



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.В.02 МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ 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: 4 з.е.
в академических часах: 144 ак.ч.

Москва, 2024

Разработчики:

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

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 анализом и построением моделей безопасности компьютерных систем.

Задачи изучения дисциплины:

- Развитие у студентов соответствующих профессиональных компетенций;
- Формирование знаний математических основ моделирования политик управления доступом;
- Формирование знаний основных моделей управления доступом и информационными потоками;
- Выработка умений и практических навыков анализа и разработки формальных моделей безопасности для защищаемых компьютерных систем.

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

Компетенции, индикаторы и результаты обучения

ПК-1 Способен разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных)

ПК-1.1 Разрабатывает профили защиты компьютерных систем

Знать:

ПК-1.1/Зн1 Теоретические основы угроз безопасности информации

Уметь:

ПК-1.1/Ум1 Разрабатывать политики безопасности, основываясь на анализе потребностей организации и действующих угроз

Владеть:

ПК-1.1/Нв1 Разрабатывать комплексные профили защиты для различных типов компьютерных систем, учитывая их специфику и назначение

ПК-1.2 Формирует политики безопасности компьютерных систем и сетей

Знать:

ПК-1.2/Зн1 Особенности разработки модели безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных)

ПК-1.2/Зн2 Принципы построения модели безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных)

Уметь:

ПК-1.2/Ум1 Умеет разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных)

Владеть:

ПК-1.2/Нв1 Формировать и внедрять политики безопасности для компьютерных систем и сетей на уровне организации

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.В.02 «Модели безопасности компьютерных систем» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 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)
4 семестр	144	4	32	32	44	Экзамен (36)
Всего	144	4	32	32	44	36

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. Основные понятия и определения в области моделирования безопасности компьютерных систем	14	4	4	6	ПК-1.2
Тема 1.1. Элементы теории графов. Модель решётки.	14	4	4	6	
Раздел 2. Модели компьютерных систем с дискреционным управлением доступом	16	4	6	6	ПК-1.1
Тема 2.1. Модели ХРУ и ТМД. Классическая модель Take-Grant. Расширенная модель Take-Grant.	16	4	6	6	
Раздел 3. Модели компьютерных систем с мандатным управлением доступом	20	6	6	8	ПК-1.1

Тема 3.1. Классическая модель БеллаЛаПадулы. Модель Биба. Модель СВС.	20	6	6	8	
Раздел 4. Модели безопасности информационных потоков	14	4	4	6	ПК-1.1 ПК-1.2
Тема 4.1. Модель изолированной программной среды. Автоматная, программная и вероятностная модели безопасности информационных потоков.	14	4	4	6	
Раздел 5. Модели компьютерных систем с ролевым управлением доступом	16	6	4	6	ПК-1.1
Тема 5.1. Модели ролевого управления доступом: иерархия ролей, механизм ограничений. Модель администрирования ролевого управления доступом.	16	6	4	6	
Раздел 6. Модели безопасности управления доступом и информационными потоками (ДП-модели)	14	4	4	6	ПК-1.2
Тема 6.1. Дискреционные ДП-модели. МРОСЛ ДП-модель.	14	4	4	6	
Раздел 7. Примеры реализации и основные направления развития формальных моделей безопасности компьютерных систем	14	4	4	6	ПК-1.1 ПК-1.2
Тема 7.1. Модели управления доступом в ОС Windows. Модели управления доступом в ОС семейства Linux. Вопросы верификации формальных моделей управления доступом и корректности их реализации. Модель управления доступом в отечественной ОС Astra Linux Special Edition.	14	4	4	6	
Итого	108	32	32	44	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Основные понятия и определения в области моделирования безопасности компьютерных систем

Тема 1.1. Элементы теории графов. Модель решётки.

Понятие и классификация угроз безопасности информации. Понятие и основные виды политик безопасности управления доступом и информационными потоками. Сущность, субъект, доступ, информационный поток. Утечка права доступа и нарушение безопасности компьютерных систем. Математические основы моделей безопасности.

Раздел 2. Модели компьютерных систем с дискреционным управлением доступом

Тема 2.1. Модели ХРУ и ТМД. Классическая модель Take-Grant. Расширенная модель Take-Grant.

Модель матрицы доступов Харрисона–Руззо–Ульмана (ХРУ): описание модели, анализ безопасности. Модель типизированной матрицы доступов (ТМД). Модель распространения прав доступа Take-Grant: основные положения, классическая и расширенная модель Take-Grant. Представление систем Take-Grant системами ХРУ.

Раздел 3. Модели компьютерных систем с мандатным управлением доступом

Тема 3.1. Классическая модель Белла-ЛаПадулы. Модель Биба. Модель СВС.

Модель Белла-ЛаПадулы: классическая модель, политика low-watermark, безопасность переходов. Недостатки модели Белла-ЛаПадулы, примеры реализации запрещённых информационных потоков. Модель мандатного контроля целостности информации Биба. Модель систем военных сообщений.

Раздел 4. Модели безопасности информационных потоков

Тема 4.1. Модель изолированной программной среды. Автоматная, программная и вероятностная модели безопасности информационных потоков.

Субъектно-ориентированная модель изолированной программной среды. Автоматная модель безопасности информационных потоков. Программная модель контроля информационных потоков. Вероятностная модель безопасности информационных потоков.

Раздел 5. Модели компьютерных систем с ролевым управлением доступом

Тема 5.1. Модели ролевого управления доступом: иерархия ролей, механизм ограничений. Модель администрирования ролевого управления доступом.

Базовая модель ролевого управления доступом. Модель администрирования ролевого управления доступом. Модель мандатного ролевого управления доступом.

Раздел 6. Модели безопасности управления доступом и информационными потоками (ДП-модели)

Тема 6.1. Дискреционные ДП-модели. МРОСЛ ДП-модель.

Элементы состояния и правила преобразования состояний системы в рамках базовой ДП-модели. ДП-модели без кооперации доверенных и недоверенных субъектов. Иерархическое представление мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в операционных системах семейства Linux.

Раздел 7. Примеры реализации и основные направления развития формальных моделей безопасности компьютерных систем

Тема 7.1. Модели управления доступом в ОС Windows. Модели управления доступом в ОС семейства Linux. Вопросы верификации формальных моделей управления доступом и корректности их реализации. Модель управления доступом в отечественной ОС Astra Linux Special Edition.

Модели управления доступом, реализованные в современных ОС, СУБД и других компьютерных системах. Проблемы адекватности формальных моделей управления доступом условиям функционирования реальных компьютерных систем. Вопросы верификации корректности реализации формальных моделей управления. Примеры и особенности реализации моделей управления доступом и информационными потоками в отечественных защищенных ОС.

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: 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 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 – 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 7. Примеры реализации и основные направления развития формальных моделей безопасности компьютерных систем

Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 7.1. Модели управления доступом в ОС Windows. Модели управления доступом в ОС семейства Linux. Вопросы верификации формальных моделей управления доступом и корректности их реализации. Модель управления доступом в отечественной ОС Astra Linux Special Edition.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие виды политик информационной безопасности рассматриваются в теории компьютерной безопасности (отметьте один или несколько ответов).

1. Мандатная
2. Древовидная
3. Многоуровневая
4. Ролевая
5. Дискреционная
6. Дискретизированная
7. Ничего из перечисленного

2. Угроза конфиденциальности информации состоит в:

1. Нарушении установленных ограничений на доступ к информации
2. Несанкционированном (случайном или преднамеренном) изменении информации
3. Несанкционированном блокировании доступа к информации
4. Реализации всех вышеперечисленных нарушений

3. Угроза целостности информации состоит в:

1. Нарушении установленных ограничений на доступ к информации
2. Несанкционированном (случайном или преднамеренном) изменении информации
3. Несанкционированном блокировании доступа к информации
4. Реализации всех вышеперечисленных нарушений

4. Угроза доступности информации состоит в:

1. Нарушении установленных ограничений на доступ к информации
2. Несанкционированном (случайном или преднамеренном) изменении информации
3. Несанкционированном блокировании доступа к информации
4. Реализации всех вышеперечисленных нарушений

5. Как формулируется основная аксиома теории компьютерной безопасности?

1. Все вопросы безопасности информации в КС описываются перечнем субъектов и объектов
2. Все вопросы безопасности информации в КС описываются уровнями субъектов и объектов
3. Все вопросы безопасности информации в КС описываются доступами субъектов к объектам
4. Все вопросы безопасности информации в КС описываются уровнями доступа субъектов и уровнями безопасности объектов
5. Ничего из перечисленного

6. Какие из перечисленных моделей являются дискреционными?

1. Модель Биба
2. Модель Харрисона-Руззо-Ульмана

3. Модель Белла-лападулы
4. Модель take-grant
5. Модель систем военных сообщений
6. Модель изолированной программной среды

7. Какие из перечисленных моделей являются моделями мандатного управления доступом?

1. Модель ТМД
2. Модель Харрисона-Руззо-Ульмана
3. Модель Белла-ЛаПадулы
4. Модель RBAC
5. Все вышеперечисленные

8. В классической модели Белла-ЛаПадулы через S обозначается:

1. Множество субъектов
2. Множество объектов
3. Множество прав доступа
4. Множество информационных потоков

9. Существует ли алгоритм проверки безопасности систем ХРУ?

1. Да, существует для общего случая
2. Нет, не существует ни для каких ХРУ
3. Существует только для монооперационных ХРУ
4. Существует для некоторых разновидностей ХРУ, а в общем случае – возможно существует, но не найден
5. Существует для некоторых разновидностей ХРУ, а в общем случае доказано, что не существует
6. Вопрос о существовании или не существовании такого алгоритма не решен ни для каких ХРУ

10. Какие из перечисленных правил являются де-факто правилами расширенной модели Take-Grant?

1. Take
2. Grant
3. Write
4. Read
5. Spy
6. Find
7. Post
8. Pass
9. Invoke
10. Observe

11. Какие из перечисленных правил являются де-юре правилами расширенной модели Take-Grant?

1. Take
2. Grant
3. Create
4. Append
5. Pass
6. Remove

12. Утечка информации – это:

1. Несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу
2. Ознакомление постороннего лица с содержанием секретной информации
3. Потеря, хищение, разрушение или неполучение переданных данных

13. Что такое аутентификация?

1. Проверка количества переданной и принятой информации

2. Нахождение файлов, которые изменены в информационной системе не-санкционированно
3. Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).
4. Определение файлов, из которых удалена служебная информация
5. Определение файлов, из которых удалена служебная информация

14. Достоинством дискретных моделей политики безопасности является:

15. Основной проблемой при реализации мандатной политики безопасности является:

1. Обеспечение безопасности информационных потоков
2. Невозможность однозначного задания правил управления доступом
3. Малое количество допустимых уровней конфиденциальности
4. Сложность модели

16. Классическая модель Белла-ЛаПадулы в первую очередь ориентирована на обеспечение защиты от угрозы:

1. Конфиденциальности информации
2. Целостности информации
3. Доступности информации
4. Отсутствия информации

17. Классическая модель Биба в первую очередь ориентирована на обеспечение защиты от угрозы:

1. Конфиденциальности информации
2. Целостности информации
3. Доступности информации
4. Незнания информации

18. Модель системы военных сообщений основана на модели:

1. Take-Grant
2. Белла-ЛаПадулы
3. ТМД
4. RBAC

19. В модели СВС роль пользователя - это:

1. Совокупность прав пользователя, определяемая характером выполняемых им действий в системе
2. Набор однотипных сущностей
3. Совокупность имен учетных записей пользователя
4. Совокупность объектов доступа, сопоставленных с пользователем

20. В рамках формального описания модель СВС представляется:

1. Конечным автоматом
2. Графом доступов
3. Множеством ссылок
4. Иерархической структурой

21. Ролевое управление доступом представляет собой развитие:

1. Политики дискреционного управления доступом
2. Политики мандатного управления доступом
3. Политики информационного невливания
4. Модели СВС

22. Модель управления доступом RBAC расшифровывается как:

1. Role Based Access Control
2. Root Based Access Control
3. RollBack Access Control
4. RollBack Alter Commit

23. В базовой модели ролевого управления доступом сессия пользователя в общем случае может обладать:

1. Несколькими ролями одновременно

2. Одной произвольной ролью
3. Одной конкретной ролью
4. Только всеми ролями одновременно

24. Базовые механизмы управления доступом ОС семейства Linux реализуют политику:

1. Мандатного управления доступом
2. Дискреционного управления доступом
3. Ролевого управления доступом
4. Типизированного управления доступом

25. Произвольную систему ТМД можно представить:

1. Системой ХРУ
2. Системой RBAC
3. Системой SVC
4. Любой из перечисленных систем

26. Начиная с Windows Vista в семействе данных ОС наравне с дискреционной политикой управления доступом реализуется:

1. Политики мандатного управления доступом
2. Политика мандатного контроля целостности
3. Политика типизированного управления доступом
4. Все перечисленные политики

27. В базовой модели ролевого управления доступом права доступа к объектам задаются через:

1. Роли
2. Другие объекты
3. Права доступа к объектам не предусмотрены
4. Учетные записи пользователей

28. В теории моделирования управления доступом под субъектом доступа чаще всего понимается:

1. Активная сущность КС, которая может изменять состояние системы через порождение процессов над объектами, в том числе, порождать новые объекты и инициализировать порождение новых субъектов
2. Пассивная сущность КС, процессы над которой могут в определенных случаях быть источником порождения новых субъектов
3. Пользователь КС
4. Ничего из перечисленного

29. В теории моделирования управления доступом под объектом доступа чаще всего понимается:

1. Активная сущность КС, которая может изменять состояние системы через порождение процессов над объектами, в том числе, порождать новые объекты и инициализировать порождение новых субъектов
2. Пассивная сущность КС, процессы над которой могут в определенных случаях быть источником порождения новых субъектов
3. Пользователь КС
4. Ничего из перечисленного

30. Верификация формальной модели – это:

1. Подтверждение посредством представления объективных свидетельств непротиворечивости формальной модели управления доступом и выполнения заданных в ее рамках условий безопасности
2. Сопоставление элементов формальной модели с объектами предметной области
3. Доказательство важности модели
4. Доказательство корректности реализации формальной модели

31. Формализованное описание формальной модели:

1. Описание формальной модели на формальном языке со строгой и одно-значно определенной семантикой, позволяющее использовать инструментальные средства

верификации

2. Описание формальной модели на математическом языке

3. Описание формальной модели с использованием основных элементов теории моделирования управления доступом

4. Комбинация всевозможных видов представления формальных моделей

32. Домены безопасности согласно "Оранжевой книге" используются в системах класса

33. Возможность получения необходимых пользователю данных или сервисов за разумное время характеризует свойство

34. В многоуровневой модели, если субъект доступа формирует запрос на чтение-запись, то уровень безопасности субъекта относительно уровня безопасности объекта должен:

35. ACL-список ассоциируется с каждым

36. Выделения пользователем и администраторам только тех прав доступа, которые им необходимы это:

37. Главным параметром криптосистемы является показатель

38. Готовность устройства к использованию всякий раз, когда в этом возникает необходимость, характеризует свойство ...

39. Модель матрицы доступов Харрисона-Руззо-Ульмана является моделью ...

40. Все процессы безопасности в КС описываются доступами субъектов к ...

41. Компьютерная система безопасна тогда и только тогда, когда субъекты не имеют никаких возможностей нарушать установленную в системе ...

42. Информационный поток, который может быть применен для нарушения политик управления доступом, называется ...

43. Можно ли политику дискреционного управления доступом выразить через ролевое управление доступом?

44. Могут ли в системе быть одновременно реализованы несколько видов политик управления доступом?

45. В модели Белла-ЛаПадулы для каждого объекта задается его ...

46. В модели Белла-ЛаПадулы для каждого субъекта задается его ..

47. В модели Биба для каждого объекта задается его ...

48. Модель Типизированной Матрицы Доступов является моделью ...

49. Модель Take-Grant является моделью

50. Существует ли алгоритм проверки возможности утечки права доступа read для заданной пары субъект-объект произвольной системы ХРУ?

51. Является ли решеткой произвольный граф?

52. Является ли обязательным требование «все сущности должны быть идентифицированы» для политики ролевого управления доступом?

53. Цель реализации политики безопасности информационных потоков состоит в том, чтобы обеспечить невозможность возникновения в КС ...

54. Цель реализации политики безопасности информационных потоков состоит в том, чтобы обеспечить невозможность возникновения в КС ...

55. Рассматриваются ли в модели ХРУ сущности-контейнеры?

56. Система ХРУ, в которой каждая команда системы содержит один примитивный оператор, называется

57. Задача проверки разрешимости произвольных систем ХРУ алгоритмически ...

58. Существует ли алгоритм проверки безопасности систем АМТМД?

59. Состояние системы в модели Take-Grant описывается соответствующим ему ...

60. Элементом какой политики управления доступом является стандартный вектор прав доступа ОС семейства Linux?

61. Активно действующая в КС абстрактная сущность, обладающая логически взаимосвязан-ным набором полномочий, необходимых для выполнения определенных функциональных обязанностей пользователями системы называется ...

62. Среди политик управления доступом в СУБД наибольшее распространения получила политика...

63. Может ли быть задана иерархия на множестве ролей в моделях ролевого управления доступом?

64. Разрешено ли чтение субъектом с большим уровнем конфиденциальности объекта с меньшим уровнем конфиденциальности в модели Белла-ЛаПадулы?

8. Оценочные материалы промежуточной аттестации

4 семестр, Экзамен

Контролируемые ИДК: ПК-1.1 ПК-1.2

Вопросы/Задания:

1. Основные элементы теории компьютерной безопасности (сущность, субъект, доступ, право доступа, информационные потоки по памяти или по времени).

2. Основная аксиома компьютерной безопасности. Проблема построения защищенной КС.

3. Основные виды политик управления доступом и информационными потоками.

4. Методы и формы представления политик безопасности.

5. Классические стандарты информационной безопасности.

6. Модель Белла-ЛаПадулы: безопасность переходов.

7. Модель мандатной политики целостности информации Биба.

8. Модель систем военных сообщений.

9. Модель безопасности информационных потоков.

10. Модель изолированной программной среды.

11. Автоматная модель безопасности информационных потоков.

12. Программная модель безопасности информационных потоков.

13. Вероятностная модель безопасности информационных потоков.

14. Базовая модель ролевого управления доступом.

15. Модель администрирования ролевого управления доступом.

16. Администрирование множеств авторизованных ролей пользователей.

17. Модель мандатного ролевого управления доступом.
18. Безопасность информационных потоков: защита от угроз конфиденциальности и целостности информации.
19. Понятие и общая характеристика скрытых каналов утечки информации.
20. Основные направления развития формальных моделей безопасности компьютерных систем.
21. Проблема адекватности реализации модели безопасности в реальной КС.
22. Основные элементы формальных моделей управления доступом и информационными потоками (ДП-моделей).
23. Правила преобразования состояний системы в рамках базовой ДП-модели.
24. ДП-модели без кооперации доверенных и недоверенных субъектов.
25. Иерархическое представление мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в операционных системах семейства Linux.
26. Примеры реализации моделей управления доступом в ОС Windows.
27. Примеры реализации моделей управления доступом в ОС семейства Linux.
28. Основные методы верификации формальных моделей управления доступом.
29. Задача проверки корректности реализации формальных моделей управления доступом.
30. Особенности модели управления доступом в отечественной ОС Astra Linux Special Edition.
31. Субъект, объект системы.
32. Право доступа.
33. Важность основной аксиомы теории компьютерной безопасности.
34. Основные угрозы безопасности информации рассматриваются в теории компьютер-ной безопасности.
35. Основные отличия между запрещенными информационными каналами по памяти и по времени.
36. Основные недостатки классической модели Белла-ЛаПадулы.

37. Схожесть подходов к определению информационного потока в расширенной модели Take-Grant и модели Белла-ЛаПадулы.

38. Отличие определений свойств безопасности классической модели Белла-ЛаПадулы и модели Биба.

39. Десять неформальных свойств модели СВС.

40. Политика управления доступом.

41. Отличие информационной не выводимости от информационного не влияния.

42. Иерархия ролей в базовой модели ролевого управления доступом.

43. Основные элементы модели RBAC.

44. Замкнутая и изолированная программные среды.

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Богульская Н. А. Модели безопасности компьютерных систем: учебное пособие: учебное пособие / Н. А. Богульская, М. М. Кучеров. - Модели безопасности компьютерных систем - Красноярск: Сибирский федеральный университет, 2019. - 206 с. - 978-5-7638-4008-7. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/100055.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

Дополнительная литература

1. Тарков М. С. Нейрокомпьютерные системы: учебное пособие: учебное пособие / М. С. Тарков. - Нейрокомпьютерные системы - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. - 170 с. - 978-5-4497-3308-5. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/142276.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://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

Смешанный тип

Автоматизированное рабочее место (АРМ) - 16 шт.

Доска настенная одноэлементная - 4 шт.

Проектор - 2 шт.

Интерактивная панель - 1 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.