

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Б1.В.ДВ.04.02
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Моделирование процессов и средств защиты информации
(наименование дисциплины)

по направлению подготовки
09.03.03 Прикладная информатика
направленность (профиль)
Прикладная информатика в информационной безопасности

Форма обучения: очная

Год набора: 2023

Общая трудоемкость: 5 ЗЕ

Распределение часов дисциплины по семестрам

Семестр	8	Итого
Форма контроля	зачет	
Вид занятий		
Лекции	12	12
Лабораторные	-	-
Практические	48	48
Руководство: курсовые работы (проекты) / РГР	-	-
Промежуточная аттестация	0.25	0.25
Контактная работа	60,25	60,25
Самостоятельная работа	119,75	119,75
Контроль	-	-
Итого	180	180

Рабочую программу составил(и):

Власов Игорь Анатольевич

(должность, ученое звание, степень, Фамилия И.О.)

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:



Отсутствует



Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана направления подготовки (специальности) 09.03.03 Прикладная информатика.

Срок действия рабочей программы дисциплины до 31.08.2027

УТВЕРЖДЕНО

На заседании института инженерной и экологической безопасности
(протокол заседания № 2 от 05.09.2022).

1. Цель освоения дисциплины

Дисциплина «Моделирование процессов и систем защиты информации» относится к группе дисциплин вариативной части образовательной программы. Дисциплина изучается на 3 курсе в 6 семестре.

Целью освоения дисциплины является теоретическая и практическая подготовка студентов по применению методов моделирования и проектирования систем защиты информации.

В процессе освоения дисциплины студент должен научиться выполнять математическое моделирование объектов и процессов по типовым методикам, в том числе с использованием стандартных пакетов прикладных программ.

2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина:

- Международные и российские нормативные акты, и стандарты по информационной безопасности
- Основы управления информационной безопасностью

Полученные знания используются при изучении следующих дисциплин:

- Техническая защита информации
- Программно-аппаратные средства защиты информации

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
ПК-10 Способен осуществлять моделирование решений по реализации программного обеспечения и управлению БД	ПК-10.10 Использует знания математического и имитационного моделирования систем защиты информации	<p>Знает Математическое и имитационное моделирование систем защиты информации</p> <p>Умеет применять модели процессов в информационном обмене в системах защиты информации, модели процессов сохранения конфиденциальности информации</p> <p>Владеет алгоритмами создания системы комплексной защиты, методологией разработки моделей, инструментарием имитационного моделирования</p>

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
	ПК-10.11 Умеет применять модели процессов в информационном обмене в системах защиты информации	Знает: Математическое и имитационное моделирование систем защиты информации
		Умеет: - разрабатывать модели управления рисками информационной безопасности
		Владет: - навыками построения имитационной модели
	ПК-10.12 Владет алгоритмами создания системы комплексной защиты, методологией разработки моделей	Знает: - алгоритм создания системы комплексной защиты, методологию разработки моделей
		Умеет: - разрабатывать ролевую матрицу доступа
		Владет: - инструментарием имитационного моделирования

4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Модуль 1	Лек	Тема 1 Основные понятия теории моделирования. Математическое и имитационное моделирование систем защиты информации Понятие модели, моделирования, адекватности модели. Цели и задачи моделирования. Процесс моделирования. Типы классификации моделей. Материальные (физические) и идеальные модели. Когнитивные, содержательные, концептуальные, формальные модели. Компьютерные модели. Методы моделирования случайных величин. Задачи имитационного моделирования. Области применения моделей. Этапы построения моделей. Преимущества и недостатки имитационного моделирования. Применение линейных регрессионных моделей эксперимента с помощью компьютерного моделирования.	8	2		-	
Модуль 1	Пр	Тема 1 Основные понятия теории моделирования. Математическое и имитационное моделирование систем защиты информации Моделирование реальных ситуаций, которые могут быть исследованы с помощью дискретно-событийных моделей	8	4			Отчет по практическому занятию №1
Модуль 1	Пр	Тема 1 Основные понятия теории моделирования. Математическое и имитационное	8	4			Отчет по практическому занятию №2

		моделирование систем защиты информации Создание ЕРС-моделей. Построение моделей.					
Модуль 1 Тема 1 Основные понятия теории моделирования. Математическое и имитационное моделирование систем защиты информации	Ср	Тема 1 Основные понятия теории моделирования. Математическое и имитационное моделирование систем защиты информации	8	20			
Модуль 1	Лек	Тема 2 Алгоритм создания системы комплексной защиты. Методология разработки моделей. Алгоритм создания системы комплексной защиты. Методология разработки моделей. Функции моделирования информационного обмена. Способ перехода от математической модели процесса к цифровой модели: нормировка параметров модели. Модель защиты информации	8	2			
Модуль 1	Пр	Тема 2 Алгоритм создания системы комплексной защиты. Методология разработки моделей. Разработка модели системы защиты информации	8	4			Отчет по практическому занятию №3
Модуль 1 .	Пр	Тема 2 Алгоритм создания системы комплексной защиты. Методология разработки моделей. Разработка модели архитектуры информационной системы	8	4			Отчет по практическому занятию №4
Модуль 1	Пр	Тема 2 Алгоритм создания системы комплексной защиты. Методология разработки моделей. Идентификация и оценка рисков	8	4			Отчет по практическому занятию №5
Модуль 1	Ср	Тема 2 Алгоритм создания системы комплексной защиты. Методология разработки моделей.	8	20			
Модуль 1	Лек	Тема 3. Модели процессов в информационном обмене в системах защиты информации. Моделирование процессов защиты информации. Разработка модели управления рисками информационной	8	2		-	

		безопасности. Модель процессов контроля информации. Модель процессов воздействия компьютерных вирусов. Модель действий инсайдера.					
Модуль 1	Пр	Тема 3. Модели процессов в информационном обмене в системах защиты информации. Обоснование рискованных решений методом «дерева решений»	8	4			Отчет по практическому занятию №6
Модуль 1	Пр	Тема 3. Модели процессов в информационном обмене в системах защиты информации. Разработка модели адаптивной системы информационной безопасности, действий инсайдера	8	4			Отчет по практическому занятию №7
	Ср	Тема 3. Модели процессов в информационном обмене в системах защиты информации.	8	20			
Модуль 1	Лек	Тема 4 Модель процессов сохранения конфиденциальности информации. Модель синтеза рационального проекта системы защиты информации. Модель процессов сохранения конфиденциальности информации. Модель процессов сохранения целостности информации. Модель процессов сохранения доступности информации. Модель процессов сохранения неотказуемости. Модель синтеза рационального проекта системы защиты информации.	8	2		-	
Модуль 1	Пр	Тема 4 Модель процессов сохранения конфиденциальности информации. Модель синтеза рационального проекта системы защиты информации. Разработка модели злоумышленника	8	4			Отчет по практическому занятию №8
Модуль 1	Пр	Тема 4 Модель процессов сохранения конфиденциальности информации. Модель синтеза рационального проекта системы защиты информации. Анализ рисков информационной безопасности на основе модели угроз и уязвимостей	8	4			Отчет по практическому занятию №9
Модуль 1	Пр	Тема 4 Модель процессов сохранения	8	4			Отчет по практическому

		конфиденциальности информации. Модель синтеза рационального проекта системы защиты информации. Моделирование инженерно-технической системы защиты информации по исходным данным для объекта информатизации					занятию №10
Модуль 1	Ср	Тема 4 Модель процессов сохранения конфиденциальности информации. Модель синтеза рационального проекта системы защиты информации.	8	20			
Модуль 1	Лек	Тема 5 Инструментарии имитационного моделирования Система моделирования GPSS. Система имитационного моделирования Arena. Методика построения моделей с помощью системы Arena. Создание VACD-модели.	8	2			
Модуль 1	Пр	Тема 5 Инструментарии имитационного моделирования Разработка моделей в продукте Arena 7.0 по составленным ранее EPC-диаграммам	8	4			Отчет по практическому занятию №11
Модуль 1	Ср	Тема 5 Инструментарии имитационного моделирования	8	20			
Модуль 1	Лек	Тема 6 Модели безопасности компьютерных систем Модели безопасности на основе дискретной политики. Модели на основе матрицы доступа. Модели распространения прав доступа. Модель Харисона-Руззо-Ульмана. Модель типизованной матрицы доступа. Модели безопасности на основе мандатной политики. Модели безопасности на основе тематической политики. Модели безопасности на основе ролевой политики.	8	2			
Модуль 1 Тема 6 Модели безопасности	Пр	Тема 6 Модели безопасности компьютерных систем Разработка ролевой матрицы доступа	8	4			Отчет по практическому занятию №12

компьютерных систем							
Модуль 1 Тема 6 Модели безопасности компьютерных систем	Ср	Тема 6 Модели безопасности компьютерных систем	8	19,75			
	ПА	Сдача зачета (итоговый тест/сдача зачета устно (письменно))	8	0,25		-	Банк тестовых заданий /Вопросы к зачету
Итого:				180			

5. Образовательные технологии

Технология	Формы обучения	Методы обучения
Технология традиционного обучения – организация учебного процесса в вузе, основанная на лекционно-семинарско-зачетной формах обучения	Лекция. Практическое занятие. Самостоятельная работа. Индивидуальное домашнее задание.	Наглядные, словесные, практические.
Технология модульного обучения – организация учебного процесса для полного овладения содержанием образовательных программ на основе независимых учебных модулей с учетом индивидуальных интересов и возможностей субъектов образовательного процесса.	Лекция-консультация. Семинар с использованием метода анализа конкретных ситуаций.	Решение ситуационных задач. Презентационный метод. Самостоятельная работа. Консультация. Индивидуальная работа.
Информационные технологии – специальные способы, программные и технические средства (кино, аудио – и видеосредства, компьютеры) для работы с информацией	Лекция-пресс-конференция. Визуальная лекция.	Презентационный метод.
Формы и методы обучения		
Дистанционное обучение	Сетевая технология – изучение курса (учебной дисциплины) посредством электронных учебно-методических материалов, размещенных в обучающей среде с использованием компьютера, подключенного к сети Интернет. CD-технология – изучение курса (учебной дисциплины), представленного студенту в виде автономной электронной обучающей системы и электронной версии учебно-методических материалов на CD-диске.	

6. Методические указания по освоению дисциплины

6.1. Рекомендации по освоению лекционного материала, подготовке к лекциям

Лекции являются одним из основных видов учебных занятий в высшем учебном заведении. В ходе лекционного курса проводится изложение современных научных материалов в систематизированном виде, а также разъяснение наиболее трудных вопросов учебной дисциплины. При изучении дисциплины следует помнить, что лекционные занятия являются направляющими в большом объеме научного материала. Большую часть знаний студент должен набирать самостоятельно из учебников и научной литературы. Конспекты лекций рекомендуется использовать при подготовке к лабораторным занятиям, экзамену, контрольным тестам, при выполнении самостоятельных заданий.

6.2. Рекомендации по организации самостоятельной работы

Самостоятельная работа включает изучение литературы, поиск информации в сети Интернет, подготовку к тестам, экзамену. Необходимо разобраться в основных понятиях. Записать возникшие вопросы и найти ответы на них на занятиях, либо

разобрать их с преподавателем. Подготовку к экзамену необходимо начинать заранее. Следует проанализировать научный и методический материал учебников, учебно-методических пособий, конспекты лекций. Знать формулировки терминов и уметь их четко воспроизводить.

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
8	ПК-10	Протоколы практических заданий №1-12
		Вопросы к зачету №№1-45

7.2. Типовые задания или иные материалы, необходимые для текущего контроля

7.2.3. Выполнение практических заданий

Темы Практических заданий

№	Тема
1	Моделирование реальных ситуаций, которые могут быть исследованы с помощью дискретно-событийных моделей
2	Создание EPC-моделей. Построение моделей.
3	Разработка модели системы защиты информации
4	Разработка модели архитектуры информационной системы
5	Идентификация и оценка рисков
6	Обоснование рискованных решений методом «дерева решений»
7	Разработка модели адаптивной системы информационной безопасности, действий инсайдера
8	Разработка модели злоумышленника
9	Анализ рисков информационной безопасности на основе модели угроз и уязвимостей
10	Моделирование инженерно-технической системы защиты информации по исходным данным для объекта информатизации
11	Разработка моделей в продукте Arena 7.0 по составленным ранее EPC-диаграммам
12	Разработка ролевой матрицы доступа

Типовой(ые) пример(ы) задания(ий)

При выполнении практических заданий студенты используют полученные теоретические знания при разработке процессов защиты информации, создают ERP модели, моделируют риски и нарушителей, инсайдеров, анализируют риски на основе модели угроз, разрабатывают ролевую матрицу доступа.

Краткое описание и регламент выполнения

1. Изучить теоретический материал и нормативно-правовую базу.
2. Оформить отчет о практической работе в соответствии с требованиями к оформлению практических работ в соответствии с тематикой задания.

Критерии оценки:

- оценка «зачтено» выставляется студенту, если практическое задание выполнено грамотно или имеет несущественные замечания, выполнен отчет по работе.
- оценка «не зачтено» выставляется студенту, если практическое задание не выполнено, имеет грубые ошибки, не подготовлен отчет.

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

Семестр 8

№ п/п	Вопросы к зачету
1.	Основы теории моделирования
2.	Основные термины и определения. Классификация методов моделирования.
3.	Принципы системного подхода в моделировании
4.	Виды показателей эффективности
5.	Выбор уровня описания системы в модели. Методология разработки моделей. Алгоритм создания системы комплексной защиты
6.	Системный подход к управлению защитой информации. Системные принципы создания комплексной защиты информации
7.	Методы теории игр в информационной безопасности
8.	Моделирование по событиям. Моделирование параллельных процессов
9.	Вероятностная модель системы контроля доступа к информации
10.	Разработка модели управления рисками информационной безопасности
11.	Разработка модели действий инсайдера
12.	Методы определения важности требований к процессам и системам защиты информации
13.	Разработка моделей защиты информации
14.	Стратегическое планирование имитационного экспериментов
15.	Методы оценки адекватности, устойчивости, чувствительности модели
16.	Модель адаптивной системы информационной безопасности
17.	Выбор уровня описания системы в модели. Этапы моделирования
18.	Модель формирования множества функций защиты информации
19.	Моделирование по событиям. Моделирование параллельных процессов
20.	Модели выбора рационального варианта средства защиты информации на основе экспертной информации
21.	Оценка качества имитационной модели. Методы оценки адекватности
22.	Виды показателей эффективности моделей
23.	Методы определения важности требований, предъявляемых к системе защиты информации

24.	Алгоритм создания системы комплексной защиты
25.	Функции моделирования информационного обмена
26.	Определение динамических диапазонов модулируемых процессов
27.	Модель представления информации с учетом надежности программно-аппаратных средств
28.	Модель процессов контроля информации
29.	Модель процессов воздействия компьютерных вирусов
30.	Разработка модели действий инсайдера
31.	Модель процессов сохранения конфиденциальности информации
32.	Модель процессов сохранения целостности информации
33.	Модель процессов сохранения доступности информации
34.	Модель процессов сохранения неотказуемости
35.	Модель синтеза рационального проекта системы защиты информации
36.	Модель адаптивной системы информационной безопасности
37.	Язык GPSS как средство построения моделей
38.	Приемы создания VACD-модели
39.	Модели безопасности на основе дискретной политики
40.	Как создать ролевую матрицу доступа?
41.	Мероприятия по созданию матрицы доступа
42.	Модели безопасности на основе ролевой политики
43.	Модели распространения прав доступа
44.	Методика построения моделей с помощью системы Arena
45.	Моделирование для имитации атак, принципы, цель, способы реализации

Семестр 8

7.3.2. Критерии и нормы оценки

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
		«зачтено»	55-100 баллов
8	Зачет (письменно/по накопительному рейтингу)	«не зачтено»	0-54 баллов

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Лисяк В.В.	Моделирование информационных систем	учебное пособие	2020	
2	Котлинский С.В.	Разработка моделей предметной области автоматизации	учебное пособие	2021	https://reader.lanbook.com/book/183204#1

8.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Душин В.К.	Теоретические основы информационных процессов и систем	учебное пособие	2019	URL: http://biblioclub.ru/index.php?page=book&id=573118
2	Антонов В.Ф	Методы и средства проектирования информационных систем	учебное пособие	2019	URL: http://biblioclub.ru/index.php?page=book&id=45866

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
					3

8.3. Перечень профессиональных баз данных и информационных справочных систем

1. Информационная безопасность. Защита информации

Адрес ресурса: <http://all-ib.ru/>

2. CNEWS безопасность

Адрес ресурса: <https://safe.cnews.ru/>

3. ISO27000.RU (ЗАЩИТА-ИНФОРМАЦИИ.SU)

Адрес ресурса: <http://www.iso27000.ru/>

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Windows	Windows (Договор № 690 от 19.05.2015г., срок действия - бессрочно);
2	OfficeStandart	OfficeStandart (Договор № 690 от 19.05.2015г., срок действия - бессрочно; Договор № 727 от 20.07.2016г., срок действия - бессрочно)
3.	Консультант+	Консультант+ (Договор №1522 от 25.12.2015, срок действия - бессрочно)

8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
1	Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации Э-705	Стол преподавательский, экран телевизионный, роутер, стойка для телевизора, веб. камера, транспарант-перетяжка, ширма, наушники, компьютер с выходом в Интернет.
2	"Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и	Столы ученические., стол преподавательский, стулья, доска (маркерная), кафедра напольная, ПК , телевизор.

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
	индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. УЛК -310	
3	Помещение для самостоятельной работы обучающихся Г-401	Стол, стулья, компьютеры
4	Помещение для самостоятельной работы обучающихся Д -409	Стол-парта двухместная, стулья, стол преподавательский-, стул преподавательский, передвижная доска, экран, процессор, проектор, компьютерные столы, компьютеры для студентов с выходом в сеть интернет, компьютер преподавателя, сетевой шкаф