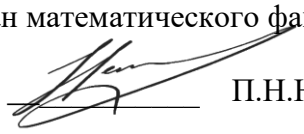
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета



П.Н.Нестеров

«18» мая 2021 г.

Рабочая программа дисциплины
«Математические модели для информационной безопасности»

Направление подготовки
10.06.01 Информационная безопасность

Направленность (профиль)
«Методы и системы защиты информации,
информационная безопасность»

Форма обучения очная

Программа рассмотрена
на заседании кафедры компьютерной безопасности
и математических методов обработки информации
от «16» апреля 2021 года, протокол № 8

Ярославль

1. Цели освоения дисциплины

Дисциплина «Математические модели для информационной безопасности» обеспечивает приобретение фундаментальных и профессиональных знаний, умений и навыков, содействует дальнейшей фундаментализации образования, развитию логического мышления и формированию математического и общенаучного мировоззрения. Целью изучения дисциплины является освоение современных подходов к построению и исследованию математических моделей систем обеспечения информационной безопасности компьютерных систем с последующим математическим доказательством их соответствия выбранной политике обеспечения информационной безопасности.

2. Место дисциплины в структуре программы аспирантуры

Дисциплина «Математические модели для информационной безопасности» является дисциплиной по выбору вариативной части.

3. Планируемые результаты обучения по дисциплине – знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций и обеспечивающие достижение планируемых результатов освоения программы аспирантуры, и критерии их оценивания

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- **Профессиональные компетенции:**
- способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-1);

Результаты обучения выпускника формулируются в следующих категориях:
«знать» – означает способность выпускника воспроизводить учебный материал с требуемой степенью научной точности (формулировать определение, с достаточной полнотой описывать процесс и явление);
«уметь» – означает способность выпускника решать типовые (адаптированные) задачи на основе воспроизведения алгоритма решения и его применения в конкретных стандартных условиях;
«владеть» – означает способность выпускника решать усложненные, в том числе комплексные задачи. Задачи данного уровня решаются на основе ранее приобретенных знаний и умений, с их трансформацией и применением в новых нетиповых условиях.

Код компетенции	**Планируемые результаты обучения**	**Критерии оценивания результатов обучения**		
		Пороговый уровень	**Продвинутый уровень**	**Высокий Уровень**
способностью выявлять основные угрозы безопасности информации, строить и	**Знать:** основные угрозы безопасности информации и способы построения	**Знает:** основные угрозы безопасности информации и способы построения	**Знает:** основные угрозы безопасности информации и способы построения	**Знает:** основные угрозы безопасности информации и способы построения

исследовать модели нарушителя в компьютерных системах (ПК-1)	модели нарушителя. **Уметь:** строить модели нарушителя в компьютерных системах . **Владеть:** навыками исследования модели нарушителя в компьютерных системах.	модели нарушителя.	модели нарушителя. **Умеет:** Строить модели нарушителя в компьютерных системах .	модели нарушителя. **Умеет:** Строить модели нарушителя в компьютерных системах . **Владеет:** Навыками исследования модели нарушителя в компьютерных системах.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 акад.часов

Дисциплина изучается в течение второго семестра. Формой итоговой промежуточной аттестации по дисциплине является зачет.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий и их трудоемкость (в академических часах)					Формы текущего контроля успеваемости Форма промежуточной аттестации *(по семестрам)*
			лекции	практические	лабораторные	консультации	самостоятельная работа	
1	Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем.	2	1				12	
2	Модели компьютерных систем с дискреционным управлением доступом**.**	2	1			0,5	12	Собеседование на консультации
3	Модель распространения прав доступа Take-Grant.	2	1			0,5	12	Собеседование на консультации
4	Модели изолированной программной среды.	2	1				12	
5	Модели компьютерных систем с мандатным управлением доступом.	2	1			0,5	12	Собеседование на консультации
6	Модели безопасности	2	1			0,5	12	

	информационных потоков.							
7	Модели компьютерных систем с ролевым управлением доступом.	2	1				12	
8	ДП-модели.	2	1				14	
		2						Зачет
	Всего		**8**			**2**	**98**	

Содержание разделов дисциплины

Тема 1. Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем.

Элементы теории компьютерной безопасности. Сущность, субъект, доступ, информационный поток.

Классификация угроз безопасности информации.

Виды информационных потоков.

Виды политик управления доступом и информационными потоками.

Утечка права доступа и нарушение безопасности КС.

Математические основы моделей безопасности. Основные понятия, автоматы, графы. Алгоритмические проблемы: разрешимые и неразрешимые алгоритмические проблемы.

Основные виды формализованных моделей безопасности КС.

Проблема адекватности реализации модели безопасности в реальной КС.

Тема 2. Модели компьютерных систем с дискреционным управлением доступом.

Модель матрицы доступов Харрисона - Руззо - Ульмана (ХРУ, HRU). Описание модели, анализ безопасности систем ХРУ.

Алгоритмическая неразрешимость проблемы утечки для модели HRU.

Модель типизированной матрицы доступов.

Тема 3. Модель распространения прав доступа Take-Grant.

Основные положения классической модели Take-Grant.

Расширенная модель Take-Grant.

Представление систем Take-Grant системами HRU.

Дискреционные ДП-модели. Базовая ДП-модель

ДП-модели без кооперации доверенных и недоверенных субъектов.

Тема 4. Модели изолированной программной среды.

Субъектно-ориентированная модель изолированной программной среды.

Корректность субъектов в ДП-моделях КС с дискреционным управлением доступом.

ДП-модель с функционально ассоциированными с субъектами сущностями.

ДП-модель для политики безопасного администрирования.

ДП-модель для политики абсолютного разделения административных и пользовательских полномочий.

ДП-модель с функционально или параметрически ассоциированными с субъектаим сущностями.

Методы предотвращения утечки прав доступа и реализации запрещенных информационных потоков.

Метод предотвращения возможности получения права доступа владения недоверенным субъектом к доверенному субъекту.

Метод реализации политики безопасности администрирования.

Метод реализации политики абсолютного разделения административных и пользовательских полномочий.

Тема 5. Модели компьютерных систем с мандатным управлением доступом.

Модель Балла - ЛаПадулы: классическая модель Белла - ЛаПадулы, пример некорректного администрирования.

Политика low-watermark в модели Белла - ЛаПадулы.

Безопасность переходов.

Модель мандатной политики целостности информации Биба.

Модель систем военных сообщений: общие положения и основные понятия.

Неформальное и формальное описания модели СВС.

Мандатная ДП-модель.

Правила преобразования состояний мандатной ДП-модели.

Безопасность в смысле Белла - ЛаПадулы.

Тема 6. Модели безопасности информационных потоков.

Автоматная модель безопасности информационных потоков.

Программная модель контроля информационных потоков.

Вероятностная модель безопасности информационных потоков.

ДП-модель безопасности информационных потоков по времени.

Тема 7. Модели компьютерных систем с ролевым управлением доступом.

Понятие ролевого управления доступом.

Базовая модель ролевого управления доступом.

Модель администрирования ролевого управления доступом.

Администрирование множеств авторизованных ролей пользователей.

Администрирование множеств прав доступа, которыми обладают роли.

Администрирование иерархии ролей.

Модель мандатного ролевого управления доступом.

Защита от угрозы конфиденциальности информации.

Защита от угрозы целостности информации.

Тема 8. ДП-модели.

Базовая ролевая ДП-модель.

Состояния базовой ролевой ДП-модели.

Правила преобразования состояний базовой ролевой ДП-модели.

Условия передачи прав доступа с участием двух субъект-сессий.

Мандатная ДП-модель.

Правила преобразования состояний мандатной ДП-модели.

ДП-модель безопасности информационных потоков по времени.

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с

назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости).

В процессе осуществления образовательного процесса используются:

– для формирования текстов материалов для промежуточной и текущей аттестации – программы Microsoft Office, издательская система LaTex;

– для поиска учебной литературы библиотеки ЯрГУ – Автоматизированная библиотечная информационная система "БУКИ-NEXT" (АБИС "Буки-Next").

7. Перечень основной и дополнительной учебной литературы, необходимых для освоения дисциплины

а) основная литература

1. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий // Руководящий документ (ГОСТ Р ИСО / МЭК 15408). М.: Гостехкомиссия Россия, 2002. - Ч. 1-3.
2. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ Гостехкомиссии России, М.: ГТК РФ, 1992.
3. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Руководящий документ Гостехкомиссии России. М. ГТК РФ, 1992.
4. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. Руководящий документ Гостехкомиссии России. М.-.ГТК РФ, 1992.
5. Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.
6. Белов Е.Б. Основы информационной безопасности. Учебное пособие для вузов. / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. М.: Горячая линия - Телеком, 2006. 544 с.
7. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. / П.Н. Девянин. М.: Горячая линия - Телеком, 2012. 320 с.
8. ГОСТ 34.12-2015. Информационная технология, Криптографическая защита информации. Блочные шифры. Москва. Стандартинформ. 2015.

9. ГОСТ 34.13-2015. Информационная технология, Криптографическая защита информации. Режимы работы блочных шифров. Москва. Стандартинформ. 2015.
10. ГОСТ 34.11-2012. Информационная технология, Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Москва. Стандартинформ. 2012.
11. ГОСТ 34.10-2012. Информационная технология, Криптографическая защита информации. Функция хэширования. Москва. Стандартинформ. 2012.
12. Trusted Computer System Evaluation Criteria. - US Department of Defense, 1985. - CSC-STD-001-83.

б) дополнительная литература

1. ГОСТ Р 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
2. Насыпный В.В. Метод защиты арифметических вычислений в компьютерных системах. М.: Прометей, 1999.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999.
4. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. М.: Радио и связь, 1999.
5. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. М.: КУДИЦ-ОБРАЗ, 2003.
6. Романьков В.А. Введение в криптографию. Курс лекций / В.А. Романьков. - М.: ФОРУМ, 2012. - 240 с.
7. Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.
8. Введение в криптографию: новые математические дисциплины / под ред. В. В. Ященко, СПб., Питер, 2001, 287с.
9. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости / А.В. Черемушкин. М.: Издательский дом "Академия", 2009.
10. Чмора А. Современная прикладная криптография / А.Л. Чмора. М.: Гелиос АРВ, 2002. 256 с.
11. Хенк К.А. ван Тилборг. Основы криптологии. Профессиональное руководство и интерактивный учебник. М.: Мир, 2005. 465 с.
12. Зензин О.С. Стандарт криптографической защиты AES. Конечные поля / О.С. Зензин, М.А. Иванов. КУДИЦ-ОБРАЗ, 2003.
13. Столлингс В. Криптография и защита сетей. Принципы и практика.-- 2-е изд. М.: Гелиос АРВ, 2001.
14. Саломаа А. Криптография с открытым ключом. М: Мир, 1996.
15. Нечаев В.И. Элементы криптографии. Основы теории защиты информации. М.: Высшая школа, 1999.
16. Ноден П., Китте К. Алгебраическая алгоритмика /под ред. Л.С. Казарина. М: Мир, 1999.
17. Ростовцев А.Г. Алгебраические основы криптографии / А.Г. Ростовцев. Санкт-Петербург. НПО "Мир и семья". ООО "Интерлайн", 2000. 354 с.
18. Ростовцев А.Г. Введение в криптографию с открытым ключом / А.Г. Ростовцев, Е.Б. Маховенко. Санкт-Петербург. НПО "Мир и семья". ООО "Интерлайн", 2001. 336 с.
19. Маховенко Е.Б. Теоретическая криптография / Е.Б. Маховенко, А.Г. Ростовцев. Санкт-Петербург. АНО НПО "Профессионал". ООО "Интерлайн", 2004.
20. Коблиц Н. Курс теории чисел и криптографии / Н. Коблиц. М.: Научное издательство "ТВП", 2001. 254 с.

21. Мао В. Современная криптография. Теория и практика / В. Мао. М.: Издательский дом "Вильямс", 2005. 768 с.
22. Харин Ю.С. Математические и компьютерные основы криптологии / Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Минск: ООО "Новое знание", 2003. 382 с.
23. Шнайер Б. Прикладная криптография / Б. Шнайер. М.: Триумф, 2002. 816 с.
24. Под ред. Погорелова Б.А., Сачкова В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006.

в) ресурсы сети «Интернет»

1.Электронные каталоги НБ ЯрГУ

(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержат библиографические записи всех видов документов, составляющих фонд библиотеки, на русском и иностранных языках.

2. Личный кабинет (http://lib.uniyar.ac.ru/opac/bk_login.php) возможность получения on-line доступа к списку выданной в автоматизированном режиме литературы, просмотра и копирования электронных версий изданий сотрудников университета (учеб. и метод. пособия, тексты лекций и т.д.) Для работы в «Личном кабинете» необходимо зайти на сайт Научной библиотеки ЯрГУ с любой точки, имеющей доступ в Internet, в пункт меню *«Электронный каталог»*; пройти процедуру авторизации, выбрав вкладку *«Авторизация»*, и заполнить представленные поля информации.

3.Электронная библиотека учебных материалов ЯрГУ

(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержит более 2500 полных текстов учебных и учебно-методических материалов по основным изучаемым дисциплинам, изданных в университете. Доступ в сети университета, либо по логину/паролю.

4.Электронный архив ЯрГУ

(http://elar.uniyar.ac.ru/jspui/community-list) представляет собой коллекцию полнотекстовых электронных публикаций в области научных исследований. База данных предназначена для использования в учебных и научных целях, облегчая доступ к информации о научных работах и их содержанию.

5. Электронная картотека «Книгообеспеченность»

(http://www.lib.uniyar.ac.ru/opac/bk_bookreq_find.php)

раскрывает учебный фонд научной библиотеки ЯрГУ, предоставляет оперативную информацию о состоянии книгообеспеченности дисциплин основной и дополнительной литературой, а также цикла дисциплин и специальностей. Электронная картотека «Книгообеспеченность» доступна в сети университета и через Личный кабинет.

Русскоязычные электронные ресурсы (внешние)

1. Научная электронная библиотека (НЭБ) (http://elibrary.ru) – это крупнейший российский информационный портал, содержащий рефераты и полные тексты более 12 млн. научных статей и публикаций. **ЯрГУ выписывает в электронном виде 66 журналов,** более 2 500 наименований журналов на английском и русском языках находятся в свободном доступе. Для работы с полными текстами необходимо зарегистрироваться. Доступ к полным текстам журналов в сети университета.

2. Электронная библиотека диссертаций Российской государственной библиотеки (http://diss.rsl.ru) содержит более 580 000 полных текстов диссертаций и авторефератов. Доступ осуществляется в сети университета.

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

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:
-учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации;
-помещения для самостоятельной работы;
-помещения для хранения и профилактического обслуживания оборудования.

Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.

Автор(ы) :

Зав. кафедрой компьютерной безопасности и математических методов обработки информации, д.ф.-м.н. Дурнев В.Г.

Приложение №1 к рабочей программе дисциплины
«Математические модели для информационной безопасности»

Оценочные средства
для проведения текущей и/или промежуточной аттестации аспирантов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1.1 Список вопросов и (или) заданий для проведения промежуточной аттестации

Вопросы к зачету (2 семестр)

Тема 1. Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем.

Элементы теории компьютерной безопасности. Сущность, субъект, доступ, информационный поток.

Классификация угроз безопасности информации.

Виды информационных потоков.

Виды политик управления доступом и информационными потоками.

Утечка права доступа и нарушение безопасности КС.

Математические основы моделей безопасности. Основные понятия, автоматы, графы.

Алгоритмические проблемы: разрешимые и неразрешимые алгоритмические проблемы.

Основные виды формализованных моделей безопасности КС.

Проблема адекватности реализации модели безопасности в реальной КС.

Тема 2. Модели компьютерных систем с дискреционным управлением доступом.

Модель матрицы доступов Харрисона - Руззо - Ульмана (ХРУ, HRU). Описание модели, анализ безопасности систем ХРУ.

Алгоритмическая неразрешимость проблемы утечки для модели HRU.

Модель типизированной матрицы доступов.

Тема 3. Модель распространения прав доступа Take-Grant.

Основные положения классической модели Take-Grant.

Расширенная модель Take-Grant.

Представление систем Take-Grant системами HRU.

Дискреционные ДП-модели. Базовая ДП-модель

ДП-модели без кооперации доверенных и недоверенных субъектов.

Тема 4. Модели изолированной программной среды.

Субъектно-ориентированная модель изолированной программной среды.

Корректность субъектов в ДП-моделях КС с дискреционным управлением доступом.

ДП-модель с функционально ассоциированными с субъектами сущностями.

ДП-модель для политики безопасного администрирования.

ДП-модель для политики абсолютного разделения административных и пользовательских полномочий.

ДП-модель с функционально или параметрически ассоциированными с субъектаим сущностями.

Методы предотвращения утечки прав доступа и реализации запрещенных информационных потоков.

Метод предотвращения возможности получения права доступа владения недоверенным субъектом к доверенному субъекту.

Метод реализации политики безопасности администрирования.

Метод реализации политики абсолютного разделения административных и пользовательских полномочий.

Тема 5. Модели компьютерных систем с мандатным управлением доступом.

Модель Балла - ЛаПадулы: классическая модель Белла - ЛаПадулы, пример некорректного администрирования.

Политика low-watermark в модели Белла - ЛаПадулы.

Безопасность переходов.

Модель мандатной политики целостности информации Биба.

Модель систем военных сообщений: общие положения и основные понятия.

Неформальное и формальное описания модели СВС.

Мандатная ДП-модель.

Правила преобразования состояний мандатной ДП-модели.

Безопасность в смысле Белла - ЛаПадулы.

Тема 6. Модели безопасности информационных потоков.

Автоматная модель безопасности информационных потоков.

Программная модель контроля информационных потоков.

Вероятностная модель безопасности информационных потоков.

ДП-модель безопасности информационных потоков по времени.

Тема 7. Модели компьютерных систем с ролевым управлением доступом.

Понятие ролевого управления доступом.

Базовая модель ролевого управления доступом.

Модель администрирования ролевого управления доступом.

Администрирование множеств авторизованных ролей пользователей.

Администрирование множеств прав доступа, которыми обладают роли.

Администрирование иерархии ролей.

Модель мандатного ролевого управления доступом.

Защита от угрозы конфиденциальности информации.

Защита от угрозы целостности информации.

Тема 8. ДП-модели.

Базовая ролевая ДП-модель.

Состояния базовой ролевой ДП-модели.

Правила преобразования состояний базовой ролевой ДП-модели.

Условия передачи прав доступа с участием двух субъект-сессий.

Мандатная ДП-модель.

Правила преобразования состояний мандатной ДП-модели.

ДП-модель безопасности информационных потоков по времени.

Приложение № 2 к рабочей программе дисциплины
«Математические модели для информационной безопасности»

Методические указания для аспирантов по освоению дисциплины

В связи с тем, что по дисциплине не предусмотрены практические занятия, а лекций лишь 8 часов, основным видом работы становится самостоятельное изучение теоретического материала. По наиболее трудным темам проводятся консультации. В процессе изучения дисциплины необходима регулярная работа с рекомендованной литературой, систематическое изучение теоретического материала.

Для проверки усвоения теоретического материала в течение обучения проводятся мероприятия текущей аттестации в виде устного опроса-собеседования на лекциях и консультациях по теоретическому материалу.

Аспиранты сдают зачет во втором семестре. Зачет проводится в форме собеседования на базе списка вопросов к зачету, который охватывает полностью всю программу дисциплины.

Учебно-методическое обеспечение самостоятельной работы аспирантов по дисциплине

В качестве учебно-методического обеспечения рекомендуется использовать литературу, указанную в разделе № 7 данной рабочей программы