МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»
Факультет компьютерных наук и информационных технологий

УТВЕРЖДАЮ
Декан факультета
Миронов С. В.
«31» августа 2021 г.

Рабочая программа дисциплины
Модели безопасности компьютерных систем

Специальность
10.05.01 Компьютерная безопасность

Специализация
Математические методы защиты информации

Квалификация выпускника
Специалист по защите информации

Форма обучения
Очная

Саратов,
2021

Статус	ФИО	Подпись	Дата
Преподаватель-разработчик	Жаркова А. В.		31.08.2021 г.
Председатель НМК	Кондратова Ю. Н.		31.08.2021 г.
Заведующий кафедрой	Абросимов М. Б.		31.08.2021 г.
Специалист Учебного управления	Юшкова И. В.		31.08.2021 г.

1. Цели освоения дисциплины

Целями освоения дисциплины являются овладение основными идеями и методами математического моделирования в проблемах компьютерной безопасности; знакомство с базисными моделями компьютерной безопасности; знание основополагающих документов в области компьютерной безопасности.

2. Место дисциплины в структуре ООП

Данная учебная дисциплина относится к обязательной части Блока 1 «Дисциплины (Модули)» учебного плана ООП и направлена на формирование у обучающихся общепрофессиональных компетенций.

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения дисциплин «Алгебра», «Дискретная математика», «Математическая логика и теория алгоритмов», «Основы информационной безопасности».

Компетенции, сформированные при изучении данной дисциплины, используются при изучении дисциплин «Защита информации от утечки по техническим каналам», «Введение в криптоанализ».

3. Результаты обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	ОПК-6.1 знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	Знать основные угрозы безопасности информации и модели нарушителя компьютерных систем. Уметь разрабатывать модели угроз и модели нарушителя компьютерных систем; определить политику контроля доступа работников к информации ограниченного доступа. Владеть навыками применения отечественных и зарубежных стандартов в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы.

	ограниченного доступа; основные угрозы безопасности информации и модели нарушителя компьютерных систем; ОПК-6.2 умеет разрабатывать модели угроз и модели нарушителя компьютерных систем; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы; ОПК-6.3 владеет навыками при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	
ОПК-8. Способен применять методы научных исследований при проведении разработок в	ОПК-8.1.2 знает основные понятия и определения, используемые при описании моделей безопасности	Знать основные понятия и определения, используемые при описании моделей безопасности

области обеспечения безопасности компьютерных систем и сетей.	компьютерных систем; основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; ОПК-8.2.2 умеет разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; ОПК-8.3.2 владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.	компьютерных систем; основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков. Уметь разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками. Владеть способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.
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.	ОПК-11.1.1 знает основные понятия и определения, используемые при описании моделей безопасности компьютерных систем; основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности	Знать основные понятия и определения, используемые при описании моделей безопасности компьютерных систем; основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности

	информационных потоков; ОПК-11.2.1 умеет разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; ОПК-11.3.1 владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.	информационных потоков. Уметь разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками. Владеть способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 часов.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Лекции	Практические занятия		ИКР	СР	
					Общая трудоёмкость	Из них – практическая подготовка			
1	2	3	4	5	6	7	8	9	10
1	Основные понятия и элементы теории компьютерной	9	1-3	6	6	–	–	6	Опрос на 5-й неделе.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Лекции	Практические занятия		ИКР	СР	
					Общая трудоёмкость	Из них – практическая подготовка			
1	2	3	4	5	6	7	8	9	10
	безопасности								
2	Модели компьютерных систем с дискреционным управлением доступом		4-6	6	6	–	–	6	
3	Модели компьютерных систем с мандатным управлением доступом		7-9	6	6	–	–	6	
4	Модели безопасности информационных потоков и изолированной программной среды		10-12	6	6	–	–	6	*Контрольная работа* на 10-й неделе
5	Модели компьютерных систем с ролевым управлением доступом		13-15	6	6	–	–	6	Опрос на 16-й неделе.
6	Развитие формальных моделей безопасности		16-18	6	6	–	–	6	

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Лекции	Практические занятия		ИКР	СР	
					Общая трудоёмкость	Из них – практическая подготовка			
1	2	3	4	5	6	7	8	9	10
	компьютерных систем								
	Промежуточная аттестация								**Зачёт**
	ИТОГО - 108ч.			**36**	**36**	**–**	**–**	**36**	**–**

Содержание дисциплины

Основные понятия и элементы теории компьютерной безопасности. Сущность, субъект, доступ, право доступа, информационные потоки по памяти или по времени. Модели ценности информации: порядковая шкала, решетка многоуровневой безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров КС. Понятие политики безопасности. Политики дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков.

Модели компьютерных систем с дискреционным управлением доступом. Модель матрицы доступов Харрисона – Руззо – Ульмана (ХРУ). Алгоритмическая неразрешимость задачи проверки безопасности систем ХРУ. Модель типизированной матрицы доступов (ТМД). Монотонные системы ТМД и их каноническая форма. Ациклические монотонные ТМД и алгоритм проверки их безопасности. Классическая модель Take-Grant. Де-юре правила преобразования графов доступов. Условия передачи прав доступа в произвольном графе доступов. Расширенная модель Take-Grant. Де-факто правила преобразования графов доступов и информационных потоков. Условия реализации информационных потоков. Алгоритм построения замыкания графа доступов и информационных потоков.

Модели компьютерных систем с мандатным управлением доступом. Классическая модель Белла – ЛаПадулы. Безопасный доступ, состояние, система. Базовая теорема безопасности. Интерпретации модели Белла-ЛаПадулы: модель реализации политики low-watermark, безопасность переходов, модель мандатной политики целостности информации Биба.

Недостатки модели Белла – ЛаПадулы. Примеры реализации запрещенных информационных потоков по памяти или по времени. Неформальное и формальное описания модели систем военных сообщений. Безопасное состояние. Безопасность переходов. Потенциальная модификация сущности с источником. Смыслы безопасности функции переходов.

Модели безопасности информационных потоков и изолированной программной среды. Автоматная модель безопасности информационных потоков. Программная модель контроля информационных потоков. Контролирующий механизм защиты. Вероятностная модель безопасности информационных потоков. Информационное невлияние. Субъектно-ориентированная модель изолированной программной среды (ИПС). Объекты, функционально ассоциированные с субъектами. Мониторы безопасности обращений и порождения субъектов. Базовая теорема ИПС.

Модели компьютерных систем с ролевым управлением доступом. Описание базовой модели ролевого управления доступом. Иерархия ролей. Механизм ограничений. Модель администрирования ролевого управления доступом. Задание иерархии ролей и ограничений в соответствии с требованиями либерального или строгого мандатного управления доступом. Безопасность информационных потоков.

Развитие формальных моделей безопасности компьютерных систем. Взаимосвязь положений классических формальных моделей безопасности КС. Критический анализ классических моделей. Проблема адекватности реализации модели безопасности в реальной КС. Обзор семейства формальных моделей управления доступом и информационными потоками (ДП-моделей) КС с дискреционным, мандатным или ролевым управлением доступом. Доверенные и недоверенные субъекты. Анализ информационных потоков по памяти или по времени. Функционально или параметрически ассоциированные с субъектами сущности.

План практических занятий

На практических занятиях студенты знакомятся с основными сведениями, требуемыми для выполнения задания, выполняют практические задания.

№ занятия	Тема	Задания для решения в аудитории	Задания для домашней работы
1	**2**	**3**	**4**
1-3	Основные понятия и элементы теории компьютерной безопасности	№ 1	№ 1
4-6	Модели компьютерных систем с дискреционным управлением доступом	№ 2	№ 2
7-9	Модели компьютерных систем с мандатным управлением доступом	№ 3	№ 3
10-12	Модели безопасности информационных потоков и изолированной программной среды	№ 4	№ 4
13-15	Модели компьютерных систем с ролевым	№ 5	№ 5

№ занятия	Тема	Задания для решения в аудитории	Задания для домашней работы
1	**2**	**3**	**4**
	управлением доступом		
16-18	Развитие формальных моделей безопасности компьютерных систем	№ 6	№ 6

5. Образовательные технологии, применяемые при освоении дисциплины

Предусматривается широкое использование в учебном процессе таких образовательных технологий как проведение коллоквиумов по ключевым для приложений темам, привлечение студентов к работе в научном семинаре кафедры, к переводам текстов из зарубежных изданий по дисциплине, демонстрация работы компьютерных программ по моделированию систем безопасности, встречи со специалистами из профильных организаций и фирм.

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, сопровождение тьюторами в образовательном пространстве. При этом основной формой организации учебного процесса является интегрированное обучение лиц с ограниченными возможностями здоровья, т.е. все студенты обучаются в смешенных группах, имеют возможность постоянно общаться со сверстниками, благодаря чему легче адаптируются в социуме.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

В рамках самостоятельной работы студенты прорабатывают лекционный материал, изучают дополнительные сведения. Контроль текущей успеваемости осуществляется в процессе проведения лекционных и практических занятий.

Фонд оценочных средств дисциплины включает в себя задания для самостоятельной работы, задания для контрольной работы, контрольные вопросы, вопросы для проведения промежуточной аттестации (зачёт). Фонд оценочных средств дисциплины приведён в приложении 1.

7. Данные для учета успеваемости студентов в БАРС

Таблица 1.1 – Таблица максимальных баллов по видам учебной деятельности

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
9	18	0	20	12	0	20	30	**100**

Программа оценивания учебной деятельности студента

9 семестр

Лекции

Посещаемость, опрос, активность и др. за один семестр – от 0 до 18 баллов.

Лабораторные занятия

Не предусмотрены

Практические занятия

Контроль выполнения практических заданий, самостоятельность при выполнении работы, правильность выполнения, посещаемость в течение одного семестра – от 0 до 20 баллов.

Самостоятельная работа

Контроль выполнения заданий в рамках самостоятельной работы, проверка усвоения изученного лекционного материала в рамках опроса, конспект занятий – от 0 до 12 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Контроль выполнения *контрольной работы*, грамотность в оформлении, правильность выполнения – от 0 до 20 баллов.

Промежуточная аттестация

Промежуточная аттестация представляет собой теоретический *зачёт*, проводимый в виде собеседования в устной форме с предварительной подготовкой студента к ответу, или в письменном виде по выбору преподавателя.

При проведении промежуточной аттестации

ответ на «отлично» / «зачтено» оценивается от 24 до 30 баллов;

ответ на «хорошо» / «зачтено» оценивается от 19 до 23 баллов;

ответ на «удовлетворительно» / «зачтено» оценивается от 15 до 18 баллов;

ответ на «неудовлетворительно» / «не зачтено» оценивается от 0 до 14 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за девятый семестр по дисциплине «Модели безопасности компьютерных систем» составляет **100** баллов.

Таблица 2.1 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Модели безопасности компьютерных систем» в оценку (зачёт)

70 баллов и более	«зачтено»
меньше 70 баллов	«не зачтено»

8. Учебно-методическое и информационное обеспечение дисциплины

а) литература:

1) Богомолов, А. М. Алгебраические основы теории дискретных систем [Текст] / А. М. Богомолов, В. Н. Салий. - Москва : Наука. Физ.-мат. лит., 1997. - 367, [1] с. : ил. - Библиогр. - ISBN 5-02-015033-9 (в пер.).

2) Богульская, Н. А. Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров. — Красноярск : СФУ, 2019. — 206 с. — ISBN 978-5-7638-4008-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157578.

3) Юрин, И. Ю. Теоретические и практические основы защиты информации [Электронный ресурс] : Учебное пособие / И. Ю. Юрин. - Саратов, 2012. - 32 с. URL: http://library.sgu.ru/uch_lit/620.pdf. Загл. с экрана. Яз. рус.

б) программное обеспечение и Интернет-ресурсы:

1) Лицензионное программное обеспечение: Microsoft Office, Microsoft Windows.

2) Свободное программное обеспечение: Adobe Acrobat Reader DC.

9. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий необходима лекционная аудитория, в которой имеются учебная доска, компьютер с возможностью выхода в сеть Интернет, мультимедийный проектор с экраном с возможностью демонстрации электронной презентации.

Для проведения практических занятий необходима аудитория, в которой имеются учебная доска, компьютер с возможностью выхода в сеть Интернет, мультимедийный проектор с экраном с возможностью демонстрации электронной презентации.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.01 Компьютерная безопасность, специализация «Математические методы защиты информации» (квалификация «Специалист по защите информации»).

Автор

Доцент кафедры теоретических основ компьютерной безопасности и криптографии, кандидат физико-математических наук А. В. Жаркова

Программа одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «31» августа 2021 года, протокол № 1.