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

Разработка и эксплуатация автоматизированных систем в защищенном исполнении
(наименование дисциплины)

10.05.05 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 «Разработка и эксплуатация автоматизированных систем в защищенном исполнении» 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: теоретическая и практическая подготовка специалистов к профессиональной деятельности, связанной с разработкой и эксплуатацией защищенных автоматизированных информационных систем.

Дисциплина направлена на формирование общепрофессиональных (ОПК-11, ОПК-14) компетенций 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: «Физика», «Высшая математика», «Основы электротехники», «Информатика», «Основы информационной безопасности».

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

Является основой для изучения следующих дисциплин: «Организация ЭВМ и вычислительных систем», «Программно-аппаратные средства обеспечения информационной безопасности», «Защита информации».

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 4 зачетных единицы, 144 ак.ч. Программой дисциплины предусмотрены лекционные (36 ч.), лабораторные (18 ч.) занятия и самостоятельная работа студента (90 ч.).

Дисциплина изучается на 4 курсе в 8 семестре. Форма промежуточной аттестации – экзамен.

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

Процесс изучения дисциплины «Разработка и эксплуатация автоматизированных систем в защищенном исполнении» 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 компоненты систем защиты информации автоматизированных систем	ОПК-11	ОПК-11.2 Проектирует компоненты систем защиты информации автоматизированных систем
Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	ОПК-14	ОПК-14.1 Осуществляет разработку и внедрение автоматизированных систем с учетом требований по защите информации

4 Объём и виды занятий по дисциплине

Общая трудоёмкость учебной дисциплины составляет 4 зачётных единицы, 144 ак.ч.

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

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)	36	36
Практические занятия (ПЗ)	–	–
Лабораторные работы (ЛР)	18	18
Курсовая работа/курсовой проект	-	-
Самостоятельная работа студентов (СРС), в том числе:	90	90
Подготовка к лекциям	9	9
Подготовка к лабораторным работам	9	9
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	18	18
Работа в библиотеке	18	18
Подготовка к экзамену (Э)	36	36
Промежуточная аттестация – экзамен (Э)	Э	Э
Общая трудоемкость дисциплины		
ак.ч.	144	108
з.е.	4	4

5 Содержание дисциплины

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

– тема 1 (Современные подходы к проектированию и разработке автоматизированных систем в защищенном исполнении);

– тема 2 (Принципы создания защищенных автоматизированных систем).

– тема 3 (Создание приложений, библиотек и программных компонентов на основе платформ производителей программного обеспечения).

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	Современные подходы к проектированию и разработке автоматизированных систем в защищенном исполнении	Современные подходы к проектированию и разработке программного обеспечения в защищенном исполнении. Нормативная документация в области построения защищенных автоматизированных систем. Органы сертификации и надзора в области создания защищенных систем. Программные продукты как сложные системы. Жизненный цикл программного обеспечения в защищенном исполнении. Основные принципы эксплуатации защищенных автоматизированных систем.	4 4 2 4 4	–	-	Изучение основных программных продуктов для построения программного обеспечения в защищенном исполнении	2
2	Принципы создания защищенных автоматизированных систем	Принципы создания защищенных автоматизированных систем с помощью платформ разработчика	10	-	-	Проектирование автоматизированной системы согласно жизненному циклу программного обеспечения в защищенном исполнении	2

Завершение таблицы 3

1	2	3	4	5	6	7	8
3	Создание приложений, библиотек и программных компонентов на основе платформ производителей программного обеспечения	Создание приложений, библиотек и программных компонентов на основе платформ производителей программного обеспечения Крипто Про, Рутокен, VIPNet, SecretNet.	8	-	-	Изучение платформ Крипто Про, VIPNet. Изучение платформы Рутокен, SecretNet. Разработка программного обеспечения с использование платформ Крипто Про, VIPNet, Рутокен, SecretNet.	2 2 2 4 4
Всего аудиторных часов			36	-		18	

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
ОПК-11, ОПК-14	Экзамен	Комплект контролирующих материалов для экзамена

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

– лабораторные работы – всего 100 баллов.

Экзаменационная оценка 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.

Экзамен по дисциплине «Разработка и эксплуатация автоматизированных систем в защищенном исполнении» 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. Современные подходы к проектированию и разработке автоматизированных систем в защищенном исполнении.

1. Сколько стадий разработки ИС определяют стандарт ГОСТ 34.601—90?

Ответ: восемь.

2. Что определяют процессы соглашения?

Ответ: Действия, необходимые для выработки соглашений между двумя организациями — заказчиком и поставщиком.

3. Что определяют технические процессы?

Ответ: Деятельность по реализации исходных требований в полезный программный продукт.

4. Что представляет собой процесс инсталляции системы?

Ответ: Установку программного продукта.

5. Подтверждение фактов, что установленные требования выполняются для конкретного применения рабочего программного продукта- это?

Ответ: валидация.

Тема 2. Принципы создания защищенных автоматизированных систем.

1. Какие ключевые этапы включает процесс менеджмента программной документации в соответствии с ГОСТ Р ИСО/МЭК 12207—2010?

Ответ: формирование стратегии идентификации, установление стандартов, определение содержания и целей документации, разработку и сопровождение документов.

2. Что должна содержать идентифицированная документация в соответствии с ГОСТ Р ИСО/МЭК 12207—2010?

Ответ: заголовок, цели, круг пользователей, процедуры ответственности и графики версий

3. Что включают методологии при разработке информационных систем?

Ответ: Методологии включают в себя набор принципов, методик и практик, направленных на достижение определенных целей и результатов в процессе разработки ИС.

4. Что представляют процессы при разработке информационных систем?

Ответ: Процессы представляют собой формальное описание бизнес-процессов разработки ИС.

5. Какие особенности и подходы характеризуют методологию RAD (Rapid Application Development) в разработке программного обеспечения?

Ответ: Методология RAD включает короткие и тщательно проработанные графики выполнения работ, работу в небольших командах программистов и цикличность разработки с обновлением функциональности приложения на каждом цикле.

Тема 3. Создание приложений, библиотек и программных компонентов на основе платформ производителей программного обеспечения.

1. Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это…

а) комплексное обеспечение ИБ

б) безопасность АС

в) угроза ИБ

г) атака на АС

д) политика безопасности

2. Автоматизированная система должна обеспечивать (возможны несколько ответов)

а) надежность

б) доступность

в) целостность

г) контролируемость

3. Основными компонентами парольной системы являются … (возможны несколько ответов)

а) интерфейс администратора

б)хранимая копия пароля

в) база данных учетных записей

г) все варианты верны

3. Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это ….

а) идентификатор пользователя

б) пароль пользователя

в) учетная запись пользователя

г) парольная система

4. К принципам информационной безопасности относятся (возможны несколько ответов)

а) скрытость

б) масштабность

в) системность

г) законность

д) открытости алгоритмов

5. Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных это:

а) защита информации

б) компьютерная безопасность

в) защищенность информации

г) безопасность данных

6.5 Вопросы для подготовки к экзамену

1) В чем состоит доктрина безопасности РФ?
2) Какие Вы знаете национальные и международные документы в области защиты информации?
3) Какие Вы знаете основные принципы обеспечения информационной безопасности при проектировании приложений?
4) В чем состоит доктрина информационной безопасности РФ, как она отображена в ГОСТах РФ?
5) Какие Вы знаете Основные принципы и понятия проектирования защищенных автоматизированных систем?
6) Какие Вы знаете признаки сложной системы? Что такое Декомпозиция сложных систем?
7) Какую Вы знаете основную нормативную документацию в области построения защищенных систем?
8) Какое Вы знаете законодательство в области построения защищенных систем?
9) Что относится к основным государственным органам, обеспечивающим сертификацию и лицензирование в области разработки и эксплуатации автоматизированных систем в защищенном исполнении?
10) Что такое жизненный цикл программного обеспечения в защищенном исполнении?
11) Что такое физическая защита информационных систем?
12) Какие Вы знаете программные средства защиты информации?
13) Какие Вы знаете этапы создания систем защиты информации?
14) Какие Вы знаете Требования по защите ИС и классы защиты ИС?
15) Что такое положение о защите информации?
16) В чем состоит безопасность глобальных сетевых технологий и методы информационного воздействия на глобальные информационные сети?
17) Что такое правовые основы защиты информации и закон о защите информации?
18) Какие Вы знаете мтандартные криптографические механизмы операционных систем?
19) В чем состоит взаимодействие с функциональными библиотеками при разработке защищенных автоматизированных систем?

20) Что такое организация передачи данных в автоматизированных системах в защищенном исполнении?

21) В чем состоит использование криптографических интерфейсов при разработке автоматизированных систем в защищенном исполнении?

22) В чем состоит обработка исключений в автоматизированных системах в защищенном исполнении?

23) В чем состоит работа с потоком данных в автоматизированных систем в защищенном исполнении?

24) Что такое расширяющие методы в автоматизированных системах в защищенном исполнении?

25) Что такое технологии разграничения доступа к структурным элементам в автоматизированных системах в защищенном исполнении?

26) В чем состоит тестирование разработанных автоматизированных систем в защищенном исполнении?

27) Что такое платформа Крипто ПРО SDK?

28) Что такое платформа VipNet SDK?

29) Что такое платформа Рутокен SDK?

30) Что такое технологии временных штампов?

31) Что такое технологии использования цифровой подписи при реализации защищенных объектов?

32) Каковы основные этапы проектирования и разработки автоматизированных систем в защищенном исполнении?

33) Какие Вы знаете продуктовые линейки современных производителей средств разработки и обеспечения работы автоматизированных систем в защищенном исполнении?

34) Что такое биометрия, как технологич создания защищенных систем?

35) Какие Вы знаете угрозы, виды угроз и дифференциация угроз?

36) Какие Вы знаете методы несанкционированного доступа в локальные сети?

37) Что такое модель нарушителя?

38) Какие Вы знаете угрозы?

39) Что такое спам и защита от спама?

7. Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. Проектирование информационных систем : учебник и практикум для вузов / Д. В. Чистов, П. П. Мельников, А. В. Золотарюк, Н. Б. Ничепорук. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 273 с. — (Высшее образование). — ISBN 978-5-534-20361-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/558007 (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. 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).

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 — (должность) — (подпись) — Е.Е. Бизянов (Ф.И.О.)

_____ (должность) — _____ (подпись) — _____ (Ф.И.О.)

_____ (должность) — _____ (подпись) — _____ (Ф.И.О.)

И.о. заведующего кафедрой
интеллектуальных систем
и информационной безопасности — (подпись) — Е.Е. Бизянов (Ф.И.О.)

Протокол № 1 заседания кафедры ИСИБ от 27.08.2024 г

И.о. декана факультета — (подпись) — В.В. Дьячкова (Ф.И.О.)

Согласовано:

Председатель методической
комиссии по направлению 09.04.01
«Информатика и вычислительная техника» — (подпись) — Е.Е. Бизянов (Ф.И.О.)

Начальник учебно-методического центра — (подпись) — О.А. Коваленко (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>