МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ
Директор института прикладной
математики и компьютерных наук
_____А.В. Замятин
«_02_» _____ 2021 г.

Модели безопасности компьютерных систем

рабочая программа дисциплины

Закреплена за кафедрой	*компьютерной безопасности*
Учебный план	*10.05.01 Компьютерная безопасность,* *профиль «Анализ безопасности компьютерных систем»*
Форма обучения	*Очная*
Общая трудоёмкость	*3 з.е.*
Часов по учебному плану	*108*
в том числе:	
аудиторная контактная работа	*69.45*
самостоятельная работа	*38.55*
Вид(ы) контроля в семестрах *экзамен/зачет/зачет с оценкой*	*Семестр 9 – зачет с оценкой*

Томск-2021

Программу составил:
канд. физ.-мат. наук
старший преподаватель кафедры
компьютерной безопасности А.С. Твардовский

Рецензент:
канд. тех. наук, доцент
Заведующий кафедрой компьютерной безопасности С.А. Останин

Рабочая программа дисциплины «Модели безопасности компьютерных систем» разработана в соответствии с образовательным стандартом высшего образования – специалитет, самостоятельно устанавливаемым федеральным государственным автономным образовательным учреждением высшего образования «Национальный исследовательский Томский государственный университет» по специальности 10.05.01 Компьютерная безопасность (Утвержден Ученым советом НИ ТГУ, протокол от 30.06.2021 г. № 06).

Рабочая программа одобрена на заседании кафедры компьютерной безопасности

Протокол от 02 июня 2021 г. № 06

Заведующий кафедрой компьютерной безопасности,
канд. техн. наук, доцент С.А. Останин

Рабочая программа одобрена на заседании учебно-методической комиссии института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 17 июня 2021 г. № 05

Председатель УМК ИПМКН,
д-р техн. наук, профессор С.П. Сущенко

Цель освоения дисциплины

Цель – изучить основные модели безопасности компьютерных систем, модели дискреционного, мандатного, ролевого управления доступом, безопасности информационных потоков и изолированной программной среды, овладеть математическим аппаратом для разработки и анализа безопасности моделей управления доступом и навыками разработки и реализации механизмов управления доступом.

1. Место дисциплины в структуре ОПОП

Дисциплина «Модели безопасности компьютерных систем» относится к обязательной части Блока 1 «Дисциплины», входит в модуль «Специализация».

Для освоения дисциплины необходимо знать основы дискретной математики и алгебры, иметь базовые представления об операционных системах и компьютерных сетях.

Пререквизиты дисциплины: Дискретная математика, Информатика, Операционные системы, Дискретная математика. Теория автоматов, Алгебра, Компьютерные сети

Постреквизиты дисциплины: Защита в операционных системах, Безопасность веб-приложений.

2. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Таблица 1.

Компетенция	**Индикатор компетенции**	**Код и наименование результатов обучения** (планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций)
ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.	ИОПК-8.3 Проводит анализ и формализацию поставленных задач, участвует в разработке математических моделей в области обеспечения безопасности компьютерных систем и сетей.	ОР-8.3.1. **Знать:** назначение и формальное описание классических моделей безопасности (ХРУ, Белла-ЛаПадулы, Take-Grant). ОР-8.3.2. **Уметь:** разрабатывать подходящую модель для обеспечения безопасности компьютерных систем и сетей. ОР-8.3.3. **Владеть:** математическим аппаратом классических моделей управления доступом.
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	ИОПК-11.1 Понимает основные формальные модели политик управления доступом и информационными потоками в компьютерных системах; ИОПК-11.2 Владеет необходимым аппаратом формального определения требований политики безопасности, построения и анализа политик управления доступом и информационными потоками в компьютерных системах; ИОПК-11.3 Формулирует политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите	ОР-11.1.1. **Знать:** основные формальные модели дискреционного, мандатного, ролевого управления доступом. ОР-11.1.2. **Знать:** основные виды политик управления доступом и информационными потоками в компьютерных системах. ОР-11.2.1. **Владеть:** аппаратом формального определения требований политики безопасности, построения и анализа политик управления доступом и информационными потоками в компьютерных системах ОР-11.2.2. **Владеть:** классическими политиками управления доступом, аппаратом их анализа и разработки. ОР-11.3.1. **Уметь:** формулировать свойства безопасности в соответствии с

	информации.	требованиями заданной политики. ОР-11.3.2. **Уметь:** разрабатывать политики безопасности компьютерных систем с учетом требований по защите информации.
ПК-2. Способен проектировать и разрабатывать средства защиты информации компьютерных систем и сетей.	ИПК-2.1 Определяет угрозы безопасности и их возможные источники, каналы утечки информации. ИПК-2.2 Разрабатывает математические модели, реализуемые в средствах защиты информации.	ОР-2.1.1. **Знать:** модели изолированной программной среды и безопасности информационных потоков. ОР-2.1.2. **Владеть:** математическим аппаратом для анализа безопасности систем управления доступом. ОР-2.2.1. **Уметь:** разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем. ОР-2.2.2. **Уметь:** разрабатывать механизмы управления доступом для современных компьютерных систем.

3. Структура и содержание дисциплины

3.1. Структура и трудоемкость видов учебной работы по дисциплине

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 часов.

Таблица 2.

Вид учебной работы	Трудоемкость в академических часах	
	9 семестр	всего
Общая трудоемкость	108	108
Контактная работа:	69,45	69,45
Лекции (Л):	32	32
Практики (ПЗ)	32	32
Лабораторные работы (ЛР)		
Семинары (СЗ)		
Групповые консультации	2	2
Индивидуальные консультации	3,2	3,2
Промежуточная аттестация	0,25	0,25
Самостоятельная работа обучающегося:	31,8	31,8
- выполнение проекта	9,9	9,9
- подготовка доклада	5	5
- изучение учебного материала,	15	15
- прохождение тестирования	1	1
Подготовка к промежуточной аттестации	6,75	6,75
Вид промежуточной аттестации (зачет, зачет с оценкой, экзамен)	**Зачет с оценкой**	**Зачет с оценкой**

3.2. Содержание и трудоемкость разделов дисциплины

Таблица 3.

Код занятия	Наименование разделов и тем и их содержание	Вид учебной работы, занятий, контроля	Семестр	Часы в электронной форме	Всего (час.)	Литература	Код (ы) результата(ов) обучения
	Раздел 1. Основные элементы и виды управления доступом		**9**		**11**	1, 2, 4, 6	ОР-11.1.1-2., ОР-8.3.1-2., ОР-11.3.1-2, ОР-2.2.1.
1.1.	Базовая терминология в области моделей контроля доступа	Лекции	9		2	1, 2, 4, 6	ОР-8.3.1., ОР-11.1.2., ОР-2.2.1.
1.2.	Дискреционная и мандатная политики	Лекции	9		2	1, 4,	ОР-11.1.1., ОР-8.3.2., ОР-11.3.1-2
1.3.	Решение задач по теме	Практики	9		5	1, 2, 4, 6	ОР-11.1.1-2., ОР-8.3.1-2., ОР-11.3.1-2, ОР-2.2.1.
1.4.	Изучение учебного материала	СРС	9		4	1, 2, 4, 6	ОР-11.1.1-2., ОР-8.3.1-2., ОР-11.3.1-2, ОР-2.2.1.
	Раздел 2. Ролевая модель		**9**		**13**	1, 2, 4	ОР-11.1.1., ОР-11.2.2., ОР-2.1.2., ОР-11.3.1-2., ОР-2.2.2.
2.1.	Базовая ролевая модель контроля доступа	Лекции	9		2	1, 2, 4	ОР-11.1.1., ОР-11.2.2., ОР-2.1.2.
2.2.	Механизмы ограничений в ролевых моделях	Лекции	9		2	1, 4	ОР-11.1.1., ОР-11.3.1-2
2.3.	Решение задач по теме	Практики	9		5	1, 2, 4	ОР-11.1.1., ОР-11.2.2., ОР-2.1.2., ОР-11.3.1-2
2.4.	Изучение учебного материала	СРС	9		2	1, 2, 4	ОР-11.1.1., ОР-11.2.2., ОР-2.1.2., ОР-11.3.1-2
2.5.	Выполнение проекта	СРС	9		2	2, 4	ОР-8.3.2., ОР-11.3.1-2, ОР-2.2.2.
	Раздел 3. Take-Grant модель		**9**		**13**	1, 2, 4	ОР-8.3.1., ОР-

							11.1.2., ОР-11.2.1., ОР-8.3.3., ОР-2.1.2., ОР-2.2.2.
3.1.	Базовая Take-Grant модель	Лекции	9		2	1, 2, 4	ОР-8.3.1., ОР-8.3.3., ОР-2.1.2.
3.2.	Расширенная Take-Grant модель	Лекции	9		2	1, 4	ОР-8.3.1., ОР-11.1.2., ОР-11.2.1.
3.3.	Решение задач по теме	Практики	9		5	1, 2, 4	ОР-8.3.1., ОР-11.1.2., ОР-11.2.1., ОР-8.3.3., ОР-2.1.2.
3.4.	Изучение учебного материала	СРС	9		2	1, 2, 4	ОР-8.3.1., ОР-11.1.2., ОР-11.2.1., ОР-8.3.3., ОР-2.1.2.
3.5.	Выполнение проекта	СРС	9		2	2, 4	ОР-8.3.2., ОР-11.3.1-2, ОР-2.2.2.
	Раздел 4. Модель изолированной программной среды и основы ДП моделей		**9**		13	1, 5	ОР-2.1-2.1., ОР-11.1.2., ОР-11.2.1.
4.1.	Модель изолированной программной среды	Лекции	9		2	1	ОР-2.1.1., ОР-2.2.1.
4.2.	Основы ДП моделей	Лекции	9		4	1, 5	ОР-2.1.1., ОР-11.1.2., ОР-11.2.1.
4.3.	Решение задач по теме	Практики	9		5	1, 5	ОР-2.1-2.1., ОР-11.1.2., ОР-11.2.1.
4.4.	Изучение учебного материала	СРС	9		4	1, 5	ОР-2.1-2.1., ОР-11.1.2., ОР-11.2.1.
	Раздел 5. Модели Белла-ЛаПадулы и Биба		9		15	1, 2, 4	ОР-8.3.1., ОР-8.3.3., ОР-11.3.1-2, ОР-11.1.2., ОР-11.2.1., ОР-2.1.2., ОР-2.2.2.
5.1.	Модель Белла-ЛаПадулы	Лекции	9		2	1, 2, 4	ОР-8.3.1., ОР-8.3.3., ОР-11.3.1-2
5.2.	Модель Low-Watermark	Лекции	9		2	1, 4	ОР-11.1.2., ОР-11.2.1., ОР-2.1.2.
5.3.	Модель целостности Биба	Лекции	9		2	1, 4	ОР-11.1.2., ОР-11.2.1., ОР-2.1.2.

5.4.	Решение задач по теме	Практики	9		5	1, 2, 4	ОР-8.3.1., ОР-8.3.3., ОР-11.3.1-2, ОР-11.1.2., ОР-11.2.1., ОР-2.1.2.
5.5.	Изучение учебного материала	СРС	9		2	1, 2, 4	ОР-8.3.1., ОР-8.3.3., ОР-11.3.1-2, ОР-11.1.2., ОР-11.2.1., ОР-2.1.2.
5.6.	Выполнение проекта	СРС	9		2	2, 4	ОР-8.3.2., ОР-11.3.1-2, ОР-2.2.2.
	Раздел 6. Разработка механизмов управления доступом для современных компьютерным систем		9		24,05	1, 2, 3, 4, 5, 6, 7	ОР-11.1.1., ОР-8.3.2., ОР-11.2.2., ОР-2.2.2.
6.1.	Списки доступа	Лекции	9		2	1, 2, 3, 7	ОР-11.1.1., ОР-8.3.2., ОР-11.2.2.
6.2.	Решётки как механизм контроля доступа	Лекции	9		2	1, 2, 3, 7	ОР-11.1.1., ОР-8.3.2., ОР-11.2.2.
6.3.	Разграничение доступа на основе атрибутов	Лекции	9		4	3, 4, 7	ОР-8.3.2., ОР-11.2.2.
6.4.	Решение задач по теме	Практики	9		7	1, 2, 3, 4, 5, 6, 7	ОР-11.1.1., ОР-8.3.2., ОР-11.2.2.
6.5.	Изучение учебного материала	СРС	9		1	1, 2, 3, 4, 7	ОР-11.1.1., ОР-8.3.2., ОР-11.2.2.
6.6.	Выполнение проекта	СРС	9		3,8	2, 4	ОР-8.3.2., ОР-11.3.1-2, ОР-2.2.2.
6.7.	Подготовка доклада	СРС	9		5	1, 2, 3, 4, 5, 6, 7	ОР-8.3.1-3., ОР-11.1-3.1-2, ОР-2.1-2.1-2.
6.8.	Прохождение тестирования	СРС	9		1	1, 2, 3, 4, 5, 6, 7	ОР-8.3.1-3., ОР-11.1-3.1-2, ОР-2.1-2.1-2.
	Подготовка к промежуточной аттестации в форме зачета с оценкой	СРС	**9**		**6,75**		ОР-8.3.1-3., ОР-11.1-3.1-2, ОР-2.1-2.1-2.
	Прохождение промежуточной аттестации в форме зачета с оценкой	Э	**9**		**2,25**		ОР-8.3.1-3., ОР-11.1-3.1-2, ОР-2.1-2.1-2.

4. Образовательные технологии, учебно-методическое и информационное обеспечение для освоения дисциплины

Основой освоения материала является курс лекций, для закрепления материалов которого проводятся практические занятия. Для проверки усвоения материала используется тестирование в системе Moodle. Для расширения кругозора по теме и разбора примеров использования изученных моделей обучающиеся выступают с докладами. Выполнение группового проекта позволяет освоить и опробовать на практике полученные знания.

Самостоятельная работа студентов при изучении дисциплины (модуля) предусмотрена в следующих видах и формах:

- изучение теоретического материала на основе курса лекций, предложенной литературы и учебно-методического обеспечения;
- прохождение теста в системе moodle;
- подготовка доклада
- выполнение группового проекта.

Промежуточная аттестация осуществляется на основе зачёта с оценкой.

Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций, и методические материалы, определяющие процедуры оценивания результатов обучения, приведены в Приложении 1 к рабочей программе «Фонд оценочных средств».

4.1. Рекомендуемая литература и учебно-методическое обеспечение

№ п/п	Авторы / составители	Заглавие	Издательство	Год издания, количество страниц
Основная литература				
1.	Девянин, П. Н.	Модели безопасности компьютерных систем. Управление доступом и информационными потоками: Учебное пособие для вузов	Москва : Гор. линия-Телеком	2012. – 320 с.
2.	Щербаков А.Ю.	Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие	М.: Книжный мир	2009. – 352 с.
3.	Bishop, M.	Computer security	Art and science	2002. – 1084 р.
4.	Гайдамакин Н.А.	Теоретические основы компьютерной безопасности. Учебное пособие	Екатеринбург: изд-во Урал. Ун-та	2008. – 212 с.
Дополнительная литература				
5.	Девянин П. Н.	Анализ безопасности управления доступом и информационными потоками в компьютерных системах.	М.: Радио и связь	2006. – 176 с.
6.	Богульская Н.	Модели безопасности компьютерных систем : Учебное пособие	Красноярск : Сибирский федеральный университет	2019. - 206 с.

7.	Бондарев В. В.	Введение в информационную безопасность автоматизированных систем : учебное пособие	Москва : Издательство МГТУ им. Н. Э. Баумана	2021. - 250 с.

4.2. Базы данных и информационно-справочные системы, в том числе зарубежные

1. Электронная библиотека (репозиторий) ТГУ [Электронный ресурс] / Электронная библиотека (репозиторий) ТГУ : [сайт]. – [Томск, 2011–2016]. – URL: http://vital.lib.tsu.ru/vital/access/manager/Index.
2. Владимир Кочетков. Философия Application Security. – URL: https://www.youtube.com/watch?v=mb7tcT-9VXk
3. Maarten Decat. Access Control. – URL: https://www.youtube.com/watch?v=7e0fMbnovMc
4. George Danezis. Access Control. – URL: https://www.youtube.com/watch?v=QaS_UBuPVWA
5. Колегов Д.Н. Моделирование безопасности управления доступом и информационными потоками на основе ДП-моделей. – URL: https://vimeo.com/97906604

4.3. Перечень лицензионного и программного обеспечения

Программное обеспечение для показа презентаций с лекциями и докладами обучающихся (напр. Adobe Acrobat Reader или Microsoft PowerPoint или их аналоги). Проекты выполняются студентами с использованием свободно-распространяемого программного обеспечения.

4.4. Оборудование и технические средства обучения

Для реализации дисциплины необходимы лекционные аудитории и аудитории для проведения практических занятий. Проектор требуются для демонстрации материала в рамках изучаемых разделов, проведения защиты проектов в конце семестра и представления докладов.

5. Методические указания обучающимся по освоению дисциплины

Для усвоения теоретического материала рекомендуется посещать лекционные занятия и участвовать в решении задач на практических занятиях. В случае возникновения трудностей рекомендуется обратиться к источникам [1, 4], содержащие комплексную информацию по материалам курса. Там же можно ознакомиться с разбором решения типовых задач. Для совместной работы над групповым проектом рекомендуется использовать соответствующие информационные технологии (например, discord, github и их аналоги).

6. Преподавательский состав, реализующий дисциплину

Твардовский Александр Сергеевич, канд. физ.-мат. наук, старший преподаватель кафедры компьютерной безопасности.

6. **Язык преподавания –** русский язык.