МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБРНАУКИ РОССИИ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ДонГТУ»)

Факультет информационных технологий и автоматизации производственных процессов

Кафедра интеллектуальных систем и информационной безопасности

УТВЕРЖДАЮ
И.о.проректора
по учебной работе
_____Д.В. Мулов

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Контроль и тестирование программно-аппаратных систем
(наименование дисциплины)

10.05.03 Информационная безопасность автоматизированных систем
(код, наименование специальности)

Безопасность открытых информационных систем
(специализация)

Квалификация специалист по защите информации
(бакалавр/специалист/магистр)

Форма обучения очная
(очная, очно-заочная, заочная)

Алчевск, 2024

1 Цели и задачи изучения дисциплины

Цели дисциплины. Целью изучения дисциплины «Контроль и тестирование программно-аппаратных систем» является освоение технологий цифровых двойников, как систем комплексного многопараметрического моделирования различных продуктов, производственных процессов и систем, а также получение навыков практического использование результатов моделирования.

Задачи изучения дисциплины:

– формирование навыков моделирования продуктов, производственных процессов и систем;

– приобретение знаний: о цифровых двойниках и принципах их практического применения и о различных видах моделирования, используемых при построении цифровых двойников;

– приобретение умений построения различных видов моделирования, используемых при построении цифровых двойников.

Дисциплина направлена на формирование профессиональной (ПК-1) компетенции выпускника.

2 Место дисциплины в структуре образовательной программы

Логико-структурный анализ дисциплины – курс входит обязательную часть БЛОКА 1 «Дисциплины (модули)» подготовки студентов по специальности 10.05.03 Информационная безопасность автоматизированных систем (Безопасность открытых информационных систем).

Дисциплина реализуется кафедрой интеллектуальных систем и информационной безопасности. Основывается на базе дисциплин из цикла подготовки бакалавров и специалистов.

Основывается на базе дисциплин: «Информатика», «Языки программирования», «Основы информационной безопасности», «Программирование микроконтроллеров».

Является основой для изучения следующих дисциплин: «Криптографические методы защиты информации», «Управление информационной безопасностью», «Подготовка и выполнение выпускной квалификационной работы».

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения профессиональных задач деятельности.

Курс является фундаментом для ориентации студентов в сфере научных исследований.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 ак.ч. Программой дисциплины предусмотрены лекционные (18 ч.), лабораторные (36 ч.) занятия и самостоятельная работа студента (54 ч.).

Дисциплина изучается на 5 курсе в 9 семестре. Форма промежуточной аттестации – зачет.

3 Перечень результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины «Контроль и тестирование программно-аппаратных систем» направлен на формирование компетенции, представленной в таблице 1.

Таблица 1 –Компетенции, обязательные к освоению

Содержание компетенции	Код компетенции	Код и наименование индикатора достижения компетенции
Способен разрабатывать системы защиты информации автоматизированных систем	ПК-1	ПК-1.2 Выполняет проектирование и реализацию системы защиты информации автоматизированных систем

4 Объём и виды занятий по дисциплине

Общая трудоёмкость учебной дисциплины составляет 3 зачётных единиц, 108 ак.ч.

Самостоятельная работа студента (СРС) включает проработку материалов лекций, подготовку к лабораторным занятиям, текущему контролю, выполнение индивидуального задания, самостоятельное изучение материала и подготовку к зачету.

При организации внеаудиторной самостоятельной работы по данной дисциплине используются формы и распределение бюджета времени на СРС для очной формы обучения в соответствии с таблицей 2.

Таблица 2 – Распределение бюджета времени на СРС

Вид учебной работы	Всего ак.ч.	Ак.ч. по семестрам
		9
Аудиторная работа, в том числе:	54	54
Лекции (Л)	18	18
Практические занятия (ПЗ)	–	–
Лабораторные работы (ЛР)	36	36
Курсовая работа/курсовой проект	-	-
Самостоятельная работа студентов (СРС), в том числе:	54	54
Подготовка к лекциям	4	4
Подготовка к лабораторным работам	18	18
Подготовка к практическим занятиям / семинарам	–	–
Выполнение курсовой работы / проекта	-	-
Расчетно-графическая работа (РГР)	-	-
Реферат (индивидуальное задание)	–	–
Домашнее задание	–	–
Подготовка к контрольным работам	-	-
Подготовка к коллоквиуму	-	-
Аналитический информационный поиск	13	13
Работа в библиотеке	13	13
Подготовка к зачету (З)	6	6
Промежуточная аттестация – зачету (З)	З	З
Общая трудоемкость дисциплины		
ак.ч.	108	108
з.е.	3	3

5 Содержание дисциплины

С целью освоения компетенции, приведенной в п.3 дисциплина разбита на 2 темы:

– тема 1 (Программно-аппаратные комплексы реального времени);

– тема 2 (Тестирование программно-аппаратных средств защиты информации).

Виды занятий по дисциплине и распределение аудиторных часов для очной формы приведены в таблице 3.

Таблица 3 – Виды занятий по дисциплине и распределение аудиторных часов (очная форма обучения)

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционных занятий	Трудоемкость в ак.ч.	Темы практических занятий	Трудоемкость в ак.ч.	Тема лабораторных занятий	Трудоемкость в ак.ч.
1	2	3	4	5	6	7	8
1	Программно-аппаратные комплексы защиты информации реального времени	Основные понятия. Задачи диагностирования в реальном масштабе времени. Особенности разработки программного обеспечения защиты информации в автоматизированных системах реального времени	2	–	–	–	–
2	Тестирование программно-аппаратных средств защиты информации	Основные понятия. Тестирование в разработке ПО, поддержке, управлении. Принципы тестирования. Особенности тестирования систем реального времени. Тестирование на проникновение. Планирование и контроль. Политика тестирования. Стратегия тестирования. Анализ и проектирование тестов. Реализация и выполнение тестов. Проверка выходных критериев и отчеты.	4 4	–	–	Формирование задания к тестированию Выполнение статического тестирования программного проекта Оценка метрик ПО Разработка через тестирование	4 6 6 6

Завершение таблицы 3

1	2	3	4	5	6	7	8
2	Тестирование программно-аппаратных средств защиты информации	Тестирование компонентов. тестирование. Системное тестирование. Приемочное тестирование. Типы тестирования и цели тестирования. Функциональное тестирование. Нефункциональное тестирование. Структурное тестирование. Процесс разработки тестов. проектирования тестов. Методы черного ящика. Эквивалентное разбиение. Методы белого ящика. Потоковый граф. Цикломатическая сложность. Тестирование базового пути. Тестирование условий.	4 4	–	–	Тестирование на проникновение Автоматизированное интеграционное тестирование	6 8
Всего аудиторных часов			18	-		36	

6 Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине

6.1 Критерии оценивания

В соответствии с Положением о кредитно-модульной системе организации образовательного процесса ФГБОУ ВО «ДонГТУ» (https://www.dstu.education/images/structure/license_certificate/polog_kred_modul.pdf) при оценивании сформированности компетенций по дисциплине используется 100-балльная шкала.

Перечень компетенций по дисциплине и способы оценивания знаний приведены в таблице 4.

Таблица 4 – Перечень компетенций по дисциплине и способы оценивания знаний

Код и наименование компетенции	Способ оценивания	Оценочное средство
ПК-1	зачет	Комплект контролирующих материалов для зачета

Всего по текущей работе в семестре студент может набрать 100 баллов, в том числе:

– лабораторные работы – всего 100 баллов.

Зачет проставляется автоматически, если студент набрал в течении семестра не менее 60 баллов и отчитался за каждую контрольную точку. Минимальное количество баллов по каждому из видов текущей работы составляет 60% от максимального.

зачет по дисциплине «Контроль и тестирование программно-аппаратных систем» проводится по результатам работы в семестре. В случае, если полученная в семестре сумма баллов не устраивает студента, во время сессии студент имеет право повысить итоговую оценку либо в форме устного собеседования по приведенным ниже вопросам (п.п. 6.5), либо в результате тестирования.

Шкала оценивания знаний при проведении промежуточной аттестации приведена в таблице 5.

Таблица 5 – Шкала оценивания знаний

Сумма баллов за все виды учебной деятельности	Оценка по национальной шкале зачёт/экзамен
0-59	Не зачтено/неудовлетворительно
60-73	Зачтено/удовлетворительно
74-89	Зачтено/хорошо
90-100	Зачтено/отлично

6.2 Домашнее задание

Домашние задания не предусмотрены.

6.3 Темы для рефератов (презентаций) – индивидуальное задание

Рефераты (индивидуальные задания) не предусмотрены.

6.4 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Тема 1. Программно-аппаратные комплексы защиты информации реального времени.

1. Тестирование это:

а) оценка степени соответствия компонента системы или процесса установленным требованиями и/или потребностям и ожиданиями пользователя/заказчика

б) действия, направленные на управление и контроль качества

в) процесс, содержащий в себе все активности жизненного цикла, касающиеся планирования, подготовки и оценки программного продукта и связанных с этим результатов работ с целью определить, что они соответствуют описанным требованиям, показать, что они подходят для заявленных целей и для определения дефектов

г) прохождение/запуск тестовых сценариев

д) оценка поведения тестируемой системы

2. Первичная цель тестирования ПО это:

а) контроль результатов работы разработчиков по

б) обнаружение отклонений от спецификаций или пожеланий заказчика

в) доказательство того, что в по нет дефектов

г) оценка того, как ведет себя по под пользовательской нагрузкой

3. Главной причиной проведения тестирования программного обеспечения является:

а) определение того, следуют ли программисты подробным правилам и стандартам, определенным в проекте

б) удостоверение в том, что проектное решение соответствует требованиям

в) предотвращение последующих изменений в требованиях

г) нахождение дефектов, которые, возможно, содержатся внутри по, поскольку люди, занимающиеся программированием, делают ошибки

4. Качество это:

а) методы и действия, являющиеся частью управления качеством, которые направлены на выполнение требований к качеству

б) ожидаемое поведение компонента или системы, функционирующей в определенных условиях, на основе спецификации или другого источника

в) отклонение ожидаемого поведения системы от фактического

г) степень, с которой компонент, система или процесс соответствует зафиксированным требованиям и/или ожиданиям и нуждам пользователя или заказчика

5. Если бы тестирование могло обнаружить все дефекты, это

а) гарантировало бы высокое качество программного продукта

б) удручало и расстраивало бы разработчиков

в) по-прежнему не гарантировало бы высокое качество программного продукта

г) устранило бы необходимость дальнейшего сопровождения

6. Выберите верное/верные утверждения при тестировании

а) все части системы должны быть протестированы с одинаковой глубиной, потому что дефекты могут быть в любом месте

б) пользовательский интерфейс должен быть протестирован особенно тщательно, потому что сбои больше всего влияют на впечатление пользователей

в) части системы, в которых риск сбоев наибольший, должны быть протестированы наиболее интенсивно

г) доступ к базе данных должен быть протестирован особенно тщательно для предотвращения добавления неверных данных или возникновения проблем с целостностью данных

д) всё проверить невозможно, необходимо найти стратегию тестирования для обеспечения правильного объема

е) всегда необходимо использовать комбинации всех возможных входных данных

Тема 2. Тестирование программно-аппаратных средств защиты информации.

1. Расположите в верной последовательности активности в тестировании:

а) проектирование тестов

б) завершение тестирования

в) анализ тестирования

г) планирование тестирования

д) реализация тестов

е) выполнение тестов

ж) Мониторинг и контроль тестированияа)

2. Этап "Анализ тестирования" отвечает на вопрос:

а) как тестировать?

б) что тестировать?

в) как проверить?

г) всё ли у нас есть для запуска тестов?

3. Выберете верные утверждения:

а) на этапе проектирования тестов происходит подготовка тестовых данных и правильная загрузка их в тестовое окружение)

б) на этапе реализации тестов происходит выполнение тестов вручную или с помощью инструментов выполнения тестов)

в) на этапе выполнения тестов происходит анализ отклонений для установления их вероятных причин (так же называем еще данную активность - локализация дефекта)а)

г) на этапе реализации тестов происходит подготовка тестовых данных и правильная загрузка их в тестовое окружение)

д) на этапе проектирования тестов происходит определение необходимых тестовых данных для поддержки тестовых условий и тестовых сценариев)

е) на этапе выполнения тестов происходит отражение двунаправленной трассируемости между базисом тестирования, тестовыми условиями, тестовыми сценариями и процедурами тестирования

4. К какому этапу тестирования относится следующая активность: "Анализ результатов тестирования"

а) анализ тестирования

б) проектирование тестов

в) реализация тестов

г) завершение тестирования

4. Выберите основные недостатки гибкой методологии разработки:

а) сложность построения стабильных процессов

б) проект может остаться незавершенным

в) может привести к низкому качеству продукта

г) сложно внести какие-либо корректировки после релиза

д) нет оценки и прогнозов задач, либо они не сбываются

5. Какой вид тестирования выполняется первым из перечисленных ниже:

а) регрессионное тестирование

б) повторное тестирование

в) дымовое (смоук) тестирование

г) приемочное тестирование

6. Выберите свойства качественных требований:

а) завершённость

б) переносимость

в) недвусмысленность

г) непротиворечивость

д) устойчивость

е) проверяемость

ж) корректность

з) надёжность

6.5 Вопросы для подготовки к зачету

1) Какие Вы знаете основные принципы создания средств защиты информации?
2) Как бы Вы описали способ контроля потоков данных, посредством применения основного правила разграничения доступа, применяемого в мандатном механизме управления доступом?
3) Что такое концепция построения программно–аппаратных средств обеспечения информационной безопасности?
4) Как бы Вы описали применение ролевого способа управления доступом?
5) Какие Вы знаете методы ограничения доступа и управления доступом?
6) Как бы Вы описали идентификацию и аутентификацию?
7) Что такое парольные системы?
8) Какие Вы знаете основные документы, определяющие требования к структуре и функциям СЗИ?
9) Какие Вы знаете методы ограничения доступа и управления доступом?
10) Что такое дискреционное управление доступом?
11) Как бы Вы описали порядок функционирования компонентов СЗИ от НСД Secret Net?
12) Какие Вы знаете методы ограничения доступа и управления доступом.
13) Что такое мандатное управление доступом?
14) Как бы Вы описали порядок функционирования ядра и основных подсистем СЗИ от НСД Secret Net?
15) Какие Вы знаете методы ограничения доступа и управления доступом?
16) Что такое ролевое управление доступом?
17) Как бы Вы описали характеристику режимов идентификации и аутентификации, реализуемых СЗИ от НСД Secret Net?
18) Что Вы знаете о структуре и функциях программно–аппаратных средств обеспечения информационной безопасности?
19) Как бы Вы описали применение механизма блокировок компьютера и видов блокировок, реализуемых СЗИ от НСД Secret Net?
20) Какие Вы знаете о назначении, режимах функционирования, основных функциях, составе устанавливаемых компонентов СЗИ от НСД Secret Net?
21) Как бы Вы описали процедуру доверенной загрузки операционной системы при применении электронных замков и устройство ввода идентификационных признаков (УВИП)?
22) Как бы Вы описали подсистемы клиента СЗИ от НСД Secret Net: ядро системы защиты, подсистема локального управления, защитные подсистемы?
23) Как бы Вы описали общий порядок функционирования СЗИ от НСД Страж NT?

24) Что такое подсистемы клиента СЗИ от НСД Secret Net: модуль входа, подсистема контроля целостности, подсистема работы с аппаратной поддержкой?

25) Как бы Вы описали порядок настройки подсистемы дискреционного и мандатного управления доступом СЗИ от НСД Страж NT?

26) Какие Вы знаете защитные механизмы СЗИ от НСД Secret Net?

27) Что такое идентификация и аутентификация пользователей.

28) Как бы Вы описали порядок тестирования, восстановления и обеспечения целостности СЗИ от НСД Страж NT?

29) Как осуществляется функционирование подсистемы учета носителей СЗИ от НСД Страж NT?

30) Как определить возможную конфигурацию аппаратных средств СЗИ от НСД SecretNet, применяемых для идентификации и аутентификации пользователей?

31) Какие Вы знаете определения и классификацию устройств ввода идентификационных признаков (УВИП)?

32) Как бы Вы пояснили применение концепций распространения прав доступа и дать их сравнительную характеристику?

33) Как бы Вы описали устройства ввода идентификационных признаков?

34) Что такое устройства iButton?

35) Какие Вы знаете результаты применения правил выбора стойких паролей?

36) Какие Вы знаете устройства ввода идентификационных признаков?

37) Что такое смарт-карты и устройства ввода на базе смарт-карт?

38) Как бы Вы описали основные подходы к разработке средств защиты информации?

39) Какие Вы знаете устройства ввода идентификационных признаков?

40) Что такое USB-ключ?

41) Что такое концепция диспетчера доступа?

42) Какие Вы знаете устройства ввода идентификационных признаков?

43) Что такое комбинированные УВИП?

44) Что такое электронные замки?

45) Какие Вы знаете о характеристиках основных принципов создания средств защиты информации и их применения?

46) Какие Вы знаете о назначении, режимах функционирования, основных функция, составе устанавливаемых компонентов СЗИ от НСД Secret Net?

47) Как бы Вы описали процедуру доверенной загрузки операционной системы при применении электронных замков и устройств ввода идентификационных признаков (УВИП)?

48) Какие Вы знаете основные документы, определяющие требования к структуре и функциям СЗИ?

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2024. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/538066 (Дата обращения: 26.08.2024).

2. Жмуров, Д. Б. Программно-аппаратные средства защиты информации: учебное пособие / Д.Б. Жмуров, С.В. Жуков. – Самара: Издательство Самарского университета, 2022 – 80 с.: ил. URL: https://repo.ssau.ru/bitstream/Uchebnye-izdaniya/Programmnoapparatnye-redstva-zashity-informacii-100726/1/978-5-7883-1799-1_2022.pdf?ysclid=m4xx9h9mct315304980 (Дата обращения 26.08.2024).

Дополнительная литература

1. Гриднев В.А. Программно-аппаратные средства защиты информации [Электронный ресурс] : учебное пособие : в 3-х ч. / В. А. Гриднев, Ю. А. Губсков, А. С. Дерябин, А. В. Яковлев. – Тамбов : Издательский центр ФГБОУ ВО «ТГТУ», 2008. – 240 с. URL: https://elar.urfu.ru/bitstream/10995/1403/5/1331981_schoolbook.pdf?ysclid=m4xx0i1ir1299737986 (Дата обращения 26.08.2024).

7.2 Базы данных, электронно-библиотечные системы, информационно-справочные и поисковые системы

1. Научная библиотека ДонГТУ : официальный сайт.— Алчевск. — URL: library.dstu.education.— Текст : электронный.
2. Научно-техническая библиотека БГТУ им. Шухова : официальный сайт. — Белгород. — URL: http://ntb.bstu.ru/jirbis2/ .— Текст : электронный.
3. Консультант студента : электронно-библиотечная система.— Москва. — URL: http://www.studentlibrary.ru/cgi-bin/mb4x .— Текст : электронный.
4. Университетская библиотека онлайн : электронно-библиотечная система.— URL: http://biblioclub.ru/index.php?page=main_ub_red .— Текст : электронный.
5. Сайт кафедры ИСИБ http://scs.dstu.education .

8 Материально-техническое обеспечение дисциплины

Материально-техническая база обеспечивает проведение всех видов деятельности в процессе обучения, соответствует требованиям ФГОС ВО.

Материально-техническое обеспечение представлено в таблице 6.

Таблица 6 – Материально-техническое обеспечение

Наименование оборудованных учебных кабинетов	Адрес (местоположение) учебных кабинетов
Специальные помещения: *Мультимедийная аудитория. (60 посадочных мест)*, оборудованная специализированной (учебной) мебелью (скамья учебная –20 шт., стол– 1 шт., доска аудиторная– 1 шт.), учебное ПК (монитор + системный блок), мультимедийная стойка с оборудованием – 1 шт., широкоформатный экран. Аудитории для проведения лекций: *Компьютерные классы (22 посадочных места),* оборудованный учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС: ПК– 11 шт.; интерактивная доска – 1 шт.	ауд. *207* корп. *4* ауд. *208* корп. *4*

Лист согласования рабочей программы дисциплины

Разработал:

и.о заведующего кафедрой

интеллектуальных систем

и информационной безопасности _____ Е.Е. Бизянов

(должность) (подпись) Ф.И.О.)

И.о. заведующего кафедрой

интеллектуальных систем

и информационной безопасности _____ Е.Е. Бизянов

(подпись) Ф.И.О.)

Протокол № 1 заседания кафедры ИСИБ от 27.08.2024 г

И.о. декана факультета _____ В.В. Дьячкова

(подпись Ф.И.О.)

Согласовано:
Председатель методической
комиссии по направлению подготовки
10.05.03 Информационная безопасность
автоматизированных систем
(образовательная программа:
Безопасность открытых
информационных систем) _____ Е.Е. Бизянов

(подпись Ф.И.О.)

Начальник учебно-методического центра _____ О.А. Коваленко

(подпись Ф.И.О.)

Лист изменений и дополнений

<table>
<tr><td colspan="2">Номер изменения, дата внесения изменения, номер страницы для внесения изменений</td></tr>
<tr><td>ДО ВНЕСЕНИЯ ИЗМЕНЕНИЙ:</td><td>ПОСЛЕ ВНЕСЕНИЯ ИЗМЕНЕНИЙ:</td></tr>
<tr><td colspan="2">Основание:</td></tr>
<tr><td colspan="2">Подпись лица, ответственного за внесение изменений</td></tr>
</table>