УТВЕРЖДЕНО
решением Ученого совета факультета математики, информационных и авиационных технологий
от « 16 » ____мая_____ 20_23 _ г., протокол №_4/23____
Председатель_____ Волков М.А.
(подпись, расшифровка подписи)
«__16__» _____мая_____2023____г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	**Модели безопасности компьютерных систем**
Факультет	**Факультет математики, информационных и авиационных технологий (ФМИАТ)**
Кафедра	**Информационной безопасности и теории управления (ИБТУ)**
Курс	**4-5**

Специальность:10.05.01 "**Компьютерная безопасность**"
Направленность (профиль/специализация): "**Математические методы защиты информации**"
Форма обучения: **очная**

Дата введения в учебный процесс УлГУ: «1» сентября 2023г.

Программа актуализированана заседании кафедры: протокол №_____ от _____ 20_____г.
Программа актуализированана заседании кафедры: протокол №_____ от _____ 20_____г.
Программа актуализированана заседании кафедры: протокол №_____ от _____ 20_____г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Перцева Ирина Анатольевна	ИБиТУ	доцент

СОГЛАСОВАНО
Заведующий кафедрой «Информационная безопасность и теория управления», реализующей дисциплину
(подпись) Андреев А.С. / *(Ф.И.О.)*
«11_»__мая____2023 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ:

Цели освоения дисциплины:

Целью дисциплины «Модели безопасности компьютерных систем» является обучение студентов принципам формального моделирования и анализа безопасности компьютерных систем, реализующих управление доступом и информационными потоками.

Задачи освоения дисциплины:

Задачами дисциплины являются:

– развитие у студентов соответствующих общекультурных, профессиональных и профессионально-специализированных компетенций;

– изучение основных формальных моделей политик безопасности, моделей дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков;

– приобретение практических навыков разработки математических моделей безопасности для защищаемых компьютерных систем;

– формирование у будущего специалиста в области компьютерной безопасности таких качеств, как строгость в суждениях, творческое мышление, организованность и работоспособность, дисциплинированность, самостоятельность и ответственность.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП:

Дисциплина «Модели безопасности компьютерных систем» Б1.О.1.1.38 относится к числу базовых дисциплин программы подготовки специалистов по направлению 10.05.01 – «Компьютерная безопасность».

Дисциплина читается в 8-ом и 9-ом семестрах 4-ого и 5-ого курсов соответственно студентам очной формы обучения.

Для ее успешного изучения необходимы знания и умения, приобретенные в следующих предшествующих учебных дисциплинах: Организационное и правовое обеспечение информационной безопасности Теоретико-числовые методы в криптографии.

Результаты освоения дисциплины «Модели безопасности компьютерных систем» будут необходимы для дальнейшего процесса обучения в рамках поэтапного формирования компетенций при изучении следующих дисциплин: Криптографические протоколы, Научно-исследовательская работа, при подготовке к сдаче государственного экзамена.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Перечень формируемых компетенций в процессе освоения материала по дисциплине (модулю) с указанием кода и наименования компетенций, соотнесенных с установленными разработчиком РПД индикаторами достижения каждой компетенции отдельно в соответствии с ФГОС ВПО, ФГОС ВО.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

ОПК – 8 Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	**Знать:** методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей **Уметь:** применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей **Владеть:** Способами применения методов научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей
ОПК - 11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	**Знать:** политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации **Уметь:** разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации **Владеть:** способностью разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) - 5

4.2. Объем дисциплины по видам учебной работы (в часах)

Вид учебной работы	Количество часов (форма обучения: очная)		
	Всего по плану	В т.ч. по семестрам	
		8	9
1	2	3	4
Контактная работа обучающихся с преподавателем в соответствии с УП	**90/90**	**54/54**	**36/36**
Аудиторные занятия:	90/90	54/54	36/36
лекции	54/54	36/36	18/18
семинары и практические занятия	0	0	0
лабораторные работы, практикумы	36	18/18	18/18
Самостоятельная работа	**54**	**18**	**36**
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр.работа, коллоквиум,	Лабораторные работы – 10	Лабораторные работы – 5	Лабораторные работы – 5

реферат и др.(не менее 2 видов)			
Курсовая работа	0	0	0
Виды промежуточной аттестации (экзамен, зачет)	–	Зачет	Экзамен
Всего часов по дисциплине	**144**	**72**	**72**

*****_*В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения*_

4.3. Содержание дисциплины (модуля.) Распределение часов по темам и видам учебной работы:

По каждой форме обучения: очная/заочная/очно-заочная заполняется отдельная таблица.

Форма обучения : очная

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	**2**	**3**	**4**	**5**	**6**	**7**	
Раздел 1. Основы формальной теории защиты информации.							
1. Основы формальной теории защиты информации.	5	3	-	-		2	Вопросы 1-5
Раздел 2. Модели систем с дискреционным разграничением доступа.							
2. Модель матрицы доступов Харрисона – Руззо – Ульмана.	7	3	-	2	1	2	Вопросы 6-7 Лабораторная работа
3. Развитие модели матрицы доступов Харрисона – Руззо – Ульмана.	7	3	-	2	1	2	Вопросы 8-11 Лабораторная работа
4. Классическая модель распространения прав доступа Take – Grant.	7	3	-	2	2	2	Вопросы 12-14 Лабораторная работа
5. Расширенная модель распространения	9	3	-	2	1	4	Вопросы 15-17 Лаборато

прав доступа Take – Grant.							рная работа
Раздел 3. ***Модели систем с мандатным разграничением доступа.***							
6. Классическая модель Белла – ЛаПадула.	9	3	-	2	1	4	Вопросы 18-20 Лабораторная работа
7. Интерпретации классической модели Белла – ЛаПадула.	10	4	-	2	2	4	Вопросы 21-23 Лабораторная работа
8. Модель систем военных сообщений.	9	3	-	2	2	4	Вопросы 24-27 Лабораторная работа
Раздел 4. ***Модели безопасности информационных потоков и изолированной программной среды.***							
9. Автоматная модель безопасности информационных потоков.	12	4	-	4	2	4	Вопросы 28-30 Лабораторная работа
10. Субъектно-ориентированная модель изолированной программной среды.	12	4	-	4	2	4	Вопросы 31-34 Лабораторная работа
Раздел 5. ***Модели систем с ролевым разграничением доступа.***							
11. Базовая модель ролевого разграничения доступа.	9	3	-	2	2	4	Вопросы 35-36 Лабораторная работа
12. Модель администрирования ролевого разграничения	10	4	-	2	2	4	Вопросы 37 Лабораторная

доступа.							работа
13. Модель мандатного ролевого разграничения доступа.	10	4	-	2	2	4	Вопросы 38-40 Лабораторная работа
Раздел 6. Применение и дальнейшее развитие моделей безопасности компьютерных систем.							
14. Проблема адекватности реализации модели безопасности в реальной компьютерной системе.	6	4	-		2	2	Вопросы 41-42
15. Базовое администрирование на примере администрирования ОС семейства Astra Linux.	16	4	-	8	2	4	Вопросы 43-44 Лабораторная работа
16. Развитие формальных моделей безопасности компьютерных систем.	6	2	-			4	Вопросы 41-44
Итого:	**144**	**54**	**-**	**36**	**24**	**54**	

5. СОДЕРЖАНИЕ ДИСЦИЛИНЫ (МОДУЛЯ)

Раздел 1.Основы формальной теории защиты информации.

Тема 1.Основы формальной теории защиты информации.

Основные понятия и определения. Аксиома представления информации в компьютерной системе. Объект. Преобразование информации. Субъект. Информационный поток. Доступ. Право доступа. Отношение активизации. Граф активизации. Пользователи. Основная аксиома теории защиты информации. Угроза безопасности информации. Угроза конфиденциальности информации. Угроза целостности информации. Угроза доступности информации. Угроза раскрытия параметров компьютерной системы. Неблагоприятные информационные потоки. Политика безопасности. Основные виды политик безопасности. Дискреционная политика безопасности. Матрица доступов.

Достоинства и недостатки дискреционной политики безопасности. Мандатная политика безопасности. Основная цель мандатной политики безопасности. Достоинства и недостатки мандатной политики безопасности. Политика безопасности информационных потоков. Цель реализации политики безопасности информационных потоков. Достоинства и недостатки политики безопасности информационных потоков. Политика ролевого разграничения доступа. Достоинства и недостатки политики ролевого разграничения доступа. Политика изолированной программной среды. Достоинства и недостатки политики изолированной программной среды. Основные виды моделей безопасности. Модели оценки ценности информации.

Раздел 2. Модели систем с дискреционным разграничением доступа.

Тема 2. Модель матрицы доступов Харрисона – Руззо – Ульмана.

Формальное описание модели Харрисона – Руззо – Ульмана (ХРУ). Примитивные операторы модели ХРУ. Команды модели ХРУ. Анализ безопасности систем ХРУ. Утечка права. Безопасное начальное состояние по отношению к праву. Монооперационные системы ХРУ. Теорема о разрешимости задачи проверки безопасности монооперационных систем ХРУ. Экспоненциальная сложность алгоритма проверки безопасности для монооперационных систем ХРУ. Теорема о неразрешимости задачи проверки безопасности произвольной системы ХРУ.

Тема 3. Развитие модели матрицы доступов Харрисона – Руззо – Ульмана.

Формальное описание модели типизированной матрицы доступа (ТМД). Примитивные операторы модели ТМД. Модель монотонной ТМД (МТМД). Каноническая форма модели МТМД (КФМТМД). Теорема о сводимости любой модели МТМД к КФМТМД. Родительские и дочерние типы. Граф создания. Модель ациклической монотонной ТМД (АМТМД). Сведение задачи проверки безопасности системы АМТМД к задаче проверки безопасности канонической формы системы АМТМД (АКФМТМД). Алгоритм построения развернутого состояния для системы АКФМТМД. Функция порождения объектов. Лемма о функции порождения объектов для развернутого состояния АМТМД. Теорема о разрешимости задачи проверки безопасности АМТМД. Экспоненциальная сложность алгоритма проверки безопасности систем АМТМД. Полиномиальная сложность алгоритма проверки безопасности систем тернарных АМТМД.

Тема 4. Классическая модель распространения прав доступа Take – Grant.

Формальное описание классической модели Take – Grant. Основная цель модели Take – Grant. Граф доступов. Де-юре правила преобразования графов доступов для классической модели Take – Grant. Санкционированное и несанкционированное получение прав доступа. Предикаты “возможен доступ” и “возможно похищение”. tg-связность вершин в графе доступа. Теорема о распространении прав доступа в субъектных системах Take – Grant. Понятия острова, моста и его начального и конечного пролетов в произвольном графе доступов. Теорема о распространении прав доступа в классической системе Take – Grant общего вида. Теорема о похищении прав доступа в классической

системе Take – Grant общего вида. Построение гомоморфизма системы Take – Grant и системы ХРУ.

Тема 5. Расширенная модель распространения прав доступа Take – Grant.

Направления развития модели Take – Grant. Формальное описание расширенной модели Take – Grant. Де-факто правила преобразования графов доступов и информационных потоков для расширенной модели Take – Grant. Предикат “возможна запись”. Теорема о разрешении на запись для расширенной модели Take – Grant. Понятие замыкания графа доступов и информационных потоков расширенной модели Take – Grant и его разновидности. Построение замыкания графа доступов и информационных потоков. Алгоритмы построения tg-замыкания, де-юре-замыкания, де-факто-замыкания. Теоремы о корректности алгоритмов построения tg-замыкания, де-юре-замыкания, де-факто-замыкания. Анализ путей распространения прав доступа и информационных потоков. Подходы к определению стоимости пути в графе доступов и информационных потоков.

Раздел 3. Модели систем с мандатным разграничением доступа.

Тема 6. Классическая модель Белла – ЛаПадула.

Формальное описание классической модели Белла – ЛаПадула. Система. Основные запросы в классической модели Белла – ЛаПадула. Состояние элемента системы и его возможные изменения. Безопасный доступ. Свойства системы, определяющие ее безопасность. Теоремы об обладании системой *-свойством, ss-свойством и ds-свойством. Базовая теорема безопасности. Основные проблемы, возникающие в классической модели Белла – ЛаПадула. Пример некорректного определения свойств безопасности. Недостатки модели Белла – ЛаПадула.

Тема 7. Интерпретации классической модели Белла – ЛаПадула.

Политика low-watermark для модели Белла – ЛаПадула. Формальное описание модели Белла – ЛаПадула при реализации политики low-watermark. Переопределение ss-свойства и *-свойства при реализации политики low-watermark. Лемма о безопасных состояниях системы при реализации политики low-watermark. Реализация неблагоприятного информационного потока в рамках политики low-watermark. Функции переходов и их использование в модели Белла – ЛаПадула. Безопасность переходов. Переопределение ss-свойства и *-свойства. Теоремы об обладании системой *-свойством и ss-свойством. Базовая теорема безопасности. Формальное описание модели мандатной политики целостности информации Биба. Отличие модели мандатной политики целостности информации Биба от классической модели Белла – ЛаПадула. Соответствие доступа требованиям политики low-watermark. Аналоги теорем безопасности классической модели Белла – ЛаПадула для требований политики low-watermark.

Тема 8. Модель систем военных сообщений.

Основные определения, связанные с системой военных сообщений (СВС). Роль пользователя. Объект. Контейнер. Сущность. Способ доступа к содержимому контейнера. Идентификатор сущности. Непосредственная ссылка. Косвенная ссылка. Операция. Сообщение. Неформальное описание модели СВС. Основные неформальные свойства модели СВС. Формальное описание модели СВС. Состояние системы. Безопасное состояние системы. История системы. Эквивалентность безопасных состояний системы. Потенциальная модификация сущности по ссылке с источником. Безопасная функция переходов. Смыслы безопасности функции переходов. Теоремы о безопасности для СВС. Базовая теорема безопасности для модели СВС.

Раздел 4. Модели безопасности информационных потоков и изолированной программной среды.

Тема 9. Автоматная модель безопасности информационных потоков.

Формальное описание автоматной модели безопасности информационных потоков. Информационное невлияние. Политика безопасности автоматной модели безопасности информационных потоков. Пример мандатной политики безопасности в автоматной модели безопасности информационных потоков. Невидимость и изолированность пользователя. Формальное описание программной модели контроля информационных потоков. Политика безопасности “допустить”. Эффективность механизма защиты. Соотношения между эффективными механизмами защиты. Контролируемый механизм защиты. Теорема об эффективности контролируемого механизма защиты. Вероятностная модель безопасности информационных потоков. Схема компьютерной системы. Информационная невыводимость. Информационное невлияние. Соответствие требованиям информационного невлияния. Пример системы автоматной модели, соответствующей требованиям информационного невлияния.

Тема 10. Субъектно-ориентированная модель изолированной программной среды.

Основные определения. Аксиома порождения компьютерных субъектов. Источник для субъекта. Объекты, функционально ассоциированные с субъектами. Потоки информации от объекта к объекту. Доступ субъекта к объекту. Правила разграничения доступа субъектов к объектам. Тождественность субъектов. Монитор обращений (МО). Виды МО. Монитор безопасности объектов (МБО). Корректность субъектов друг относительно друга. Абсолютная корректность субъектов друг относительно друга. Достаточное условие гарантированного выполнения политики безопасности в компьютерной системе. Монитор порождения субъектов (МПС). Монитор безопасности субъектов (МБС). Замкнутость компьютерной системы по порождению субъектов. Изолированное множество субъектов программной среды. Второе достаточное условие гарантированного выполнения политики безопасности в компьютерной системе. Изолированная программная среда (ИПС). Порождение с контролем неизменности объекта-источника. Базовая теорема ИПС. Метод субъектно-объектного взаимодействия в рамках ИПС. Практическая реализация ИПС для

современной компьютерной системы. Состояние компьютерной системы. Условие одинакового состояния. Достаточное условие ИПС при ступенчатой загрузке.

Раздел 5. Модели систем с ролевым разграничением доступа.

Тема 11. Базовая модель ролевого разграничения доступа.

Понятие ролевого разграничения доступа (РРД). Понятие роли. Формальное описание базовой модели РРД. Общая структура элементов базовой модели РРД. Иерархия ролей. Механизм ограничений в базовой модели РРД.

Тема 12. Модель администрирования ролевого разграничения доступа.

Формальное описание модели администрирования РРД. Иерархия ролей. Группы административных ролей. Администрирование множеств авторизованных ролей пользователей. Пример иерархии ролей и иерархии администрирования ролей. Предварительные условия для роли. Функции администрирования множеств авторизованных ролей пользователей на множестве административных ролей. Администрирован1.ие множеств прав доступа, которыми обладают роли. Функции для администрирования множеств прав доступа на множестве административных ролей. Пример определения функций для администрирования множеств прав доступа на множестве административных ролей. Администрирование иерархии ролей. Роли-возможности. Роли-группы. Роли-объединения. Отношение превосходства для роли-объединения. Функции для администрирования возможностей и групп пользователей на множестве административных ролей. Функции для администрирования иерархии ролей на множестве административных ролей. Примеры определения функций для администрирования иерархии ролей на множестве административных ролей.

Тема 13. Модель мандатного ролевого разграничения доступа.

Защита от угрозы конфиденциальности информации. Формальное описание модели мандатного РРД. Виды мандатного разграничения доступа. Безопасный доступ. Иерархии на множестве ролей. Соответствие модели РРД требованиям либерального мандатного разграничения доступа. Соответствие модели РРД требованиям строгого мандатного разграничения доступа. Задание иерархии ролей и ограничений в соответствии с требованиями либерального или строгого мандатного управления доступом. Теорема о безопасности информационных потоков. Защита от угроз конфиденциальности и целостности информации. Безопасный доступ. Иерархии на множестве ролей. Соответствие модели РРД требованиям либерального мандатного контроля целостности. Соответствие модели РРД требованиям строгого мандатного контроля целостности. Соответствие модели РРД требованиям либерального мандатного разграничения доступа и контроля целостности.

Раздел 6. Применение и дальнейшее развитие моделей безопасности компьютерных систем.

Тема 14. Проблема адекватности реализации модели безопасности в реальной компьютерной системе.

Общая постановка задачи построения защиты системы. Гомоморфизм компьютерной системы и ее математической модели безопасности. Проблема адекватности реализации модели безопасности в реальной компьютерной системе. Критический анализ классических моделей безопасности. Проблемы реализации дискреционной политики безопасности. Реализация атаки с использованием программных закладок вида “троянский конь”. Проблемы реализации мандатной политики безопасности. Примеры реализации неблагоприятных информационных потоков по памяти и по времени и способы противодействия их появлению.

Тема 15. Базовое администрирование на примере администрирования ОС семейства Astra Linux.

Угрозы безопасности компьютерной системы. Уровни возможностей нарушителя. Требования безопасности. Цель политики безопасности администрирования. Математическая модель политики безопасного администрирования. Доверенные и недоверенные субъекты. Подсистемы комплексной системы защиты. Функции ОС по защите информации от НСД. Требования к настройке, конфигурированию и администрированию ОС и их обоснование.

Тема 16. Развитие формальных моделей безопасности компьютерных систем.

Взаимосвязь положений классических формальных моделей безопасности компьютерных систем. Развитие формальных моделей безопасности компьютерных систем. Обзор семейства формальных моделей управления доступом и информационными потоками (ДП-моделей) компьютерных систем с дискреционным, мандатным или ролевым управлением доступом.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Данный вид работы не предусмотрен УП.

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

Цикл лабораторных работ включает в себя 10 объемных лабораторных работ. Задачами цикла являются:

– Изучение и анализ основных формальных моделей безопасности компьютерных систем;

– Приобретение практических навыков базового администрирования встроенных СЗИ ОС;

– Исследование возможностей построения политик безопасного администрирования для современных ОС.

Тема 1. Модель Харрисона – Руззо – Ульмана.

Цель работы: анализ и реализация на практике модели ХРУ и ее вариаций.

Содержание работы: модель ХРУ, модель монооперационной ХРУ, алгоритмы проверки безопасности системы ХРУ и ее вариаций.

Результат: отчет о проделанной работе.

Методические указания: выполнение задания должно вестись с использованием программных продуктов, перечисленных в списке п.10 в), отчет должен содержать подробный анализ модели и проделанной работы.

Тема 2. Модель типизированной матрицы доступа.

Цель работы: анализ и реализация на практике модели ТМД и ее вариаций.

Содержание работы: модель ТМД, модель МТМД, модель АМТМД, алгоритм построения развернутого состояния для системы АКФМТМД, алгоритмы проверки безопасности системы ТМД и ее вариаций.

Результат: отчет о проделанной работе.

Методические указания: выполнение задания должно вестись с использованием программных продуктов, перечисленных в списке п.10 в), отчет должен содержать подробный анализ модели и проделанной работы.

Тема 3. Модель Take – Grant.

Цель работы: анализ и реализация на практике классической модели Take – Grant.

Содержание работы: классическая модель Take – Grant, распространение и похищение прав доступа в классической модели Take – Grant, алгоритмы проверки безопасности классических систем Take – Grant.

Результат: отчет о проделанной работе.

Методические указания: выполнение задания должно вестись с использованием программных продуктов, перечисленных в списке п.10 в), отчет должен содержать подробный анализ модели и проделанной работы.

Тема 4. Расширенная модель Take – Grant.

Цель работы: анализ и реализация на практике расширенной модели Take – Grant.

Содержание работы: расширенная модель Take – Grant, алгоритмы построения замыканий графа доступов и информационных потоков в расширенной модели Take – Grant, анализ путей распространения прав доступа и информационных потоков в расширенной модели Take – Grant, алгоритмы проверки безопасности расширенных систем Take – Grant.

Результат: отчет о проделанной работе.

Методические указания: выполнение задания должно вестись с использованием программных продуктов, перечисленных в списке п.10 в), отчет должен содержать подробный анализ модели и проделанной работы.

Тема 5. Модель Белла – ЛаПадула.

Цель работы: анализ и реализация на практике классической модели Белла – ЛаПадула и ее вариаций.

Содержание работы: классическая модель Белла – ЛаПадула, модель мандатной политики целостности информации Биба, функции переходов, свойства безопасности и алгоритмы ее проверки для модели Белла – ЛаПадула и ее вариаций.

Результат: отчет о проделанной работе.

Методические указания: выполнение задания должно вестись с использованием программных продуктов, перечисленных в списке п.10 в), отчет должен содержать подробный анализ модели и проделанной работы.

Тема 6. Модель систем военных сообщений.

Цель работы: анализ и реализация на практике модели СВС.

Содержание работы: модель СВС, функции переходов для модели СВС, алгоритмы проверки безопасности систем СВС.

Результат: отчет о проделанной работе.

Методические указания: выполнение задания должно вестись с использованием программных продуктов, перечисленных в списке п.10 в), отчет должен содержать подробный анализ модели и проделанной работы.

Тема 7. Автоматная модель безопасности информационных потоков.

Цель работы: анализ и реализация на практике автоматной модели безопасности информационных потоков и ее вариаций.

Содержание работы: автоматная модель безопасности информационных потоков, модель контроля информационных потоков, вероятностная модель безопасности информационных потоков, эффективность механизма защиты, алгоритмы проверки эффективности контролирующего механизма защиты, информационной невыводимости и информационного невлияния.

Результат: отчет о проделанной работе.

Методические указания: выполнение задания должно вестись с использованием программных продуктов, перечисленных в списке п.10 в), отчет должен содержать подробный анализ модели и проделанной работы.

Тема 8. Субъектно-ориентированная модель изолированной программной среды.

Цель работы: анализ и реализация на практике субъектно-ориентированной модели ИПС.

Содержание работы: правила разграничения доступа субъектов к объектам, корректность субъектов друг относительно друга, МБО, МПС, МБС, порождение с контролем неизменности объекта-источника, гарантированное выполнение политики безопасности в компьютерной системе, построение ИПС.

Результат: отчет о проделанной работе.

Методические указания: выполнение задания должно вестись с использованием программных продуктов, перечисленных в списке п.10 в), отчет должен содержать подробный анализ модели и проделанной работы.

Тема 9. Модель администрирования ролевого разграничения доступа.

Цель работы: анализ и реализация на практике модели администрирования РРД.

Содержание работы: базовая модель РРД, иерархия ролей, администрирование множеств авторизованных ролей пользователей, администрирование множеств прав доступа, которыми обладают роли, администрирование иерархии ролей, построение модели администрирования РРД.

Результат: отчет о проделанной работе.

Методические указания: выполнение задания должно вестись с использованием программных продуктов, перечисленных в списке п.10 в), отчет должен содержать подробный анализ модели и проделанной работы.

Тема 10. Модель мандатного ролевого разграничения доступа.

Цель работы: анализ и реализация на практике модели мандатного РРД.

Содержание работы: модель мандатного РРД, построение мандатного РРД и его соответствие требованиям строгого мандатного разграничения доступа, либерального мандатного разграничения доступа, строгого мандатного контроля целостности, либерального мандатного контроля целостности.

Результат: отчет о проделанной работе.

Методические указания: выполнение задания должно вестись с использованием программных продуктов, перечисленных в списке п.10 в), отчет должен содержать подробный анализ модели и проделанной работы.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Данный вид работы не предусмотрен УП.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ (ЗАЧЕТУ)

1. Основные понятия и определения дисциплины (объект, субъект, доступ, право доступа, преобразование информации, информационный поток, активизация, пользователь). Аксиома представления информации в компьютерной системе. Основная аксиома теории защиты информации.
2. Понятие угрозы безопасности информации. Основные виды угроз безопасности информации. Неблагоприятные информационные потоки и их реализация.
3. Понятие политики безопасности. Основные виды политик безопасности (дискреционная политика безопасности, мандатная политика безопасности). Цели, достоинства и недостатки политик каждого вида.
4. Основные виды политик безопасности (политика безопасности информационных потоков, политика ролевого разграничения доступа, политика изолированной программной среды). Цели, достоинства и недостатки политик каждого вида.
5. Модель решетки. Примеры различных моделей решетки.
6. Основные модели оценки ценности информации (аддитивная модель, анализ риска, порядковая шкала, решетка подмножеств). Цели, достоинства и недостатки каждой из моделей оценки ценности информации.
7. Классификация моделей безопасности компьютерных систем.
8. Формальное описание модели ХРУ. Примитивные операторы модели ХРУ. Команды модели ХРУ. Примеры команд для модели ХРУ.
9. Анализ безопасности систем ХРУ. Понятия утечки права, безопасного начального состояние по отношению к праву и монооперационной системы ХРУ. Теорема о разрешимости задачи проверки безопасности для монооперационных систем ХРУ.
10. Теорема о неразрешимости задачи проверки безопасности произвольной системы ХРУ.
11. Формальное описание модели ТМД. Примитивные операторы модели ТМД. Команды модели ТМД. Примеры команд для модели ТМД.
12. Модель монотонной ТМД и ее каноническая форма. Теорема о сводимости любой модели МТМД к КФМТМД.
13. Родительские и дочерние типы в модели ТМД. Граф создания типов для модели ТМД. Модель ациклической монотонной ТМД. Алгоритм проверки безопасности системы АМТМД.
14. Алгоритм построения развернутого состояния для системы АКФМТМД. Свойства данного алгоритма. Функция порождения объектов.
15. Теорема о разрешимости задачи проверки безопасности АМТМД. Сложность алгоритмов проверки безопасности систем АМТМД и тернарных систем АМТМД.
16. Формальное описание классической модели Take – Grant. Граф доступов. Основная цель классической модели Take – Grant. Де-юре правила преобразования графов доступов для классической модели Take – Grant.
17. Санкционированное получение прав доступа в классической модели Take – Grant. tg-связность вершин в графе доступов классической модели Take – Grant. Предикат “возможен доступ”. Теорема о распространении прав доступа в субъектных системах Take – Grant.

18. Понятия острова, моста и его начального и конечного пролетов в произвольном графе доступов классической модели Take – Grant. Теорема о распространении прав доступа в классической системе Take – Grant общего вида.
19. Похищение прав доступа в классической модели Take – Grant. Предикат “возможно похищение”. Теорема о похищении прав доступа в классической системе Take – Grant общего вида.
20. Построение гомоморфизма системы Take – Grant и системы ХРУ.
21. Формальное описание расширенной модели Take – Grant. Де-факто правила преобразования графов доступов и информационных потоков для расширенной модели Take – Grant.
22. Предикат “возможна запись”. Теорема о разрешении на запись для расширенной модели Take – Grant.
23. Замыкание графа доступов и информационных потоков расширенной модели Take – Grant. Алгоритмы построения замыкания и tg-замыкания графа доступов и информационных потоков. Корректность указанных алгоритмов.
24. Алгоритмы построения де-юре-замыкания и де-факто-замыкания графа доступов и информационных потоков. Корректность указанных алгоритмов.
25. Анализ путей распространения прав доступа и информационных потоков. Подходы к определению стоимости пути в графе доступов и информационных потоков.
26. Формальное описание классической модели Белла – ЛаПадула. Понятие системы. Основные запросы в классической модели Белла – ЛаПадула. Состояние элемента системы и его возможные изменения.
27. Свойства системы, определяющие ее безопасность в классической модели Белла – ЛаПадула. Безопасная система.
28. Теоремы об обладании системой *-свойством, ss-свойством и ds-свойством для классической модели Белла – ЛаПадула. Базовая теорема безопасности.
29. Пример некорректного определения свойств безопасности для классической модели Белла – ЛаПадула.
30. Формальное описание модели Белла – ЛаПадула, реализующей политику low-watermark. Основные операции модели. Переопределение ss-свойства и *-свойства. Лемма о безопасных состояниях системы.
31. Функции переходов и их использование в модели Белла – ЛаПадула. Безопасность переходов. Переопределение ss-свойства и *-свойства. Теоремы об обладании системой *-свойством и ss-свойством.
32. Безопасная функция переходов для модели Белла – ЛаПадула. Базовая теорема безопасности в терминах функции переходов.
33. Формальное описание модели мандатной политики целостности информации Биба и ее свойства. Соответствие доступа требованиям политики low-watermark.
34. Модель СВС. Основные определения, связанные с данной моделью (роль пользователя, объект, контейнер и способ доступа к его содержимому, сущность и ее идентификатор, непосредственная и косвенная ссылки, операция, сообщение). Постулаты безопасности для СВС.
35. Неформальное описание модели СВС. Основные неформальные свойства модели СВС.
36. Формальное описание модели СВС. Состояние системы.
37. Безопасное состояние для СВС. История системы. Эквивалентность безопасных состояний системы. Потенциальная модификация сущности по ссылке с источником.
38. Смыслы безопасности функции переходов для модели СВС. Теоремы о безопасности для модели СВС.
39. Формальное описание автоматной модели безопасности информационных потоков. Информационное невлияние. Политика безопасности автоматной модели безопасности информационных потоков. Невидимость и изолированность пользователя.
40. Формальное описание программной модели контроля информационных потоков. Политика безопасности “допустить”. Эффективность механизма защиты. Соотношения между эффективными механизмами защиты.
41. Контролируемый механизм защиты. Теорема об эффективности контролируемого механизма защиты.
42. Вероятностная модель безопасности информационных потоков. Схема компьютерной системы. Информационная невыводимость.
43. Информационное невлияние. Соответствие требованиям информационного невлияния. Примеры.

44. Субъектно-ориентированная модель ИПС. Аксиома порождения компьютерных субъектов. Источник для субъекта. Объекты, функционально ассоциированные с субъектами. Потоки информации от объекта к объекту.
45. Доступ субъекта к объекту. Правила разграничения доступа субъектов к объектам. Тождественность субъектов. Монитор обращений. Виды МО.
46. Монитор безопасности объектов. Корректность субъектов друг относительно друга. Достаточное условие гарантированного выполнения политики безопасности в компьютерной системе.
47. Мониторы порождения и безопасности субъектов. Замкнутость компьютерной системы по порождению субъектов. Изолированное множество субъектов программной среды. Второе достаточное условие гарантированного выполнения политики безопасности в компьютерной системе.
48. Порождение субъекта с контролем неизменности объекта-источника в рамках ИПС. Базовая теорема ИПС. Метод субъектно-объектного взаимодействия в рамках ИПС.
49. Практическая реализация ИПС для современной компьютерной системы. Состояние компьютерной системы. Условие одинакового состояния. Достаточное условие ИПС при ступенчатой загрузке.
50. Понятия роли. Ролевое разграничение доступа. Формальное описание базовой модели РРД. Общая структура элементов базовой модели РРД.
51. Иерархия ролей в базовой модели РРД. Механизм ограничений в базовой модели РРД.
52. Формальное описание модели администрирования РРД. Иерархия ролей в модели администрирования РРД.
53. Администрирование множеств авторизованных ролей пользователей в модели РРД. Пример иерархии ролей и иерархии администрирования ролей.
54. Предварительные условия для роли в модели РРД. Функции администрирования множеств авторизованных ролей пользователей на множестве административных ролей. Примеры.
55. Администрирование множеств прав доступа, которыми обладают роли в модели РРД. Функции для администрирования множеств прав доступа на множестве административных ролей. Примеры.
56. Администрирование иерархии ролей для модели РРД. Роли-возможности. Роли-группы. Роли-объединения. Отношение превосходства для роли-объединения.
57. Функции для администрирования возможностей, групп пользователей и иерархии ролей на множестве административных ролей для модели РРД. Примеры определения функций для администрирования иерархии ролей на множестве административных ролей.
58. Формальное описание модели мандатного РРД. Виды мандатного разграничения доступа. Безопасный доступ. Иерархии на множестве ролей.
59. Защита от угрозы конфиденциальности информации для модели РРД. Элементы модели мандатного РРД. Виды мандатного разграничения доступа. Безопасный доступ. Иерархии на множестве ролей.
60. Соответствие модели РРД требованиям строгого и либерального мандатных разграничений доступа. Задание иерархии ролей и ограничений в соответствии с требованиями либерального или строгого мандатного управления доступом. Теорема о безопасности информационных потоков.
61. Защита от угроз конфиденциальности и целостности информации для модели РРД. Безопасный доступ. Иерархии на множестве ролей. Соответствие модели РРД требованиям либерального мандатного контроля целостности.
62. Соответствие модели РРД требованиям строгого мандатного контроля целостности. Соответствие модели РРД требованиям либерального мандатного разграничения доступа и контроля целостности.
63. Общая постановка задачи построения защиты системы. Гомоморфизм компьютерной системы и ее математической модели безопасности. Проблема адекватности реализации модели безопасности в реальной компьютерной системе.
64. Проблемы реализации дискреционной политики безопасности. Реализация атаки с использованием программных закладок вида “троянский конь”.
65. Проблемы реализации мандатной политики безопасности. Пример реализации неблагоприятных информационных потоков по памяти.
66. Пример реализации неблагоприятных информационных потоков по времени для мандатной политики безопасности. Способы противодействия появлению неблагоприятных информационных потоков.

67. Угрозы безопасности компьютерной системы в рамках политики безопасного администрирования. Уровни возможностей нарушителя. Требования безопасности. Цель политики безопасности администрирования.
68. Элементы математической модели политики безопасного администрирования. Доверенные и недоверенные субъекты. Непосредственное подчинение. Граф подчиненности.
69. Исходные предположения и угрозы для математической модели политики безопасного администрирования.
70. Функции ОС Astra Linux SE по защите информации от НСД. Краткое описание реализации.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

Форма обучения:___очная _____

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа, подготовка к сдаче зачета, экзамена и др.)***	**Объем в часах**	**Форма контроля (*проверка решения задач, реферата и др.)***
Раздел 1. Основы формальной теории защиты информации.	Проработка учебного материала контрольная работа, подготовка к сдаче зачета, экзамена	2	Ответы на вопросы
Раздел 2. Модели систем с дискреционным разграничением доступа.	Проработка учебного материала контрольная работа, подготовка к сдаче зачета, экзамена	10	Ответы на вопросы, лабораторная работа
Раздел 3. Модели систем с мандатным разграничением доступа.	Проработка учебного материала контрольная работа, подготовка к сдаче зачета, экзамена	12	Ответы на вопросы, лабораторная работа
Раздел 4. Модели безопасности информационных потоков и изолированной программной среды.	Проработка учебного материала контрольная работа, подготовка к сдаче зачета, экзамена	8	Ответы на вопросы, лабораторная работа
Раздел 5. Модели систем с ролевым разграничением	Проработка учебного материала контрольная работа, подготовка к сдаче зачета, экзамена	12	Ответы на вопросы, лабораторная

доступа.			работа
Раздел 6. Применение и дальнейшее развитие моделей безопасности компьютерных систем.	Проработка учебного материала контрольная работа, подготовка к сдаче зачета, экзамена	10	Ответы на вопросы, лабораторная работа

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная :

1. Богульская, Н. А. Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров. — Красноярск : Сибирский федеральный университет, 2019. — 206 с. — ISBN 978-5-7638-4008-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/100055.html
2. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие для вузов / Девянин П. Н. - 2-е изд. , испр. и доп. - Москва : Горячая линия - Телеком, 2013. - 338 с. - ISBN 978-5-9912-0328-9. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785991203289.html

дополнительная:

1. Магазанник, В. Д. Человеко-компьютерное взаимодействие : Учебн. пособие. / Магазанник В. Д. - Москва : Логос, 2007. - 256 с. - ISBN 978-5-98704-241-0. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785987042410.html
2. Климентьев, К. Е. Компьютерные вирусы и антивирусы : взгляд программиста / Климентьев К. Е. - Москва : ДМК Пресс, 2013. - 656 с. - ISBN 978-5-94074-885-4. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785940748854.html

учебно-методическая:

1. Методические указания для самостоятельной работы студентов по дисциплине «Модели безопасности компьютерных систем» для специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения / В. М. **Барахов**; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 420 КБ). - Текст : электронный. http://lib.ulsu.ru/MegaPro/Download/MObject/10160

Согласовано:

Ведущий специалист НБ УлГУ / Терехина Л.А. / ___ / 04.05.2023 /
должность сотрудника научной библиотеки ФИО подпись дата

б) Программное обеспечение:

Для образовательного процесса по данной дисциплине необходим стационарный класс ПК со следующим установленным программным обеспечением:

– ОС Astra Linux SE 1.6 (желательно в виртуальной среде);
– Пакет офисных продуктов (для формирования отчетов).

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2023]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство «ЮРАЙТ». – Москва, [2023]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО «Политехресурс». – Москва, [2023]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО «Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг». – Москва, [2023]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО «Букап». – Томск, [2023]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС «Лань». – Санкт-Петербург, [2023]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС Znanium.com : электронно-библиотечная система : сайт / ООО «Знаниум». - Москва, [2023]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. / ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2023].

3. Базы данных периодических изданий:

3.1. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2023]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.2. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД «Гребенников». – Москва, [2023]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2023]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

Согласовано:
Инженер ведущий / Щуренко Ю.В. / _____ / 04.05.2023
Должность сотрудника УИТТ / ФИО / подпись / дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций, для выполнения лабораторных работ и практикумов, для проведения текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций.

Аудитории укомплектованы специализированной мебелью. Аудитории для проведения лекций оборудованы мультимедийным оборудованием для предоставления информации большой аудитории. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной инфромационно-образовательной среде, электронно-библиотечной системе. Перечень оборудования, используемого в учебном процессе, указывается в соответствии со сведениями о материально-техническом обеспечении и оснащенности образовательного процесса, размещенными на официальном сайте УлГУ в разделе «Сведения об образовательной организации».

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

Разработчик _____ доцент _____ И.А. Перцева
подпись / должность / ФИО