МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / Д.Г. Демидов /
«16» 02 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита информации в системах обработки данных»

Направление подготовки
10.04.01 «Информационная безопасность»

Профиль
«Системы управления информационной безопасностью»

Квалификация
Магистр

Формы обучения
Очная

Москва, 2023 г.

Разработчик(и):
Доцент кафедры «Информационная безопасность»,
к.т.н, доцент:

/ И.В. Калуцкий /

Согласовано:
И.о. заведующего кафедрой «Информационная безопасность»,

А.Ю. Гневшев

Руководитель образовательной программы
Доцент. к.т.н.

/С.А. Кесель/

Содержание

1	Цели, задачи и планируемые результаты обучения по дисциплине	4
2	Место дисциплины в структуре образовательной программы	6
3	Структура и содержание дисциплины	6
3.1	Виды учебной работы и трудоемкость	6
3.2	Тематический план изучения дисциплины	7
3.3	Содержание дисциплины	8
3.4	Тематика семинарских/практических и лабораторных занятий	11
3.5	Тематика курсовых проектов (курсовых работ)	13
4	Учебно-методическое и информационное обеспечение	13
4.1	Нормативные документы и ГОСТы	13
4.2	Основная литература	16
4.3	Дополнительная литература	17
4.4	Электронные образовательные ресурсы	17
4.5	Лицензионное и свободно распространяемое программное обеспечение	17
4.6	Современные профессиональные базы данных и информационные справочные системы	17
5	Материально-техническое обеспечение	17
6	Методические рекомендации	18
6.1	Методические рекомендации для преподавателя по организации обучения	18
6.2	Методические указания для обучающихся по освоению дисциплины	18
7	Фонд оценочных средств	19
7.1	Методы контроля и оценивания результатов обучения	19
7.2	Шкала и критерии оценивания результатов обучения	27
7.3	Оценочные средства	28

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Защита информации в системах обработки данных» следует отнести:

Сформировать компетенции обучающегося в области защиты информации в системах обработки данных различных уровней и типов.

К **основным задачам** освоения дисциплины «Защита информации в системах обработки данных» следует отнести:

- Рассмотреть базовые дискреционные модели безопасности
- Рассмотреть базовую модель изолированной программной среды
- Рассмотреть базовые мандатные модели безопасности
- Рассмотреть базовые модели ролевого управления доступом
- Рассмотреть базовые модели безопасности информационных потоков
- Рассмотреть различные ДП-модели

Обучение по дисциплине **«Защита информации в системах обработки данных»** направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ПК-1. Способен анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	ИПК-1.1. Применяет знания направлений развития информационных технологий, основных видов политик безопасности объектов защиты; ИПК-1.2. Умеет прогнозировать эффективность функционирования, оценивать затраты и риски объектов защиты; ИПК-1.3. Владеет навыками формирования политики безопасности объектов защиты
ПК-4. Способен разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	ИПК-4.1. Знает: программы и методики испытаний средств и систем обеспечения информационной безопасности в соответствии с нормативными актами. ИПК-4.2. Умеет: разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности ИПК-4.3. Владеет: навыками проведения испытаний средств и систем обеспечения информационной безопасности

2 Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации в системах обработки данных» относится к числу профессиональных учебных дисциплин обязательной части базового цикла (Б1.1) основной образовательной программы магистратуры (Б1.1.2)

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП: «Управление информационной безопасностью», «Построение и совершенствование систем управления информационной безопасностью»,

«Производственная практика (научно-исследовательская работа)», «Производственная практика (проектно-технологическая)», «Производственная практика (преддипломная)».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных(е) единиц(ы) (144 часов) во втором семестре.

1. Виды учебной работы и трудоемкость
(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**72**	2	1-18
	В том числе:			
1.1	Лекции			
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	72	2	1-18
2	**Самостоятельная работа**	**72**	2	1-18
3	**Промежуточная аттестация**	**Экзамен**	Экзамен	По расписанию
	Итого:	**144**		

2. Тематический план изучения дисциплины

(по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Раздел 1. Модели дискреционного управления доступом						
1.1	Тема 1. Основные понятия и определения	2					2
1.2	Тема 2. Модели ХРУ	4			2		2
1.3	Тема 3. Модель типизированной матрицы доступов	4			2		2
1.4	Тема 4. Модель Take-Grant	4			2		2
1.5	Тема 5. Расширенная модель Take-Grant	6			4		2
2	Раздел 2. Модели ИПС и мандатного управления доступом						
2.1	Тема 1. Субъектно-ориентированная модель ИПС	4			2		2
2.2	Тема 2. Модели Белла-ЛаПадулы	6			2		4
2.3	Тема 3. Модель СВС	6			2		4
3	Раздел 3. Безопасность информационных потоков и ролевое управление доступом						
3.1	Тема 1. Автоматная, программная и вероятностная модели безопасности информационных потоков	6			2		4
3.2	Тема 2. Базовая модель ролевого управления доступом	4			2		2
3.3	Тема 3. Модель администрирования ролевого управления доступом	8			4		4
3.4	Тема 4. Модель мандатного ролевого управления доступом	8			4		4
4	Раздел 4. Базовая и ИПС ДП-модели						
4.1	Тема 1. Базовая ДП-модель	4			2		2
4.2	Тема 2. ДП-модель без кооперации доверенных и недоверенных субъектов	8			4		4
4.3	Тема 3. ФАС ДП-модель	6			2		4
4.4	Тема 4. ПБА и ПАР ДП-модели	4			2		2
4.5	Тема 5. ФПАС-модель	2					2
4.6	Тема 6. Применение ФАС ДП-модели для анализа безопасности веб-систем, ФС ДП-модель	6			4		2
4.7	Тема 7. Методы предотвращения утечки прав доступа в реализации запрещенных информационных потоков	6			4		2
5	Раздел 5. Мандатная ДП-модель и ДП-модели безопасности информационных потоков						
5.1	Тема 1. Правила преобразованияй мандатной ДП-модели	4			2		2

5.2	Тема 2. Безопасность в смысле Белла-ЛаПадулы и условия повышения субъектом уровня доступа	4			2		2
5.3	Тема 3. ДП-модель с блокирующими доступами доверенных субъектов	4			2		2
5.4	Тема 4. Мандатная ДП-модель с блокирующими доступами доверенных субъектов и с отождествлением порожденных субъектов	4			2		2
5.5	Тема 5. Мандатная ДП-модель КС, реализующих политику строгого мандатного управления доступом	6			4		2
6	Раздел 6 Мандатная сущностно-ролевая ДП-модель.						
6.1	Тема 1. Состояние системы МРОСЛ	4			2		2
6.2	Тема 2. Параметризация модели МРОСЛ	6			4		2
6.3	Тема 3. Задание мандатного управления доступом и контроля целостности для состояний системы МРОСЛ	8			4		4
6.4	Тема 4. Правила преобразования состояний МРОСЛ	6			4		2
Итого		**144**			**72**		**72**

3. Содержание дисциплины

Раздел 1. Модели дискреционного управления доступом

Тема 1. Основные понятия и определения

Тема 2. Модели ХРУ

Тема 3. Модель типизированной матрицы доступов

Тема 4. Модель Take-Grant

Тема 5. Расширенная модель Take-Grant

Раздел 2. Модели ИПС и мандатного управления доступом

Тема 1. Субъектно-ориентированная модель ИПС

Тема 2. Модели Белла-ЛаПадулы

Тема 3. Модель СВС

Раздел 3. Безопасность информационных потоков и ролевое управление доступом

Тема 1. Автоматная, программная и вероятностная модели безопасности информационных потоков

Тема 2. Базовая модель ролевого управления доступом

Тема 3. Модель администрирования ролевого управления доступом

Тема 4. Модель мандатного ролевого управления доступом

Раздел 4. Базовая и ИПС ДП-модели

Тема 1. Базовая ДП-модель

Тема 2. ДП-модель без кооперации доверенных и недоверенных субъектов

Тема 3. ФАС ДП-модель

Тема 4. ПБА и ПАР ДП-модели

Тема 5. ФПАС-модель

Тема 6. Применение ФАС ДП-модели для анализа безопасности веб-систем, ФС ДП-модель

Тема 7. Методы предотвращения утечки прав доступа в реализации запрещенных информационных потоков

Раздел 5. Мандатная ДП-модель и ДП-модели безопасности информационных потоков

Тема 1. Правила преобразованияй мандатной ДП-модели

Тема 2. Безопасность в смысле Белла-ЛаПадулы и условия повышения субъектом уровня доступа

Тема 3. ДП-модель с блокирующими доступами доверенных субъектов

Тема 4. Мандатная ДП-модель с блокирующими доступами доверенных субъектов и с отождествлением порожденных субъектов

Тема 5. Мандатная ДП-модель КС, реализующих политику строгого мандатного управления доступом

Раздел 6. Мандатная сущностно-ролевая ДП-модель.

Тема 1. Состояние системы МРОСЛ

Тема 2. Параметризация модели МРОСЛ

Тема 3. Задание мандатного управления доступом и контроля целостности для состояний системы МРОСЛ

Тема 4. Правила преобразования состояний МРОСЛ

4. Тематика семинарских/практических и лабораторных занятий

Семинарские/практические занятия в учебном плане не запланированы.

3.4.2 Лабораторные занятия

1. Решение задач модели ХРУ
2. Решение задач моделей Take-Grant
3. Решение задач моделей с мандатным управлением доступом
4. Решение задач моделей безопасности информационных потоков
5. Решение задач моделей с ролевым управлением доступом
6. Решение задач базовой дискреционной ДП модели
7. Решение задач ДП-моделей ИПС
8. Решение задач мандатной ДП-модели
9. Решение задач ДП-моделей безопасности информационных потоков
10. Решение задач модели МРОСЛ

11. Тематика курсовых проектов (курсовых работ)

Курсовые проекты в учебном плане не запланированы.

4 Учебно-методическое и информационное обеспечение

1. Нормативные документы и ГОСТы

1. "Методический документ. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021)
2. ГОСТ Р 53131-2008 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения».
3. ГОСТ Р ИСО/МЭК 27005-2010 Национальный стандарт российской федерации информационная технология методы и средства обеспечения безопасности менеджмент риска информационной безопасности
4. "ГОСТ Р ИСО/МЭК 27001-2021. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"

5. ГОСТ Р ИСО/МЭК 27002-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности»

2. Основная литература

1. Груздева, Л. М. Защита информации : учебное пособие / Л. М. Груздева. — Москва : РУТ (МИИТ), 2019. — 144 с. — ISBN 978-5-7876-0326-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/188703

2. Информационная безопасность и защита информации в цифровой экономике элементы теории и тестовые задания : учебное пособие / И. Д. Алекперов, В. В. Храмов, А. А. Горбачева, Д. С. Фомичев. — Ростов-на-Дону : ИУБиП, 2020. — 114 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/248747

3. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401

4. Потерпеев, Г. Ю. Безопасность операционных систем : учебное пособие / Г. Ю. Потерпеев, В. С. Нефедов, А. А. Криулин. — Москва : РТУ МИРЭА, 2021. — 93 с. — ISBN 978-5-7339-1393-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182416

3. Дополнительная литература

1. Внуков, А. А. Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512269
2. «Защита информационных процессов в компьютерных системах» (Пушкарёв, В. В. Защита информационных процессов в компьютерных системах : учебное пособие / В. В. Пушкарёв, В. П. Пушкарёв. — Москва : ТУСУР, 2012. — 131 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/4925
3. Мандрица, И. В. Управление проектами по информационной безопасности и экономика защиты информации. Часть 1 / И. В. Мандрица, В. И. Петренко, О. В. Мандрица. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-45723-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/311825

4. Электронные образовательные ресурсы

1. ЭОР разрабатывается.
2. Московский Политех подключен к ЭБС: Юрайт, АйПиАр и Лань
3. https://mospolytech.ru/obuchauschimsya/biblioteka/

5. Лицензионное и свободно распространяемое программное обеспечение

Для выполнения лабораторных работ и самостоятельной работы необходимо следующее программное обеспечение:

1. Microsoft Windows.
2. Веб-браузер, Chrome.

6. Современные профессиональные базы данных и информационные справочные системы

1. Справочная правовая система "КонсультантПлюс" https://www.consultant.ru/
2. Официальный сайт ФСТЭК России https://fstec.ru/
3. Образовательная платформа «Юрайт» https://urait.ru/

5 Материально-техническое обеспечение

И лекционные и лабораторные занятия могут проводится дистанционно в формате онлайн. Преподавателю для проведения занятий необходим ноутбук с возможностью использования сервиса корпоративной платформы Microsoft Teams или других платформ для проведения занятий, например, Webinar. У студентов должна быть возможность выхода в Интернет.

6 Методические рекомендации

1. Методические рекомендации для преподавателя по организации обучения

При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

2. Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студентов помогает получить дополнительные теоретические и практические знаниями по изучаемой дисциплине, развивает сознательное отношение к интеллектуальному труду.

В процессе самостоятельной работы, студенты дорабатывают конспекты лекций, готовятся к экзамену, изучают рекомендованную литературу, осуществляют подборку нормативно-правовых документов и проводят ознакомительный анализ с ними, готовятся к лабораторным работам, выполняют домашние задания;

Самостоятельная работа позволяет закрепить и углубить знания, полученные во время аудиторных занятий, а также изучить отдельные темы учебной программы.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Лекционные занятия дают общее представление по изучаемой теме, основной знания студент получает в процессе выполнения лабораторных работ и самостоятельной работы.

Практические занятия проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами на лекциях и в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста по ИБ.

Домашним заданием, по большей части, является подготовка к следующей лабораторной работе. Студентам предлагается выполнить подбор литературы, нормативно-правовых документов, по тематике лабораторной работы, и предварительное ознакомление с ними.

При проведении лабораторной работы преподаватель *выполняет, в основном,* функции ведущего - следит за регламентом времени, помогает уточнить формулировки, отвечает на вопросы студентов, проверяет выполненные работы. На следующем занятии, подводится итог проведенной работы, студентам сообщаются результаты, ведется обсуждение рассмотренных вопросов подводится итог занятию в целом.

По результатам выполнения всех видов учебной работы, предусмотренных учебным планом (подготовка конспектов лекций, успешное выполнение лабораторных работ, подготовка домашнего задания, присутствие и активная работа на занятиях) по данной дисциплине (модулю), преподаватель может рассмотреть возможность проставления положительной оценки на экзамене «Автоматом», при этом учитываются результаты текущего контроля успеваемости в течение семестра. В случае, если студент длительно отсутствовал на занятиях, не выполнял задания он всё равно допускается до экзамена, но на экзамене, таким студентам, преподаватель может задавать любое количество вопросов по всем темам данной дисциплины (в рамках отведённого времени), дабы убедиться, что студент самостоятельно освоил дисциплину.

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

7 Фонд оценочных средств

1. Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- домашние задания и их защита;
- лабораторные работы
- дифференцированный зачёт.

2. Шкала и критерии оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю)

ПК-1. Способен анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: направления развития информационных (телекоммуникационных) технологий	Обучающийся демонстрирует полное отсутствие знаний направлений развития информационных (телекоммуникационных) технологий	Обучающийся демонстрирует неполное знание направлений развития информационных (телекоммуникационных) технологий	Обучающийся демонстрирует частичное знание направлений развития информационных (телекоммуникационных) технологий	Обучающийся демонстрирует полное знание направлений развития информационных (телекоммуникационных) технологий
уметь: прогнозировать эффективность функционирования объектов защиты	Обучающийся не умеет прогнозировать эффективность функционирования объектов защиты	Обучающийся демонстрирует неполное умение прогнозировать эффективность функционирования объектов защиты	Обучающийся демонстрирует частичное умение прогнозировать эффективность функционирования объектов защиты	Обучающийся демонстрирует полное умение прогнозировать эффективность функционирования

				объектов защиты
владеть: методами оценки затрат и рисков, формирования политик безопасности объектов защиты	Обучающийся не владеет методами оценки затрат и рисков, формирования политик безопасности объектов защиты	Обучающийся в неполном объеме владеет методами оценки затрат и рисков, формирования политик безопасности объектов защиты	Обучающийся частично владеет методами оценки затрат и рисков, формирования политик безопасности объектов защиты	Обучающийся в полном объеме владеет методами оценки затрат и рисков, формирования политик безопасности объектов защиты
ПК-4. Способен разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности				
знать: принципы разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует полное отсутствие знаний принципов разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует неполное знание принципов разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует частичное знание принципов разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует полное знание принципов разработки программ и методик испытаний средств и систем обеспечения информационной безопасности

уметь: использовать программы и методики испытаний средств и систем обеспечения информационной безопасности	Обучающийся не умеет использовать программы и методики испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует неполное умение использовать программы и методики испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует частичное умение использовать программы и методики испытаний средств и систем обеспечения информационной безопасности	Обучающийся демонстрирует полное умение использовать программы и методики испытаний средств и систем обеспечения информационной безопасности
владеть: принципами разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся не владеет принципами разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся в неполном объеме владеет принципами разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся частично владеет принципами разработки программ и методик испытаний средств и систем обеспечения информационной безопасности	Обучающийся в полном объеме владеет принципами разработки программ и методик испытаний средств и систем обеспечения информационной безопасности

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен

Промежуточная аттестация обучающихся, в форме экзамена, проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	Описание
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

3. Оценочные средства

7.3.1. Примерные задания по лабораторным работам

7.3.2 Примерный список вопросов для экзамена

1. Виды политик управления доступом и информационными потоками
2. Основные определения и классическая классификация угроз безопасности информации
3. Диаграмма основных видос формальных моделей безопасности
4. Описание модели ХРУ
5. Анализ безопасности истем ХРУ
6. Описание модели ТМД
7. Анализ безопасности систем ТМД
8. Описание классической модели Take-Grant
9. Анализ безопасности классической модели Take-Grant
10. Описание расширенной модели Take-Grant
11. Анализ безопасности расширенной модели Take-Grant
12. Описание субъектно-ориентированной модели ИПС
13. Определение классической модели Белла-ЛаПадулы
14. Политика low-watermark в модели Белла-ЛаПадулы
15. Безопасность переходов в модели Белла-ЛаПадулы

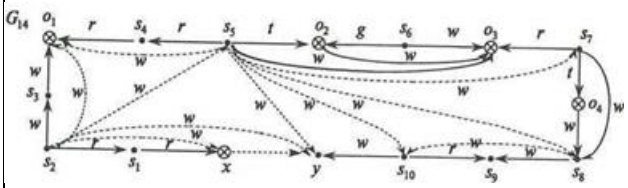
16. Модель мандатной политики целостности информации Биба
17. Описание модели СВС
18. Автоматная и программная модели безопасности информационных потоков
19. Вероятностная модель безопасности информационных потоков
20. Описание базовой модели ролевого управления доступом
21. Основные положения и администрирование множеств авторизованных ролей пользователей в ролевом управлении доступом
22. Администрирование множеств прав доступа и иерархии ролей в ролевом управлении доступом
23. Защита от угрозы конфиденциальности информации в модели мандатного ролевого управления доступом
24. Защита от угроз конфиденциальности и целостности информации в модели мандатного ролевого управления доступом
25. Определение базовой ДП-модели
26. Условия передачи прав доступа в базовой ДП-модели
27. Условия реализации информационного потока по памяти в базовой ДП-модели
28. Условия реализации информационного потока по времени в базовой ДП-модели
29. Условия передачи прав доступа в базовой ДП-модели без кооперации доверенных и недоверенных субъектов
30. Условия реализации запрещенных информационных потоков по памяти и по времени в базовой ДП-модели без кооперации доверенных и недоверенных субъектов
31. Определение ФАС ДП-модели и условия истинности предикатов
32. Корректные субъекты в ФАС ДП-модели
33. Определение ПБА ДП-модели
34. Условия реализации политики безопасного администрирования в ПБА ДП-модели
35. Определение ПАР ДП-модели
36. Определение ФПАС ДП-модели
37. Использование ФАС-модели для анализа веб-системы
38. Метод предотвращения возможности получения права доступа владения недоверенным субъектом к доверенному субъекту
39. Метод реализации ПБА
40. Метод реализации ПАР
41. Определения и предположения в мандатной ДП-модели
42. Правила преобразования состояний мандатной ДП-модели
43. Безопасность в смысле Белла-ЛаПадулы для мандатной ДП-модели
44. Условия повышения субъектом уровня доступа в мандатной ДП-модели
45. Определение ДП-модели с блокирующими доступами доверенных субъектов
46. Условия истинности предиката can_write_time_block в ДП-модели с блокирующими доступами
47. доверенных субъектов
48. Определение мандатной ДП-модели с блокирующими доступами доверенных субъектов
49. Условия истинности предиката can_write_time_down_block в ДП-модели с блокирующими
50. доступами доверенных субъектов
51. Мандатная ДП-модель с отождествлением порожденных субъектов
52. Определение мандатной ДП-модели КС, реализующих политику строгого мандатного управления доступом
53. Предикат can_write_time_down_block в мандатной ДП-модели КС, реализующих политику строгого мандатного управления доступом
54. Определение состояния системы МРОСЛ

55. Функционально или параметрически ассоциированные сущности в системе МРОСЛ
56. Доступы и права доступа в системе МРОСЛ
57. Задание мандатного управления доступом для состояний системы МРОСЛ
58. Задание мандатного контроля целостности для состояний системы МРОСЛ
59. Де-юре правила преобразования состояний МРОСЛ
60. Де-факто правила преобразования состояний МРОСЛ

Примеры заданий

1.

№ п/п	Условия типовых задач (задач, кейсов)	Ответ
1	Задание. Задает ли решетку представленный граф:	В соответствии с определением выполнены все свойства отношения частичного порядка «≤» на множестве {a, b, c, d, e, f}. Для каждой пары вершин, соединенных в графе путем, существует наименьшая верхняя и наибольшая нижняя границы. Например, справедливы равенства f ⊕ b = f и f ⊗ b = b. Для каждой пары, не соединенных в графе путем, приведем значения наименьших верхних и наибольших нижних границ: d ⊕ e = a, d ⊗ e = f; b ⊕ e = a, b ⊗ e = f; d ⊕ c = a, d ⊗ c = f; b ⊕ c = a, b ⊗ c = f. Следовательно, по определению граф задает решетку.
2	Проверьте, истинен ли предикат *can_share*(α, *x*, *y*, G_0) для графа доступов G_0 на рисунке:	Введем обозначения для объектов и субъектов графа доступов $G_0 = (S_0, O_0, E_0)$. Существует субъект $s = s' \in S_0$ такой, что верно условие $(S_i, y, a) \in E_0$, следовательно, условие 1 теоремы выполнено. Так как *s* является субъектом, и существует субъект $x' \in S_0$ такой, что он соединен с объектом *x* начальным пролетом моста, то условие 2 теоремы выполнено. Выделим в графе G_0 острова $I_1 = \{x', s_1\}$, $I_2 = \{s_2\}$, $I_3 = \{s_3, s_4\}$, $I_4 = \{s_5, s_6, s\}$. Каждая пара соседних островов соединена мостом: I_1 и I_2 соединены мостом, проходящим через вершины s_1, o_2, o_3, s_2; I_2 и I_3 соединены мостом, проходящим через вершины s_2, o_4, o_5, s_3; I_3 и I_4 соединены мостом, проходящим через вершины s_4, o_6, s_5. Следовательно, условие 3 теоремы выполнено. Таким образом, выполнены все условия теоремы, и предикат *can_share*(α, *x*, *y*, G_0) является истинным.

3	Задание. Проверьте, истинен ли предикат *can_write*(x, y, G_0) для графа доступов G_0 на рисунке ниже. Решение задачи должно быть получено путем непосредственного применения де-юре и де-факто правил.	Введем обозначения для объектов и субъектов графа доступов G_0. Применим к графу G_0 следующие де-юре правила: op_1 = *grant*(w, s_6, o_2, o_3); op_2 = *take*(w, s_5, o_2, o_3); op_3 = *take*(w, s_7, o_4, s_8). Получим граф G_3 такой, что выполняется условие $G_0 \vdash_{op1} G_1 \vdash_{op2} G_2 \vdash_{op3} G_3$. Применим к графу G_3 следующие де-факто правила: op_4 = *spy*(s_2, s_1, x); op_5 = *find*(s_2, s_3, o_1); op_6 = *spy*(s_5, s_4, o_1); op_7 = *post*(s_5, s_2, o_1); op_8 = *post*(s_7, s_5, o_3); op_9 = *find*(s_5, s_7, s_8); op_{10} = *post*(s_{10}, s_8, s_9); op_{11} = *find*(s_5, s_8, s_{10}); op_{12} = *find*(s_5, s_{10}, y); op_{13} = *find*(s_2, s_5, y); op_{14} = *pass*(s_2, y, x). Получим граф G_{14} такой, что выполняются условия $G_0 \vdash_{op1} G_1 \vdash_{op2} \ldots \vdash_{op14} G_{14} = (S_{14}, O_{14}, E_{14} \cup F_{14})$ И (x,y,w) $\in F_{14}$.
		 Следовательно, предикат *can_write*(x, y, G_0) является истинным.