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

Методы проектирования защищенных открытых информационных 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 «Методы проектирования защищенных открытых информационных систем» является формирование у будущих специалистов теоретических знаний и практических навыков для решения научно-исследовательских и прикладных задач.

Задачи изучения дисциплины. Формирование у студентов теоретических знаний в области методов и средств проектирования защищенных открытых информационных систем.

Дисциплина направлена на формирование общепрофессиональных (ОПК-14) компетенций выпускника.

2 Место дисциплины в структуре образовательной программы

Логико-структурный анализ дисциплины – курс входит в обязательную часть БЛОКА 1 «Дисциплины (модули)» подготовки студентов по специальности 10.05.03 Информационная безопасность автоматизированных систем (10.05.03-05 Безопасность открытых информационных систем).

Дисциплина реализуется кафедрой интеллектуальных систем и информационной безопасности. Основывается на базе дисциплин: «Безопасность сетей ЭВМ», «Основы информационной безопасности», «Безопасность систем баз данных», «Моделирование угроз информационной безопасности».

Является основой для изучения следующих дисциплин: «Преддипломная практика». Приобретенные знания, могут быть использованы при подготовке и защите выпускной квалификационной работы, а также в профессиональной деятельности.

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения профессиональных задач деятельности, связанных с применением знаний в области проектирования защищенных открытых информационных систем.

Курс является фундаментом для ориентации студентов в сфере разработки систем информационной безопасности.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 ак.ч. Программой дисциплины предусмотрены лекционные (18 ак.ч.), лабораторные (18 ак.ч.) занятия, самостоятельная работа студента (36 ак.ч.).

Дисциплина изучается на 5 курсе в 10 семестре. Форма промежуточной аттестации – зачет.

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

Процесс изучения дисциплины «Методы проектирования защищенных открытых информационных 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 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 2 зачётных единицы, 72 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 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
		8
Аудиторная работа, в том числе:	36	36
Лекции (Л)	18	18
Практические занятия (ПЗ)	-	-
Лабораторные работы (ЛР)	18	18
Курсовая работа/курсовой проект	-	-
Самостоятельная работа студентов (СРС), в том числе:	36	36
Подготовка к лекциям	4	4
Подготовка к лабораторным работам	8	8
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	6	6
Работа в библиотеке	3	3
Подготовка к зачету	15	15
Промежуточная аттестация – зачет (З)	З	З
Общая трудоемкость дисциплины		
ак.ч.	72	72
з.е.	2	2

5 Содержание дисциплины

С целью освоения компетенций, приведенных в п.3 дисциплина разбита на 5 тем:

– тема 1 (Информационные технологии и системы);

– тема 2 (Модели жизненного цикла ИС);

– тема 3 (Разработка моделей ИС);

– тема 4 (Базовые составляющие объектно-ориентированного подхода);

– тема 5 (Модели и диаграммы).

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	Информационные технологии и системы	Основные понятия. Стандарты на ИС. Жизненный цикл ИС. Структура и процессы жизненного цикла. Характеристика основных процессов. Роли участников в проекте.	2	-	-	-	-
2	Модели жизненного цикла ИС.	Методология RAD. Экстремальное программирование. Особенности анализа и проектирования крупных систем. Документы, содержащие требования на разработку систему. Виды требований, фиксируемых в техническом задании. Основные принципы проектирования.	4	-	-	Разработка функциональной модели (методология IDEF0)	4
3	Разработка моделей ИС	Классификация моделей ИС. Разработка функциональной модели ИС (IDEF0, DFD). Разработка информационной модели ИС (ERD, IDEF1X, IE, методология Питера Чена). Разработка поведенческой модели ИС (блок-схемы, EPC, BPMN).	4	-	-	Разработка информационной модели ИС (ERD, IDEF1X, IE, методология Питера Чена)	4

Окончание таблицы 3

1	2	3	4	5	6	7	8
4	Базовые составляющие объектно-ориентированного подхода	Базовые составляющие объектно-ориентированного подхода. История Унифицированного процесса и UML. Назначение и структура UML. Место Унифицированного процесса в проекте. Процесс. Персонал. Продукт. Проект. Утилиты.	4	-	-	Разработка поведенческой модели (блок-схемы)	4
5	Модели и диаграммы	Модель и диаграмма вариантов использования. Диаграммы автоматов. Модель анализа. Диаграммы классов анализа. Диаграммы коммуникации и последовательности. Пакеты. Модель проектирования. Диаграммы классов. Диаграммы деятельности. Модель реализации. Диаграммы компонентов и развертывания.	4	-	-	Разработка диаграмм вариантов использования, автоматов, классов, компонентов	6
Всего аудиторных часов		18		-		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-14	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 «Методы проектирования защищенных открытых информационных систем» проводится по результатам работы в семестре. В случае, если полученная в семестре сумма баллов не устраивает студента, во время зачетной недели студент имеет право повысить итоговую оценку либо в форме устного собеседования по приведенным ниже вопросам (п.п. 6.6), 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

Домашнее задание не предусмотрено.

6.3 Расчетно-графическая работа (РГР)

Расчетно-графическая работа не предусмотрена.

6.4 Темы для рефератов (презентаций) – индивидуальное задание

Рефераты не предусмотрены.

6.5 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Тема 1 (Информационные технологии и системы)

1) Какие стандарты на ИС Вы знаете?
2) Что такое жизненный цикл ИС?
3) Какова структура жизненного цикла ИС?
4) Каковы процессы жизненного цикла ИС?
5) Каковы роли участников в проекте?

Тема 2 (Модели жизненного цикла ИС)

1) Что из себя представляет методология RAD?
2) Что такое экстремальное программирование?
3) Каковы особенности анализа и проектирования крупных систем?
4) Какие документы содержат требования на разработку системы?
5) Какие требования фиксируются в техническом задании?

Тема 3 (Разработка моделей ИС)

1) Как можно классифицировать модели ИС?
2) Что из себя представляет функциональная модель ИС?
3) Что из себя представляет информационная модель ИС?
4) В чем заключается методология Питера Чена?
5) Что из себя представляет поведенческая модель ИС?

Тема 4 (Базовые составляющие объектно-ориентированного подхода)

1) В чем заключаются базовые составляющие объектно-ориентированного подхода?
2) Что из себя представляет унифицированный процесс и UML.?
3) В чем заключается назначение UML?
4) Какова структура UML?
5) Каково место Унифицированного процесса в проекте?

Тема 5 (Модели и диаграммы)

1) Что такое диаграммы автоматов?
2) Что такое модель анализа?

3) Что такое диаграммы классов анализа?
4) Что такое диаграммы коммуникации и последовательности?
5) Что такое диаграммы классов??

6.6 Вопросы для подготовки к зачету

1) Что такое этап реализации?
   а) построение выводов по данным, полученным путем имитации;
   б) теоретическое применение результатов программирования;
   в) *практическое применение модели и результатов моделирования?*
2) Для чего служит прикладное программное обеспечение?
   а) планирования и организации алгоритмов управления объектом;
   б) планирования и организации вычислительного процесса в ЭВМ;
   в) *реализация алгоритмов управления объектом*.
3) Тождественная декомпозиция это операция, в результате которой…
   а) *любая система превращается в саму себя;*
   б) средства декомпозиции тождественны;
   в) система тождественна.
4) На что не ориентируются при выборе системы управления, состоящей из нескольких элементов?
   а) на функциональную полноту.
   б) *на быстродействие и надежность;*
   в) на определенное число элементов.
5) Что понимается под программным обеспечением?
   а) набор специальных программ для моделирования;
   б) *соответствующим образом организованный набор программ и данных*;
   в) набор специальных программ для работы САПР.
6) Параллельная коррекция системы управления позволяет…
   а) скорректировать АЧХ системы;
   б) *обеспечить введение интегралов и производных от сигналов ошибки;*
   в) осуществить интегральные законы регулирования.
7) Модульность структуры состоит
   а) *в разбиении программного массива на модули по функциональному признаку*;
   б) в построении модулей по иерархии;
   в) на принципе вложенности с вертикальным управлением.
8) Результаты имитационного моделирования…
   а) являются источником информации для построения реального объекта;

б) *носят случайный характер, отражают лишь случайные сочетания действующих факторов, складывающихся в процессе моделирования*;

в) являются неточными и требуют тщательного анализа.

9) Какими могут быть средства декомпозиции?

а) реальными и нереальными;

б) имитационными;

в) *материальными и абстрактными*.

10) Что осуществляется на этапе подготовки данных?

а) описание модели на языке, приемлемом для используемой ЭВМ;

б) определение границ характеристик системы, ограничений и измерителей показателей эффективности;

в) *происходит отбор данных, необходимых для построения модели, и представлении их в соответствующей форме*.

11) Как называется показатель, количественно выражающийся суммой ежегодных прямых и косвенных затрат на функционирование корпоративной системы защиты информации?

а) экономическая эффективность бизнеса;

б) общая величина затрат на внедрение системы ИБ;

в) *совокупная стоимость владения системой ИБ*;

г) коэффициент возврата инвестиций.

12) Эффективность защиты информации это…

а) *степень соответствия результатов защиты информации поставленной цели*;

б) мера или характеристика для оценки эффективности защиты информации;

в) значения показателей эффективности защиты информации, установленные нормативными документами.

13) Показатель эффективности защиты информации –

а) *мера или характеристика для оценки эффективности защиты информации*;

б) степень соответствия результатов защиты информации поставленной цели;

в) значения показателей эффективности защиты информации, установленные нормативными документами.

14) Нормы эффективности защиты информации –

а) *значения показателей эффективности защиты информации, установленные нормативными документами*;

б) совокупность действий по разработке и/или практическому применению методов и средств контроля эффективности защиты информации;

в) степень соответствия результатов защиты информации поставленной цели.

15) Мероприятие по контролю эффективности защиты информации –

а) *совокупность действий по разработке и/или практическому применению методов и средств контроля эффективности защиты информации*;

б) степень соответствия результатов защиты информации поставленной цели;

в) значения показателей эффективности защиты информации, установленные нормативными документами.

16) Категорирование защищаемой информации [объекта защиты] –

а) *установление градаций важности защиты защищаемой информации [объекта защиты]*;

б) степень соответствия результатов защиты информации поставленной цели;

в) значения показателей эффективности защиты информации, установленные нормативными документами.

17) Метод [способ] контроля эффективности защиты информации –

а) *порядок и правила применения определенных принципов и средств контроля эффективности защиты информации*;

б) установление градаций важности защиты защищаемой информации [объекта защиты];

в) проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации.

18) Контроль состояния защиты информации –

а) *проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации*;

б) установление градаций важности защиты защищаемой информации [объекта защиты];

в) проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации.

19) Контроль организации защиты информации –

а) *проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации*;

б) проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации.

20) Что в сфере информационной безопасности принято считать риском?

а) *потенциальную возможность понести убытки из-за нарушения безопасности информационной системы*;

б) потенциально возможное происшествие неважно, преднамеренное или нет, которое может оказать нежелательное воздействие на компьютерную систему, а также информацию, хранящуюся и обрабатывающуюся в ней;

в) характеристику, которая делает возможным возникновение угрозы.

21) Что принято считать ресурсом или активом информационной системы?

а) модель информационной системы;

б) все элементы, имеющие материальную ценность независимо от того подлежат они защите или нет;

в) *именованный элемент информационной системы, имеющий (материальную) ценность и подлежащий защите.*

22) Что отличает риск от угрозы?

а) объем вероятных потерь;

б) *наличие количественной оценки возможных потерь и (возможно) оценки вероятности реализации угрозы*;

в) угроза и риск - понятия идентичные.

23) Почему аналитический метод определения минимальных затрат при расчетах защиты информационной системы неприменим?

а) потому, что расчеты ресурсов подвержены флуктуациям, связанными с колебаниями на рынке услуг в сфере безопасности ИС;

б) *потому, что на практике точные зависимости между затратами и уровнем защищенности определить не представляется возможны*м;

в) потому, что уровень защищенности информационной системы неадекватен затратам на ее защиту.

24) Идентифицируется ли риск уязвимостью, через которую может быть реализована некая угроза в отношении определенного ресурса?

а) *да*;

б) нет;

в) да, но только в случае отсутствия угрозы.

25) На какие ресурсы может быть направлена угроза?

а) только на информационные ресурсы;

б) только на аппаратные ресурсы;

в) *на любые виды ресурсов (информационный, аппаратный, программный и т.д.).*

26) Что представляет собой система с полным перекрытием?

а) система, в которой ведется учет всех вторжений, блокируются только вредоносные проникновения;

б) *система, в которой имеются средства защиты на каждый возможный путь проникновения*;

в) система, в которой обеспечивается селективная безопасность.

27) Что происходит с размером ожидаемых потерь при увеличении затрат на защиту?

а) *падает*;

б) находится в зависимости от других факторов;

в) не изменяется.

28) Каким параметром принято определять степень разрушительности?

а) коэффициентом разрушительности;

б) *стоимостью ресурса*;

в) коэффициентом риска.

29) Что в сфере информационной безопасности принято считать риском?

а) *потенциальную возможность понести убытки из-за нарушения безопасности информационной системы*;

б) потенциально возможное происшествие неважно, преднамеренное или нет, которое может оказать нежелательное воздействие на компьютерную систему, а также информацию, хранящуюся и обрабатывающуюся в ней;

в) характеристику, которая делает возможным возникновение угрозы

30) Какую лицензию должна получить испытательная лаборатория для проведения работ по сертификации средств защиты информации, используемых на объектах информатизации, обрабатывающих информацию ограниченного доступа, не содержащую сведения, составляющие государственную тайну?

а) на проведение работ, связанных с созданием средств защиты информации на осуществление работ, связанных с созданием средств защиты информации, содержащей сведения, составляющие государственную тайну;

б) на деятельность по технической защите конфиденциальной информации;

в) *на деятельность по разработке и производству средств защиты конфиденциальной информации*.

31) Кто выдает предписания на приостановление работ на аттестованном объекте информатизации?

а) *ФСТЭК России*;

б) орган по аттестации;

в) лицензиат, имеющий лицензию на ТЗКИ;

г) заявитель.

32) Туннелирование может применяться для достижения следующих целей:

а) *передача через сеть пакетов, принадлежащих протоколу, который в данной сети не поддерживается*;

б) расширение спектра поддерживаемых протоколов;

в) уменьшение нагрузки на сеть.

33) Какие из перечисленных мер защиты относятся к организационным?

а) защита периметра сети с помощью межсетевого экрана;

б) *создание службы защиты информации*;

в) *определение порядка доступа к защищаемым объектам*;

г) использование антивирусных средств защиты.

34) Какие из перечисленных характеристик не входят в систему обеспечения безопасности Клементса:

а) O - набор защищаемых объектов; T - набор угроз; M - набор средств обеспечения безопасности; P- набор креативных функций; Z - набор виндикативных инструментов;

б) O - набор защищаемых объектов; T - набор угроз; M - набор средств обеспечения безопасности; P- набор креативных функций;

в) O - набор защищаемых объектов; T - набор угроз; M - набор средств обеспечения безопасности; P- набор креативных функций; Z - набор виндикативных инструментов;

г) *P- набор креативных функций; Z - набор виндикативных инструментов*.

35) Аутентификация на основе пароля, переданного по сети в открытом виде, плоха, потому что не обеспечивает защиты от:

а) *перехвата*;

б) *воспроизведения*;

в) *атак на доступность*.

36) Аутентификация на основе пароля, переданного по сети в зашифрованном виде и снабженного открытой временной меткой, плоха, потому что не обеспечивает защиты от:

а) *перехвата*;

б) *воспроизведения*;

в) атак на доступность.

37) Демилитаризованная зона располагается:

а) перед внешним межсетевым экраном;

б) *между межсетевыми экранами*;

в) за внутренним межсетевым экраном.

38) К межсетевым экранам целесообразно применять следующие принципы архитектурной безопасности:

а) усиление самого слабого звена;

б) *эшелонированность обороны*;

в) *невозможность перехода в небезопасное состояние.*

39) Системы анализа защищенности помогают предотвратить:

а) *известные атаки*;

б) новые виды атак;

в) нетипичное поведение пользователей.

40) Каким термином обозначается анализ регистрационной информации системы защиты?

а) мониторинг;

б) *аудит*;

в) аккредитация;

г) сертификация.

41) Какие компоненты присутствуют в модели системы защиты с полным перекрытием?

а) *область угроз*;

б) область рисков;

в) *защищаемая область*;

г) *система защиты*;

д) область безопасности.

42) Как называется возможность осуществления угрозы T в отношении объекта O?

а) слабость;

б) неполнота;

в) *уязвимость*;

г) риск.

43) Чем характеризуется степень сопротивляемости механизма защиты?

а) *вероятностью его преодоления*;

б) количеством угроз, которым этот механизм препятствует;

в) величиной потерь в случае успешного прохождения;

г) стоимостью механизма защиты.

44) Защищенность системы защиты определяется как величина…

а) обратная суммарному количеству рисков;

б) обратная остаточному риску;

в) *обратная уязвимости*;

г) равная сумме всех уязвимостей

45) В чем заключается идеология открытых систем информационной безопасности?

а) в строгом соответствии систем информационной безопасности законодательству страны, котором они созданы

б) *в строгом соблюдении совокупности профилей, протоколов и стандартов де-факто и де-юре*;

в) в открытости информации о стоимости реализации конкретной системы защиты

г) в открытости программных кодов средств защиты от производителей разных стран.

46) Достоинствами линейно-функциональной структуры являются:

а) стабильность (наиболее эффективны в стабильной среде);

б) *экономия на управленческих расходах*;

в) *быстрое решение простых проблем, находящихся в компетенции одной функциональной службы*;

г) широкая специализация работников, которая расширяет их профессиональный горизонт;

д) *ориентация на действующие технологии и сложившийся рынок*;

е) *ориентация на ценовую конкуренцию*;

ж) большой объем полномочий функциональных и линейных руководителе, позволяющий быстро решать сложные проблемы.

47) В соответствии с какими основными принципами производится структуризация компании по дивизионам:

а) *по продуктовому*;

б) по уровню зрелости бизнеса;

в) по уровню доходов;

г) *в зависимости от ориентации на конкретного потребителя*;

д) *по региональному*;

е) по уровню прибыли.

6.7 Тематика и содержание курсового проекта

Курсовой проект не предусмотрен.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. Григорьев М.В. Проектирование информационных систем : учебное пособие для вузов / М.В. Григорьев, И.И. Григорьева. — Москва : Издательство Юрайт, 2024. — 278 с. — (Высшее образование). — Текст : электронный // Образовательная платформа Юрайт. — (Высшее образование: Бакалавриат) ─ [Электронный ресурс]: https://urait.ru/bcode/530832 – Режим доступа: для авторизованных пользователей (Дата обращения 26.08.2024).

Дополнительная литература

1. Мельников Д. А. Информационная безопасность открытых систем :учебник / Д. А. Мельников. - Москва: Флинта, Наука, 2013. — 328 с. [Электронный ресурс]: https://dl.libcats.org/genesis/792000/b01732bdd8b0a73317bcda100f5aa225/_as/[A.B._Vavrenyuk,_N.P._Vasilev,_E.V._Velmyakina,_D.(libcats.org).pdf (дата обращения: 26.08.2024).

2. Душкин А.В. Методологические основы построения защищенных автоматизированных систем: учебное пособие / А.В. Душкин, О.В. Ланкин, С.В. Потехецкий, А.П. Данилкин. - Воронеж: ВГУИТ, 2013. - 263 с. - Текст: электронный // Лань: электронно-библиотечная система. - URL: (дата обращения: 04.11.2023). - Режим доступа: для авториз. пользователей. 100 с. - . [Электронный ресурс]: https://e.lanbook.com/book/72890 Режим доступа: для авторизованных пользователей (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. IPR BOOKS : электронно-библиотечная система.—Красногорск. — URL: http://www.iprbookshop.ru/. — Текст : электронный.

6. 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 (парта трехместная – 18 шт., парта двухместная – 6 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:	ауд. *207* корп. *4* ауд. *217* корп. *3* ауд. *211* корп. *4*

Лист согласования РПД

Разработал:
ст. преподаватель кафедры
интеллектуальных систем и
информационной безопасности
(должность) (подпись) Р.Н. Погорелов (Ф.И.О.)

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

Протокол № 1 заседания кафедры от 27.08. 2024г.

И.о. декана факультета
информационных технологий
и автоматизации производственных
процессов:
(наименование факультета) (подпись) В.В. Дьячкова (Ф.И.О.)

Согласовано

Председатель методической
комиссии по специальности 10.05.03 (подпись) Е.Е. Бизянов (Ф.И.О.)
Информационная безопасность
автоматизированных систем

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>