предупреждения и предотвращения угроз нарушения конфиденциальности информации на контекстном уровне.
4	Повышение эффективности функционирования систем защиты информации.	Методы решения задач на поиск оптимальных систем по заданным критериям. Расчет показателей эффективности функционирования системы. Взаимосвязь между эффективностью и свойствами систем. Методы оценки эффективности функционирования систем. Оценка эффективности систем в условиях неопределенности. Показатели оценки эффективности и методы их определения. Способы вычисления сложных показателей эффективности. Методы и модели построения оптимальных СЗИ.
5	Предупреждение, обнаружение и противодействие угрозам и компьютерным атакам	Защищаемая информация и основные способы несанкционированного доступа (НСД) в автоматизированной системе: виды информации, подлежащей защите. Классы и виды компьютерных атак. Основные методы и средства защиты информации. Роль и место программно-аппаратных средств защиты информации в КСЗИ: классификация средств защиты информации. Основные функции средств защиты информации от НСД. Механизмы защиты, реализуемые в программно-аппаратных СЗИ от НСД. Управление доступом. Регистрация и контроль критичных событий. Контроль целостности данных.

Номер темы	Наименование темы	Содержание темы
		Криптографическая защита. Примеры средств защиты информации от НСД. Защита от разрушающих программных воздействий, понятие разрушающих программных воздействий.
6	Управление информационной безопасностью.	Процессный подход к построению СУИБ и циклическая модель PDCA. Цели и задачи, решаемые СУИБ. Стандартизация в области построения СУИБ: сходства и различия стандартов. Стратегии определения области деятельности СУИБ. Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему). Основные этапы разработки СУИБ и роль руководства организации на каждом из этапов. Политика ИБ и политика СУИБ: сходства и различия. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.

### 4.3. Лабораторные работы (ЛБ)

Учебным планом не предусмотрены.

### 4.4. Практические занятия (ПР)

№ п/п	Номер темы дисциплины	Тематика практических занятий	Трудоемкость (в акад. часах)
1	1	Задачи информационной безопасности.	2
2	2	Построение систем защиты информации.	2
3	3	Средства идентификации, классификации и анализа угроз нарушения информационной безопасности.	2
4	4	Повышение эффективности функционирования систем защиты информации.	2
5	5	Предупреждение, обнаружение и противодействие угрозам и компьютерным атакам	2
6	6	Управление информационной безопасностью.	2
<b>Всего:</b>			<b>12</b>

## 5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине

Виды самостоятельной работы обучающегося, порядок и сроки ее выполнения:

подготовка к лекциям и практическим занятиям с использованием конспекта лекций, материалов практических занятий и приведенных ниже

(п 8.1 и 8.2) источников (в соответствии с расписанием занятий);

оформление отчетов по выполненным практическим заданиям и теоретическая подготовка к их сдаче (в соответствии с расписанием занятий).

Перечень вопросов для проведения текущего контроля и промежуточной аттестации – в соответствии с тематикой дисциплины.

## **6. Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине**

### **6.1. Описание показателей и критериев оценивания знаний, умений и владений на различных этапах их формирования, описание шкал оценивая**

#### **6.1.1. Показатели и критерии оценивания, используемые шкалы оценивания**

<b>Показатели оценивания</b>	<b>Критерии оценивания</b>	<b>Средства оценивания</b>	<b>Шкалы оценивания</b>
<b>Умение</b>	Правильность выполнения учебных заданий, аргументированность выводов	<i>Текущий контроль:</i> выполнение устных/письменных заданий, тестирование  <i>Промежуточная аттестация:</i> экзамен	Шкала 1
<b>Знание</b>	Правильность и полнота ответов, глубина понимания вопроса	<i>Текущий контроль:</i> выполнение устных/письменных заданий, тестирование  <i>Промежуточная аттестация:</i> экзамен	Шкала 1
<b>Владение</b>	Обоснованность и аргументированность выполнения учебной деятельности	<i>Текущий контроль:</i> выполнение практического задания, тестирование  <i>Промежуточная аттестация:</i> экзамен	Шкала 2

#### **6.1.2. Описание шкал оценивания степени сформированности знаний, умений и владений**

##### **Шкала 1. Оценка сформированности знаний, умений и владений**

<b>Обозначения</b>		<b>Формулировка требований к степени сформированности знаний, умений и владений</b>		
<b>Цифр.</b>	<b>Оценка</b>	<b>Знать</b>	<b>Уметь</b>	<b>Владеть</b>
1	Неудовлетворительно	Отсутствие знаний	Отсутствие умений	Отсутствие навыков
2	Неудовлетворительно	Фрагментарные знания	Частично освоенное умение	Фрагментарное применение
3	Удовлетворительно	Общие, но не структурированные	В целом успешное, но не	В целом успешное, но не

Обозначения		Формулировка требований к степени сформированности знаний, умений и владений		
Цифр.	Оценка			
		<b>Знать</b> знания	<b>Уметь</b> систематически осуществляемое умение	<b>Владеть</b> систематическое применение
4	Хорошо	Сформированные, но содержащие отдельные пробелы знания	В целом успешное, но содержащие отдельные пробелы умение	В целом успешное, но содержащее отдельные пробелы применение навыков
5	Отлично	Сформированные систематические знания	Сформированное умение	Успешное и систематическое применение навыков

**Шкала 2.** Комплексная оценка сформированности знаний, умений и владений

Обозначения		Формулировка требований к степени сформированности знаний, умений и владений
Цифр.	Оценка	
1	Неудовлетворительно	Не имеет необходимых представлений о проверяемом материале
2	Удовлетворительно или неудовлетворительно (по усмотрению преподавателя)	Знать на уровне <b>ориентирования</b> , представлений. Субъект учения знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает их в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения
3	Удовлетворительно	Знать и уметь на <b>репродуктивном</b> уровне. Субъект учения знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях
4	Хорошо	Знать, уметь, владеть на <b>аналитическом</b> уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения
5	Отлично	Знать, уметь, владеть на <b>системном</b> уровне. Субъект учения знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания учебной дисциплины, его значимость в содержании учебной дисциплины



**6.2. Типовые контрольные задания или иные материалы,** необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования знаний, умений и владений в процессе освоения образовательной программы.

**Типовые вопросы и задания для текущего контроля** (оценка сформированности элементов (знаний, умений, навыков) в рамках текущего контроля по дисциплине) по разделам дисциплины

***Примеры вопросов по теме 1:***

1. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
2. Национальные интересы РФ и стратегические национальные приоритеты.
3. Роль специалиста по защите информационной безопасности в обеспечении национальной безопасности государства.
4. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
5. Информационная безопасность Российской Федерации.
6. Интересы личности и общества в информационной сфере.
7. Интересы государства в информационной сфере.
8. Виды угроз информационной безопасности Российской Федерации.
9. Источники угроз информационной безопасности Российской Федерации.
10. Внешние и внутренние источники угроз информационной безопасности.
11. Направления обеспечения информационной безопасности государства.

***Пример практического задания по теме 1:***

Задание 1. Какая информация приводится в разделе «Требования к документированию» в соответствии с ГОСТ 34.602-2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

Ключ.

1. Перечень подлежащих разработке документов;
2. Требования по использованию ЕСКД и ЕСПД при разработке документов;
3. Вид представления и количество документов.

***Примеры вопросов по теме 2:***

1. Принципы построения и виды обеспечений АИС в ЗИ.
2. Стратегии разработки программного обеспечения АИС в ЗИ.
3. Модели жизненного цикла АИС в ЗИ, реализующие различные стратегии.
4. Технологии и методы проектирования АИС в ЗИ.
5. Разработка технического задания на АИС в ЗИ.

6. Графические элементы стандарта функционального моделирования.
7. Виды диаграмм стандарта функционального моделирования.
8. Преимущества и недостатки использования стандарта функционального моделирования.
9. Стандарт диаграмм потоков данных.
10. Стандарт моделирования атомарных функций в виде потоков работ.

***Пример практического задания по теме 2:***

Задание 1. Для разработки защищенной автоматизированной системы предполагается использовать инструментальное средство Bizagi Modeler, реализующее нотацию BPMN 2.0. Перечислите виды маркеров, которые при этом могут быть использованы:

Ключ

1. Подпроцесс;
2. Обычный цикл;
3. Параллельное выполнение;
4. Последовательное исполнение;
5. Компенсация;
6. Операция «по случаю» (Ad-Hoc).

***Примеры вопросов по теме 3:***

1. Уязвимости в средствах ограничения программной среды, средствах стирания информации и контроля удаления информации относятся:

- \*к уязвимостям в средствах защиты информации;
- к активным уязвимостям;
- к пассивным уязвимостям.

2. Уязвимости в средствах ограничения программной среды, средствах стирания информации и контроля удаления информации, средствах защиты каналов передачи информации относятся:

- \*к уязвимостям в средствах защиты информации;
- к активным уязвимостям;
- к пассивным уязвимостям.

3. Классификация уязвимостей автоматизированных систем по типу уязвимости включает:

- \* уязвимость в программно-аппаратном обеспечении автоматизированных систем;
- уязвимости, находящиеся вне контролируемой зоны места расположения защищенной автоматизированной информационной системы;
- уязвимости, связанные с человеческим фактором.

4. Классификация уязвимостей в программно-аппаратном обеспечении автоматизированных систем по типу компонента таких систем, в котором содержится уязвимость включает:

- \*уязвимость рабочих станций защищенной автоматизированной информационной системы;
- уязвимости, связанные с человеческим фактором;

уязвимость в программно-аппаратном обеспечении автоматизированных систем.

5. Классификация уязвимостей автоматизированных систем по этапу жизненного цикла этих систем, на котором внедряется уязвимость, включает:

\*уязвимость технологического этапа;

уязвимость этапа установки программного обеспечения;

уязвимость в программно-аппаратном обеспечении автоматизированных систем.

***Пример практического задания по теме 3:***

Задание 1. Для защиты автоматизированной системы в защищенном исполнении предполагается использовать аппаратно-программный комплекс шифрования (АПШК) «Континент». Перечислите, какие компоненты может включать в свой состав данный комплекс.

Ключ:

1. Криптографический шлюз (КШ);
2. Центр управления сетью (ЦУС);
3. Сервер доступа (СД);
4. Детектор компьютерных атак (ДА);
5. Криптокоммутатор (КК);
6. Программа управления комплексом (ПУ);
7. Автоматизированное рабочее место генерации ключей (АРМ ГК);
8. Клиент аутентификации пользователя.

***Примеры вопросов по теме 4:***

1. Что такое большие системы?
2. Назовите принципы построения оптимальных СЗИ.
3. Перечислите методы перехода к скалярному показателю качества.
4. Назовите основные критерии оптимизации проектируемых систем.
5. Дайте определение эффективности как свойство достижения цели.

***Пример практического задания по теме 4:***

Задание 1. Проведите расчет технико-экономической эффективности и поиска оптимальной системы автоматизированной обработки информации по упрощенной методике.

***Примеры вопросов по теме 5:***

1. Генераторы случайных и псевдослучайных чисел. Применение их в приложениях сетевой безопасности.
2. Электронная подпись. Общие принципы работы, достоинства и недостатки.
3. Алгоритм электронной подписи DSA.
4. Алгоритм электронной подписи. Наборы параметров.
5. Обеспечение доступности информационных ресурсов в вычислительных сетях. Сетевые экраны. Классификация СЭ по ФСТЭК.
6. Обеспечение доступности информационных ресурсов в вычислительных сетях. Системы обнаружения и предотвращения вторжений. Классификации

ФСБ и ФСТЭК.

7. Технологии виртуальных частных сетей (VPN). Общие принципы, достоинства и недостатки.

8. Российские VPN-технологии, особенности, основные компоненты.

9. Технология ViPNet: состав и назначение компонентов.

10. Драйвер сетевой защиты ViPNet: принцип работы, основные функции.

11. ViPNet Client: варианты изготовления, принцип работы, основные функции.

12. ViPNet Coordinator: варианты изготовления, принцип работы, основные функции.

13. События и инциденты информационной безопасности. Состав и назначение комплекса ViPNet IDS 3.

14. Сигнатурный и эвристический анализ при выявлении событий информационной безопасности.

***Пример практического задания по теме 5:***

Задание 1. Какие действия надо выполнить для ViPNet Coordinator HW 4, чтобы сменить пароль пользователя этого сетевого узла? Пароль администратора данного сетевого узла?

Ключ: пароль пользователя может быть изменен локально, т.е. на координаторе, так и в удостоверяющем и ключевом центре (УКЦ) комплекса ViPNet Administrator 4. Пароль администратора – только в УКЦ.

Ответ: Для смены пароля пользователя возможно выполнить одно из следующих действий:

- издать новый DST-файл и развернуть его на координаторе;
- сменить пароль в УКЦ и успешно разослать обновления по сети ViPNet;
- перейти на самом координаторе в терминале ViPNet shell в режим администратора (команда enable) и выполнить смену пароля.

Для смены пароля администратора возможно выполнить только одно из первых двух вышеописанных действий.

***Пример вопросов по теме 6:***

1. Влияние инцидентов ИБ на бизнес-процессы.
2. Формы правовой защиты информации на предприятии.
3. Нормативные акты предприятия по информационной безопасности.
4. Метод оценки рисков на основе модели информационных потоков.
5. Роль стандартов информационной безопасности. Критерии оценки безопасности информационных систем.
6. Документы предприятия, в которых отражаются вопросы обеспечения информационной безопасности.

***Пример практического задания по теме 6:***

Вопросы письменной работы:

1. Анализ рисков ИБ: основные подходы, основные этапы процесса.
2. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.

3. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).

4. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.

5. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.

6. Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.

Задание 1. Каким документом определяются требования по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (ГИС). Какие работы осуществляются при принятии решения о необходимости защиты информации, содержащейся в информационной системе. Как проводится классификация ГИС, сколько классов установлено и от чего они зависят. В какой документ включаются требования к классу защищенности ГИС, на основании каких ГОСТов он оформляется. Каким документом закрепляются результаты классификации ГИС.

**Перечень вопросов для подготовки к экзамену** (оценка сформированности элементов (знаний, умений, навыков) в рамках промежуточной аттестации по дисциплине).

1. Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны.

2. Методы нарушения конфиденциальности, целостности и доступности информации.

3. Причины, виды, каналы утечки и искажения информации.

4. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.

5. Компьютерная система как объект информационной войны.

6. Формальные модели безопасности автоматизированных систем.

7. Назначение формальных моделей безопасности.

8. Политика безопасности.

9. Монитор безопасности обращений.

10. Дискреционная и мандатная модели разграничения доступа к данным.

11. Формальные модели управления доступом к данным.

12. Модель Харрисона-Руззо-Ульмана.

13. Интегрированное использование моделей разграничения доступа к данным в информационной системе.

14. Ролевое управление доступом к данным.

15. Моделирование предметной области с применением инструментального средства графического описания процессов в нотации

BPMN. Спецификация и области применения нотации BPMN. Операции. Логические операторы.

16. Моделирование предметной области с применением инструментального средства графического описания процессов в нотации BPMN. События. Соединительные элементы

17. Моделирование предметной области с применением инструментального средства графического описания процессов в нотации BPMN.Arteфакты. Элементы данных. Зоны ответственности. Исполняемые сценарии

18. Основные понятия в области моделирования данных.

19. Характеристика нотаций моделирования данных.

20. Шифрование на уровне базы данных.

21. Роли в программных проектах по созданию АИС в ЗИ.

22. Выполнение проекта по созданию АИС в ЗИ.

23. Наблюдение за проектом по созданию АИС в ЗИ.

24. Идентификация и анализ риска в программном проекте по созданию АИС в ЗИ.

25. Оценка риска информационной безопасности в программном проекте по созданию АИС в ЗИ.

26. Характеристика систем контроля версий программного обеспечения АИС в ЗИ.

27. Операции в системах контроля версий программного обеспечения АИС в ЗИ.

28. Понятие вычислительной сети. Классификация вычислительных сетей: ВАН, РАН, ЛАН, САН, МАН, ГАН. Локальные и распределенные вычислительные сети (ЛАН и ВАН).

29. Понятие вычислительной сети. Сетевые топологии.

30. Понятие вычислительной сети. Архитектуры сетей и архитектуры сетевых служб.

31. Классификация сред передачи данных. Коаксиальный кабель, витая пара, оптоволокно, беспроводная передача данных.

32. Сетевые модели OSI и TCP/IP (DoD). Назначение уровней, сравнение моделей.

33. Сетевые модели OSI и TCP/IP (DoD). Межуровневая инкапсуляция данных.

34. Методы и средства анализа сетевого трафика. Инструментальные программные пакеты (Wireshark, tcpdump). Особенности конфигурирования виртуальной машины для анализа трафика.

35. Обеспечение конфиденциальности данных в вычислительных сетях. Основные термины: идентификация, аутентификация, за-, рас- и дешифрование. Виды алгоритмов шифрования.

36. Симметричное шифрование. Алгоритм шифрования.

37. Симметричное шифрование. Алгоритм шифрования «Магма».

38. Асимметричное шифрование. Алгоритмы шифрования на базе эллиптических кривых.

39. Обеспечение целостности данных в вычислительных сетях. Криптографические хэш-функции, основные определения и требования.

40. Криптографические хэш-функции. Алгоритмы хэширования SHA-1.

41. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.

42. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).

43. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.

44. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.

45. Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.

46. Внедрение процессов управления ИБ: этапы и последовательность. Ввод СУИБ в эксплуатацию: возможные проблемы и способы их решения.

47. Правовые аспекты построения СУИБ организации.

48. Аудит первой, второй и третьей сторонами.

49. Подготовка и представление отчетов в устной и письменной форме о результатах аудита.

50. Влияние инцидентов ИБ на бизнес-процессы.

**6.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности.**

Процедуры и средства оценивания элементов знаний, умений и владений по дисциплине «Методы и системы защиты информации, информационная безопасность»

Процедура проведения	Средство оценивания				
	Текущий контроль				Промежуточный контроль
	Выполнение устных заданий	Выполнение письменных заданий	Выполнение практических заданий	Выполнение тестовых заданий	Экзамен
Продолжительность контроля	По усмотрению преподавателя	По усмотрению преподавателя	По усмотрению преподавателя	По усмотрению преподавателя	В соответствии с принятыми нормами времени
Форма проведения контроля	Устный опрос	Письменный опрос	Письменный опрос	Письменный опрос	В письменной форме
Вид проверочного задания	Устные вопросы	Письменные задания	Практические задания	Письменный опрос	Экзаменационный билет
Форма отчета	Устные ответы	Ответы в письменной форме	Ответы в письменной форме	Ответы в письменной форме	Ответы в письменной форме
Раздаточный материал	Нет	Справочная литература	Справочная литература	Справочная литература	Справочная литература

## **7. Методические указания для обучающихся по освоению дисциплины**

Дисциплина «Методы и системы защиты информации, информационная безопасность» предусматривает лекции и практические занятия. Успешное изучение дисциплины требует посещения лекций, активной работы на практических занятиях, выполнения учебных заданий преподавателя, ознакомления с основной и дополнительной литературой.

В ходе лекций преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации на практическое занятие и указания на самостоятельную работу.

При подготовке к лекционным занятиям аспирантам необходимо: перед очередной лекцией необходимо просмотреть конспект материала предыдущей лекции. При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале опять не удалось, то обратитесь к лектору (по графику его консультаций) или к преподавателю на практических занятиях.

Практические занятия завершают изучение наиболее важных тем учебной дисциплины. Они служат для закрепления изученного материала, развития умений и навыков подготовки докладов, сообщений, приобретения опыта устных публичных выступлений, ведения дискуссии, аргументации и защиты выдвигаемых положений, а также для контроля преподавателем степени подготовленности аспирантов по изучаемой дисциплине.

При подготовке к практическому занятию аспиранты имеют возможность воспользоваться консультациями преподавателя.

При подготовке к практическим занятиям аспирантам необходимо:

приносить с собой рекомендованную преподавателем литературу к конкретному занятию;

до очередного практического занятия по рекомендованным литературным источникам проработать теоретический материал, соответствующей темы занятия;

в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения;

в ходе семинара давать конкретные, четкие ответы по существу вопросов; на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов (анализов, ситуаций), в случае затруднений обращаться к преподавателю.

Аспирантам, пропустившим занятия (независимо от причин), не имеющие письменного решения задач или не подготовившиеся к данному практическому занятию, рекомендуется не позже чем в 2-недельный срок явиться на консультацию к преподавателю и отчитаться по теме, изучавшейся на занятии.



Аспиранты, не отчитавшиеся по каждой не проработанной ими на занятиях теме к началу экзаменационной сессии не допускаются к экзамену.

## **8. Ресурсное обеспечение дисциплины**

### **8.1. Основная и дополнительная учебная литература, необходимая для освоения дисциплины**

#### **а) основная литература:**

1. Суворова Г.М. Информационная безопасность. Учебное пособие для ВУЗов/ Г.М. Суворова - 2-е изд. – М.: Издательство Юрайт, 2024. – 277 с.

2. Алгоритм выявления угроз информационной безопасности в распределенных мультисервисных сетях органов государственного управления/ А.Ю. Пучков, А.М. Соколов, С.С. Широков, Н.Н. Проимнов // Прикладная информатика. – 2023. – Т.18 – С.85-102

3. Васильев В.И. Оценка актуальных угроз безопасности информации с помощью технологии трансформеров / В.И. Васильев, А.М. Вульфин, Н.В. Кучкарова // Вопросы кибербезопасности – 2022. – №2 – С.27-38.

#### **б) дополнительная литература:**

1. Остапенко Г.А. Информационные операции и атаки в социотехнических системах [Текст]. – М.: Горячая линия- Телеком, 2007. – 134 с.: ил. – (Специальность). – Библиогр.: с. 123-132.

2. Назаров А.Н. Информационная безопасность в сетях общего пользования [Электронный ресурс]: учебно-методическое пособие / А.Н. Назаров, Е.Г. Андрианова. – М.: РТУ МИРЭА, 2023. – Электрон. опт. диск (ISO).

3. Федин Ф.О. Информационная безопасность баз данных. Ч. 1 [Электронный ресурс]: учебное пособие / Ф. О. Федин, О. В. Трубиенко, С.В. Чискидов. – М.: РТУ МИРЭА, 2020. – Электрон. опт. диск (ISO).

4. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учеб. пособие для сред. проф. образования / В.Ф. Шаньгин – М.: ИД «ФОРУМ», 2008. – 415 с.: ил. – (Проф. образование). – Библиогр.: с. 401-408 (105 назв.).

5. Информационная безопасность открытых систем: Учебник для вузов / С.В. Запечников [и др.]. – М.: Горячая линия-Телеком, 2006-2008.

6. Партыка Т.Л. Информационная безопасность: Учеб. пособие для сред. проф. образования / Т.Л. Партыка, И.И. Попов. – М.: ФОРУМ, 2011. – 431 с.: ил. – (Профессиональное образование). – Библиогр.: с. 404-406 (32 назв.).

7. Филин С.А. Информационная безопасность [Текст]. – М.: Альфа-Пресс, 2006. – 411 с.: ил. – Библиогр.: с. 405-409.

8. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Текст]. – М.: ДМК Пресс, 2008. – 542 с.: ил. – Библиогр.: с. 524-529.

9. Зязин В.П. Технические средства и методы защиты информации [Электронный ресурс]: учеб. пособие / В.П. Зязин, М.Ю. Паждин, С.В. Филатов. – М.: МИРЭА, 2013. – Электрон. опт. диск (ISO).

10. Бирюков А.А. Информационная безопасность: защита и нападение [Текст] / А.А. Бирюков. – М.: ДМК Пресс, 2013. – 473 с.: ил. – Библиогр.: с. 473.
11. Грибунин В.Г. Комплексная система защиты информации на предприятии [Текст] / В.Г. Грибунин, В.В. Чудовский. – М.: Академия, 2009. – 412 с.: ил. – (Высшее профессиональное образование). – Библиогр.: с. 403-406.
12. Грушо А.А. Теоретические основы компьютерной безопасности [Текст] / А.А. Грушо, Э.А. Применко, Е.Е. Тимонина. – М.: Академия, 2009. – 268 с.: ил. – (Высшее профессиональное образование). – Библиогр.: с. 261-263.
13. Мельников В.П. Информационная безопасность и защита информации [Текст] / В.П. Мельников, С.А. Клейменов, А.М. Петраков. – М.: Академия, 2009. – 331 с.: ил. – (Высшее профессиональное образование). – Библиогр.: с. 327-328.
14. Информационная безопасность и защита информации: Метод. указ. по выполнению лаб. работ. – М.: МИРЭА, 2009. – 31 с.: ил.
15. Технические средства и методы защиты информации [Текст] / Зайцев А.П., Шелупанов А.А., ред.. – М.: Горячая линия- Телеком, 2009. – 615 с.: ил. – (Специальность). – Библиогр.: с. 608-609.
16. Романов О.А. Организационное обеспечение информационной безопасности: Учебник для вузов / О.А. Романов, С.А. Бабин, С.Г. Жданов. – М.: Академия, 2008. – 189 с.. – (Высшее профессиональное образование). – Библиогр.: с. 185.

## **8.2. Ресурсы информационно-телекоммуникационной сети Интернет, необходимые для освоения дисциплины**

1. <http://library.mirea.ru/>  
научно-техническая библиотека РТУ МИРЭА.
2. <https://e.lanbook.com/>  
электронно-библиотечная системы (ЭБС) Издательства «Лань».

## **8.3. Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем:**

- Аппаратные модули криптографической защиты информации «Diamond VPN/FW»;
- Криптошлюз АПКШ «Континент» 3.9.ЦУС.Платформа IPC500. КС;
- Astra Linux Special Edition. РУСБ. 10015-01 версии 1.6 (релиз Смоленск) (ФСТЭК);
- RedCheck Professinal;
- Клиент МК СЗ "Diamond VPN/FW";
- ПО СКЗИ "Dcrypt 1.0 v.2";
- ПО Secret Net Studio 8;
- ПО СЗИ Secret Net LSP+;
- "Acronis" Защита Данных для рабочей станций;

- ПО для ЭВМ "КриптоАРМ VipNet;
- АПКШ «Континент» версии 3.9;
- Vipnet IDS 1000.

**8.4. Материально-техническая база,** необходимая для осуществления образовательного процесса по дисциплине

- учебная аудитория;
- компьютерный класс.