



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.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
«Б1.О.04 ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ»**

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: 10 з.е.
в академических часах: 360 ак.ч.

Москва, 2024

Разработчики:

Преподаватель кафедры Информационно-измерительных систем
Рябов В. С.

Рабочая программа дисциплины (модуля) составлена 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

Содержание

1. Цель и задачи освоения дисциплины (модуля)
2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы
3. Место дисциплины в структуре ОП
4. Объем дисциплины и виды учебной работы
5. Содержание дисциплины
 - 5.1. Разделы, темы дисциплины и виды занятий
 - 5.2. Содержание разделов, тем дисциплины и формы текущего контроля
6. Оценочные материалы текущего контроля
7. Оценочные материалы промежуточной аттестации
8. Порядок проведения промежуточной аттестации
9. Материально-техническое и учебно-методическое обеспечение дисциплины
 - 9.1. Перечень основной и дополнительной учебной литературы
 - 9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся
 - 9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине
 - 9.4. Оборудование и технические средства обучения
10. Методические указания по освоению дисциплины (модуля)

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - формирование у обучающихся способности решать задачи, связанные с технологиями обеспечения информационной безопасности объектов различного применения и степени сложности.

Задачи изучения дисциплины:

- Изучение методов и средств выявления угроз и оценка уязвимости информационных систем;
- Формирование навыков разработки требований и критериев оценки информационной безопасности;
- Приобретение умений для обоснования выбора состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;
- Формирование навыков разработки систем, комплексов, средств и технологий обеспечения информационной безопасности;
- Формирование навыков разработки программ и методик испытаний средств и систем обеспечения информационной безопасности.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание

ОПК-1.1 Анализирует систему обеспечения информационной безопасности и формулирует требования по ее улучшению

Знать:

ОПК-1.1/Зн1 Содержание основных стандартов в области информационной безопасности

Уметь:

ОПК-1.1/Ум1 Организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения защиты информации в информационных системах

Владеть:

ОПК-1.1/Нв1 Анализировать сложные системы обеспечения информационной безопасности, выявляя их слабые места и области для улучшения

ОПК-1.2 Разрабатывает проект технического задания на создание системы обеспечения информационной безопасности

Знать:

ОПК-1.2/Зн1 Основные принципы классификации уязвимостей защиты по размещению данных в информационной системе

Уметь:

ОПК-1.2/Ум1 Применять современные программные инструментариумы для моделирования угроз, анализа и оценки рисков информационной безопасности, а также использовать системы поддержки принятия решений при выборе эффективных проектов защиты

ОПК-1.2/Ум2 Применять эффективные методы управления безопасностью информационных систем

Владеть:

ОПК-1.2/Нв1 Разрабатывать комплексные и структурированные технические задания на создание систем обеспечения информационной безопасности, учитывая все аспекты проекта

ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности

ОПК-2.1 Разрабатывает технический проект системы (подсистемы, компоненты системы) обеспечения информационной безопасности в соответствии с техническим заданием, нормативно-правовой, организационно-распорядительной и методической документацией

Знать:

ОПК-2.1/Зн1 Методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения защиты информации в информационных системах

Уметь:

ОПК-2.1/Ум1 Применять современные технологии моделирования и проектирования программных и программно-аппаратных систем

ОПК-2.1/Ум2 Подбирать меры и средства обеспечения информационной безопасности объекта защиты

ОПК-2.1/Ум3 Определять основные мероприятия по организации разработки системы защиты информации на объектах информатизации; разрабатывать технические проекты, документы, регламентирующие обеспечение информационной безопасности объектов информатизации (подсистемы либо компонента системы)

Владеть:

ОПК-2.1/Нв1 Разрабатывать комплексные технические проекты систем обеспечения информационной безопасности, интегрируя различные компоненты и подсистемы в единую архитектуру

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.О.04 «Защищенные информационные системы» относится к обязательной части образовательной программы и изучается в семестре(ах): 3, 4.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
3 семестр	180	5	34	34	112	Зачет
4 семестр	180	5	32	64	84	Зачет с оценкой

Всего	360	10	66	98	196	
-------	-----	----	----	----	-----	--

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Лекционные занятия	Практические занятия	Самостоятельная работа	Планируемые результаты с обучения, соотнесенные с результатами освоения программы
Раздел 1. Понятия и сущность защищённых автоматизированных систем	22	6	4	12	ОПК-1.1
Тема 1.1. Анализ и оценка информационных рисков, угроз и уязвимостей информационной системы. Аудит информационной безопасности.	22	6	4	12	
Раздел 2. Общие принципы проектирования и разработки защищённых автоматизированных систем	46	8	8	30	ОПК-1.2
Тема 2.1. Сбор исходных данных об информационной системе. Разработка технического задания на создание системы защиты информации. Проектирование, внедрение, эксплуатация защищенных информационных систем.	46	8	8	30	
Раздел 3. Основные технологии построения защищенных информационных систем	46	8	8	30	ОПК-2.1
Тема 3.1. Моделирование с помощью различных нотаций. IDEF – методологии.	46	8	8	30	
Раздел 4. Защищенные ОС как основа построения защищенных информационных систем	66	12	14	40	ОПК-1.1 ОПК-1.2

Тема 4.1. Базовые средства защиты современных ОС семейства Linux. Встроенные средства защиты информации на примере современных отечественных ОС (ОС Astra Linux).	66	12	14	40	
Раздел 5. Технологии виртуализации при построении защищенных информационных систем	58	10	24	24	ОПК-1.2 ОПК-2.1
Тема 5.1. Технологии контейнерной виртуализации. Технологии виртуализации как средство обеспечения защиты при построении информационных систем. Интеграция встроенных средств защиты информации и технологий виртуализации на примере отечественных защищенных ОС (ОС Astra Linux)	58	10	24	24	
Раздел 6. Применение криптографических методов защиты информации при построении информационных систем	54	10	24	20	ОПК-1.1
Тема 6.1. Криптографические проколы. Электронная цифровая подпись. Средства криптографической защиты информации.	54	10	24	20	
Раздел 7. Перспективные направления в области проектирования защищенных информационных систем	40	8	12	20	ОПК-1.2 ОПК-2.1
Тема 7.1. Применение облачных технологий при построении защищенных информационных систем.	40	8	12	20	
Раздел 8. Средства разработки и тестирования защищенных информационных систем	28	4	4	20	ОПК-1.2 ОПК-2.1
Тема 8.1. Верификация, статический анализ кода, динамический анализ, тестирование на проникновение.	28	4	4	20	
Итого	360	66	98	196	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Понятия и сущность защищённых автоматизированных систем

Тема 1.1. Анализ и оценка информационных рисков, угроз и уязвимостей информационной системы. Аудит информационной безопасности.

Основные понятия информационной безопасности. Защищенные информационные системы и требования к ним. Понятие, виды и структура информационных систем. Объекты защиты и угрозы безопасности в информационных системах. Комплексный подход к защите информации. Уровни формирования режима информационной безопасности: законодательный, административный, процедурный и программно-технический. Современная нормативная база в области создания защищенных информационных систем. ГОСТ Р ИСО/МЭК 27031-2012. ГОСТ Р 51583-2014. Анализ и оценка информационных рисков, угроз и уязвимостей информационной системы. Аудит информационной безопасности.

Раздел 2. Общие принципы проектирования и разработки защищённых автоматизированных систем

Тема 2.1. Сбор исходных данных об информационной системе. Разработка технического задания на создание системы защиты информации. Проектирование, внедрение, эксплуатация защищенных информационных систем.

Стадии и этапы разработки автоматизированных систем. Организация работ, функции заказчиков и разработчиков. Жизненный цикл информационной системы. Модели жизненного цикла. Сбор исходных данных об информационной системе. Требования к архитектуре информационных систем для обеспечения безопасности ее функционирования. Разработка технического задания на создание системы защиты информации. Проектирование, внедрение, эксплуатация защищенных информационных систем.

Раздел 3. Основные технологии построения защищенных информационных систем

Тема 3.1. Моделирование с помощью различных нотаций. IDEF – методологии.

Моделирование с помощью различных нотаций. Специальные методы моделирования, используемые при построении защищенных систем обработки информации. Описание модели безопасности. IDEF – методологии. Технология Data Mining, как процесс поддержки принятия решений, при построении защищенных систем обработки информации. Организационные и технические методы защиты информации. Основные подсистемы систем защиты информации, современное представление и реализация.

Раздел 4. Защищенные ОС как основа построения защищенных информационных систем

Тема 4.1. Базовые средства защиты современных ОС семейства Linux. Встроенные средства защиты информации на примере современных отечественных ОС (ОС Astra Linux).

Основные методы и средства обеспечения защиты ОС. Базовые средства защиты современных ОС семейства Linux. Технологии обеспечения безопасности других ОС (Windows, MacOS) Проектирование, внедрение и эксплуатация наложенных средств защиты информации. Встроенные средства защиты информации на примере современных отечественных ОС (ОС Astra Linux).

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 5. Технологии виртуализации при построении защищенных информационных систем

Тема 5.1. Технологии контейнерной виртуализации. Технологии виртуализации как средство обеспечения защиты при построении информационных систем. Интеграция встроенных средств защиты информации и технологий виртуализации на примере отечественных защищенных ОС (ОС Astra Linux)

Современные технологии программной и аппаратной виртуализации. Технологии контейнерной виртуализации. Технологии виртуализации как средство обеспечения защиты при построении информационных систем. Интеграция встроенных средств защиты информации и технологий виртуализации на примере отечественных защищенных ОС (ОС Astra Linux).

Раздел 6. Применение криптографических методов защиты информации при построении информационных систем

Тема 6.1. Криптографические проколы. Электронная цифровая подпись. Средства криптографической защиты информации.

Классификация криптографических алгоритмов. Основные направления и цели использования криптографических методов. Криптографические проколы. Электронная цифровая подпись. Требования к средствам криптографической защиты информации. Примеры средств криптографической защиты информации.

Раздел 7. Перспективные направления в области проектирования защищенных информационных систем

Тема 7.1. Применение облачных технологий при построении защищенных информационных систем.

Применение облачных технологий при построении защищенных информационных систем. Применение технологий искусственного интеллекта при проектировании и эксплуатации защищенных информационных систем.

Раздел 8. Средства разработки и тестирования защищенных информационных систем

Изучение государственных стандартов, содержащих требования, устанавливаемые российским законодательством к средствам разработки и тестированию программного обеспечения. Разработка безопасного программного обеспечения. Основные технологии обеспечения доверия к разрабатываемым средствам защиты информации. Верификация, статический анализ кода, динамический анализ, тестирование на проникновение.

Текущий контроль

Вид (форма) контроля
Тестирование

6. 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: Зачет, 3 семестр.

Зачет оценивается по следующей шкале:

- оценка «зачтено» 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; а также автоматически, когда обучающийся за промежуточную аттестацию имеет оценки «отлично»;
- оценка «не зачтено» выставляется обучающемуся в случае наличия грубых ошибок при изложении ответа на основные вопросы программы, свидетельствующих о неправильном понимании предмета; при решении практических задач показано незнание способов их решения, материал изложен беспорядочно и неуверенно.

Промежуточная аттестация: Зачет с оценкой, 4 семестр.

Зачет 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 наличии 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.

7. Оценочные материалы текущего контроля

Раздел 4. Защищенные ОС как основа построения защищенных информационных систем ***Контролируемые ИДК: ОПК-1.1 ОПК-1.2***

Тема 4.1. Базовые средства защиты современных ОС семейства Linux. Встроенные средства защиты информации на примере современных отечественных ОС (ОС Astra Linux).

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Эффективность защиты информации это...

1. Степень соответствия результатов защиты информации поставленной цели
2. Мера или характеристика для оценки эффективности защиты информации
3. Значения показателей эффективности защиты информации, установленные нормативными документами.

2. Показатель эффективности защиты информации –

1. Мера или характеристика для оценки эффективности защиты информации
2. Степень соответствия результатов защиты информации поставленной цели
3. Значения показателей эффективности защиты информации, установленные нормативными документами

3. Нормы эффективности защиты информации –

1. Значения показателей эффективности защиты информации, установленные нормативными документами
2. Совокупность действий по разработке и/или практическому применению методов и средств контроля эффективности защиты информации
3. Степень соответствия результатов защиты информации поставленной цели

4. Мероприятие по контролю эффективности защиты информации –

1. Совокупность действий по разработке и/или практическому применению методов и средств контроля эффективности защиты информации
2. Степень соответствия результатов защиты информации поставленной цели
3. Значения показателей эффективности защиты информации, установленные нормативными документами

5. Категорирование защищаемой информации (объекта защиты) –

1. Установление градаций важности защиты защищаемой информации (объекта защиты)
2. Степень соответствия результатов защиты информации поставленной цели
3. Значения показателей эффективности защиты информации, установленные нормативными документами

6. Контроль состояния защиты информации –

1. Проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации
2. Установление градаций важности защиты защищаемой информации (объекта защиты)
3. Проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации

7. Средство контроля эффективности защиты информации –

1. Техническое, программное средство, вещество и/или материал, предназначенные или используемые для контроля эффективности защиты информации

2. Проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации

8. Контроль организации защиты информации –

1. Проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации

2. Проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации

9. Что в сфере информационной безопасности принято считать риском?

1. Потенциальную возможность понести убытки из-за нарушения безопасности информационной системы

2. Потенциально возможное происшествие неважно, преднамеренное или нет, которое может оказать нежелательное воздействие на компьютерную систему, а также информацию, хранящуюся и обрабатывающуюся в ней

3. Характеристику, которая делает возможным возникновение угрозы

10. Что отличает риск от угрозы?

1. Объем вероятных потерь

2. Наличие количественной оценки возможных потерь и (возможно) оценки вероятности реализации угрозы

3. Угроза и риск - понятия идентичные

11. Какие из перечисленных мер защиты относятся к организационным?

1. Защита периметра сети с помощью межсетевого экрана

2. Создание службы защиты информации

3. Определение порядка доступа к защищаемым объектам

4. Использование антивирусных средств защиты

12. Для чего служит прикладное программное обеспечение?

1. Планирования и организации алгоритмов управления объектом

2. Планирования и организации вычислительного процесса в ЭВМ

3. Реализация алгоритмов управления объектом

13. Что такое этап реализации?

1. Построение выводов по данным, полученным путем имитации

2. Теоретическое применение результатов программирования

3. Практическое применение модели и результатов моделирования

14. Что осуществляется на этапе подготовки данных?

1. Описание модели на языке, приемлемом для используемой ЭВМ

2. Определение границ характеристик системы, ограничений и измерителей показателей эффективности

3. Происходит отбор данных, необходимых для построения модели, и представлении их в соответствующей форме

15. Что такое этап реализации?

1. Построение выводов по данным, полученным путем имитации

2. Теоретическое применение результатов программирования

3. Практическое применение модели и результатов моделирования

Раздел 8. Средства разработки и тестирования защищенных информационных систем

Контролируемые ИДК: ОПК-1.2 ОПК-2.1

Тема 8.1. Верификация, статический анализ кода, динамический анализ, тестирование на проникновение.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие меры безопасности можно принять для защиты личной информации на мобильном устройстве?

1. Установка брандмауэра (Firewall)
2. Шифрование данных (Encryption)
3. Автоматическая блокировка устройства через определенный промежуток времени (Auto-Lock)
4. Все вышеперечисленные меры правильные

2. Какие существуют основные уровни обеспечения защиты информации?

1. Законодательный
2. Административный
3. Программно-технический
4. Физический
5. Вероятностный
6. Процедурный
7. Распределительный

3. Что такое компьютерный вирус?

1. Разновидность программ, которые способны к размножению
2. Разновидность программ, которые самоуничтожаются
3. Разновидность программ, которые не работают
4. Разновидность программ, которые плохо работают

4. К методам защиты от НСД относятся?

1. Разделение доступа
2. Разграничение доступа
3. Увеличение доступа
4. Ограничение доступа
5. Аутентификация и идентификация

5. Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется?

1. Системой угроз
2. Системой защиты
3. Системой безопасности
4. Системой уничтожения

6. Какое управление доступом является базовым для ОС семейства Linux?

1. Дискреционное управление доступом
2. Ролевое управление доступом
3. Мандатное управление доступом

7. От какой угрозы безопасности информации защищает мандатное управление доступом?

1. Конфиденциальности
2. Целостности
3. Доступности

8. Каким видом анализа программного кода является фаззинг-тестирование?

1. Динамическим анализом
2. Статическим анализом
3. Тестированием на проникновение

9. Стандартной утилитой настройки межсетевого экрана в ОС семейства Linux является

1. Ifconfig
2. Iptables
3. Tcpdump
4. Netstat

10. Какие из перечисленных мероприятий входят в перечень необходимых для обеспечения комплексной защиты ОС семейства Linux?

1. Своевременная установка обновлений безопасности
2. Использование межсетевого экрана
3. Регулярная смена паролей и ключей аутентификации
4. Все перечисленные

11. В какой криптосистеме используется два ключа?

1. Двойного шифрования
2. С закрытым ключом
3. С открытым ключом
4. Симметричной

12. Как называется процедура предоставления пользователям ОС прав на выполнение определённых действий?

1. Авторизация
2. Аудиенция
3. Аутентификация
4. Идентификация

13. Механизм защиты от переполнения буфера называется:

1. Stack Guard
2. Stack Protection
3. Stack Force
4. Stack Value

14. Уязвимость — это:

1. Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации
2. Влияние неопределённости на цели
3. Попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к активу или его несанкционированного использования

15. Эксплоит — это:

1. Программное обеспечение или фрагмент кода, которое использует уязвимости в программном обеспечении для реализации одной или нескольких угроз безопасности
2. Программное обеспечение или фрагмент кода, которое указывает разработчику на недочёты в его программном коде
3. Инструмент для тестирования программного обеспечения
4. Программное обеспечение, которое используют администраторы для настройки сервера

16. Метод пароля и его модификация, метод вопрос-ответ, метод секретного алгоритма — это методы...

17. Техническое, криптографическое, программное и иное средство, предназначенное для защиты информации, средство, в котором оно реализовано, а также средство контроля эффективности защиты информации — все это ...

18. Для обхода защиты ASLR чаще всего используете метод

19. Атака, основной целью которой является ограничение доступности некоторого ресурса или информационной системы в целом, называется

20. Для организации аутентификации в ОС семейства Linux чаще всего применяется механизм

8. Оценочные материалы промежуточной аттестации

3 семестр, Зачет

Контролируемые ИДК: ОПК-1.1 ОПК-2.1 ОПК-1.2

Вопросы/Задания:

1. Основные понятия информационной безопасности
2. Основные положения ГОСТ Р ИСО/МЭК 27031-2012
3. Основные этапы разработки автоматизированных систем (АС)
4. Основные положения ГОСТ Р 51583-2014
5. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации
6. Основные составляющие методологии проектирования АИС
7. Основные принципы формирования требований к автоматизированной системе в защищенном исполнении
8. Методы и модели описания систем
9. Основные этапы жизненного цикла защищенных АС
10. Основные работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении

4 семестр, Зачет с оценкой

Контролируемые ИДК: ОПК-1.1 ОПК-2.1 ОПК-1.2

Вопросы/Задания:

1. Основные задачи и этапы проектирования автоматизированных систем в защищенном исполнении
2. Основные функции подсистемы защиты операционной системы
3. Основные модели разграничения доступа, реализованные в современных ОС
4. Основные отличия наложенных и встроенных средств защиты информации
5. Основные понятия информационной безопасности
6. Основные направления и цели использования криптографических методов
7. Основные этапы разработки безопасного программного обеспечения
8. Основные технологии обеспечения доверия к разрабатываемым средствам защиты информации
9. К какому методу относятся метод пароля и его модификация, метод вопрос-ответ, метод секретного алгоритма?
10. Какой метод чаще всего используется для обхода защиты ASLR?

11. Как называется атака, основной целью которой является ограничение доступности некоторого ресурса или информационной системы в целом?
12. Какой механизм применяется для организации аутентификации в ОС семейства Linux чаще всего?
13. Основные понятия информационной безопасности
14. Основные положения ГОСТ Р ИСО/МЭК 27031-2012
15. Основные положения ГОСТ Р 51583-2014
16. Основные этапы разработки автоматизированных систем (АС)
17. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации
18. Основные составляющие методологии проектирования АИС
19. Основные принципы формирования требований к автоматизированной системе в защищенном исполнении
20. Методы и модели описания систем
21. Основные этапы жизненного цикла защищенных АС
22. Основные работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. - Защита компьютерной информации. Эффективные методы и средства - Саратов: Профобразование, 2024. - 543 с. - 978-5-4488-0074-0. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/145909.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

Дополнительная литература

1. Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум: лабораторный практикум / М. А. Лапина, Д. М. Марков, Т. А. Гиш, М. В. Песков, В. В. Меденец. - Комплексное обеспечение информационной безопасности автоматизированных систем - Ставрополь: Северо-Кавказский федеральный университет, 2016. - 242 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/62945.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

Не используются.

Ресурсы «Интернет»

1. <https://www.iprbookshop.ru/> - IPR BOOKS
2. <https://rusneb.ru/> - Национальная электронная библиотека (НЭБ)
3. <https://www.elibrary.ru/> - НЭБ eLIBRARY

9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения

(обновление производится по мере появления новых версий программы)

Не используется.

Перечень информационно-справочных систем

(обновление выполняется еженедельно)

Не используется.

9.4. Оборудование и технические средства обучения

Учебная аудитория

Маркерная доска - 0 шт.

Моноблок - 64 шт.

Проектор - 4 шт.

10. Методические указания по освоению дисциплины (модуля)

С целью успешного освоения данного предмета студенту необходимо выполнять домашние работы по указанным преподавателям темам и представленным на занятиях материалам. Для более успешного выполнения работы студенту предлагается использование учебно-методических материалов, соответствующих указанной теме.

Самостоятельная работа студентов описывается и регулируется:

- Методическими рекомендациями по дисциплине;
- Методическими рекомендациями по организации самостоятельной работы студентов МИИГАиК;

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.