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

Информационная безопасность 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 «Информационная безопасность открытых информационных систем» является приобретение студентами фундаментальных представлений о функциях современной ИБОИС и о структуре ее функциональных компонентов, дается определение задач ИБОИС и ее границ, говорится об адекватном позиционировании и средствах интеграции ИБОИС в современной ИТ структуре.

Задачи изучения дисциплины. Приобретение студентами знаний, умений и практических навыков, необходимых для понимания обеспечения информационной безопасности открытых информационных систем. Изучить алгоритмы работы техники, протоколов, коррекция инструкций и положений, основные принципы построения защищенных открытых информационных систем для решения задач различного рода.

Дисциплина направлена на формирование общепрофессиональных (ОПК-5) и профессиональных (ПК-1) 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: «Физика», «Математический анализ», «Электроника и схемотехника ЭВМ», «Программно-аппаратные средства защиты информации», «Разработка и эксплуатация автоматизированных систем в защищенном исполнении».

Является основой для изучения следующих дисциплин: «Управление информационной безопасностью», «Разработка и эксплуатация автоматизированных систем в защищенном исполнении», «Интеллектуальные системы информационной безопасности».

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения профессиональных задач деятельности, связанных с применением вычислительных систем.

Курс является фундаментом для ориентации студентов в сфере разработки информационных систем.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 ак.ч. Программой дисциплины предусмотрены лекционные (18 ак.ч.), лабораторные (18 ак.ч.) занятия, самостоятельная работа студента (72 ак.ч.).

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

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

Процесс изучения дисциплины «Информационная безопасность 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 применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5	ОПК-5.2 Применяет нормативные и методические документы, регламентирующие деятельность по защите информации
Способен разрабатывать системы защиты информации автоматизированных систем	ПК-1	ПК-1.1 Осуществляет формирование требований к защите информации автоматизированных систем

4 Объём и виды занятий по дисциплине

Общая трудоёмкость учебной дисциплины составляет 3 зачётных единицы, 108 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:	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:	72	72
Подготовка к лекциям	4	4
Подготовка к лабораторным работам	12	12
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	10	10
Работа в библиотеке	10	10
Подготовка к экзамену	36	36
Промежуточная аттестация – экзамен (Э)	Э	Э
Общая трудоемкость дисциплины		
ак.ч.	108	108
з.е.	3	3

5 Содержание дисциплины

С целью освоения компетенций, приведенных в п.3 дисциплина разбита на 8 тем:

– тема 1 (Понятие открытой системы);

– тема 2 (Связь в распределенных системах);

– тема 3 (Понятие транзакции);

– тема 4 (Распределенные базы данных);

– тема 5 (Объектно-распределенные системы);

– тема 6 (Распределенные Web-приложения);

– тема 7 (Организация защищенного канала связи между клиентом и сервером);

– тема 8 (Контроль доступа к ресурсам).

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	Понятие открытой системы	Понятие распределенной системы. Преимущества и недостатки распределенных систем. Масштабируемость. Прозрачность. Целостность и репликация. Аппаратные и программные средства построения распределенных систем	2	-	-	Удаленное взаимодействие с помощью технологии NET Remoting	2
2	Связь в распределенных системах	Связь в распределенных системах. Удаленный вызов процедур. Сохранность. Типы связей.	2	-	-	-	-
3	Понятие транзакции	Понятие транзакции. Распределенные транзакции. Принцип ACID. Вложенные транзакции.	2	-	-	Удаленное взаимодействие с помощью технологии API Java.net.	2
4	Распределенные базы данных	Распределенные базы данных. Целостность данных. Прозрачность расположения. Обработка распределенных запросов.	2	-	-	-	-
5	Объектно-распределенные системы	Объектно-распределенные системы. Технологии CORBA, DCOM, Java RMI.	2	-	-	Разработка распределенного приложения с помощью технологии Java RMI	2

Завершение таблицы 3

1	2	3	4	5	6	7	8
6	Распределенные Web-приложения	Распределенные Web-приложения. Платформы Java EE, Net.	2	-	-	Разработка распределенного приложения с помощью технологии CORBA средствами языка программирования Java	4
7	Организация защищенного канала связи между клиентом и сервером	Организация защищенного канала связи между клиентом и сервером. Основные сетевые механизмы безопасности. Идентификация и аутентификация. Протоколирование и аудит. Целостность и конфиденциальность сообщений.	4	-	-	Разработка распределенного приложения с помощью технологии JMS	4
8	Контроль доступа к ресурсам	Контроль доступа к ресурсам. Использование брандмауэров и систем обнаружения вторжений	2	-	-	Разработка распределенного приложения с помощью технологии EJB	4
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-5, ПК-1	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.

Оценка по экзамену 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 «Информационная безопасность открытых информационных 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 в форме устного собеседования по приведенным ниже вопросам.

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 Темы для рефератов (презентаций) – индивидуальное задание

Рефераты не предусмотрены.

6.4 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Тема 1 (Понятие открытой системы)

1) Что представляет из себя распределенная система?
2) В чем отличие между параллельной и распределенной системами?
3) Каковы технологии масштабируемости программных систем?
4) Что такое распределенная система?
5) Что такое открытая система?

Тема 2 (Связь в распределенных системах)

1) По каким признакам можно разграничить понятия «вычислительная машина» и «вычислительная система»?
2) Что из себя представляет Модель OSI?
3) Какие уровни модели OSI Вы знаете?
4) Что из себя представляют межуровневые взаимодействия?
5) Что из себя представляют протокольные взаимодействия?

Тема 3 (Понятие транзакции)

1) Чем отличаются между собой идентификация и аутентификация?
2) Что из себя представляет транзакция?
3) Что из себя представляют распределенные транзакции?
4) «Удаленный вызов процедур», что это?
5) Что из себя представляют «заглушки»?

Тема 4 (Распределенные базы данных)

1) Что из себя представляют распределенные базы данных?
2) В чем заключается целостность данных?
3) Что такое «Прозрачность расположения» данных?
4) Что из себя представляют распределенные запросы?
5) В чем заключается обработка распределенных запросов?

Тема 5 (Объектно-распределенные системы)

1) Что такое «Обращение к удаленному объекту»?
2) В чем заключается статическое обращение к объекту?
3) В чем заключается динамическое обращение к объекту?
4) Что такое неявная привязка ссылок на объект?
5) Что такое явная привязка ссылок на объект?

Тема 6 (Распределенные Web-приложения);

1) Что из себя представляют расширенные модели RPC?
2) Что из себя представляет архитектура CORBA?
3) В чем заключаются задачи ORB?
4) Что из себя представляет интерфейс к объекту в CORBA?
5) Что из себя представляют IDL-стабы?

Тема 7 (Организация защищенного канала связи между клиентом и сервером;

1) Что из себя представляет интерфейс динамических вызовов?
2) Что из себя представляет репозиторий интерфейсов?
3) Что такое «сервант» в CORBA?
4) В чем заключается назначение протокола IIOP/GIOP?
5) Что из себя представляет объектный адаптер?

Тема 8 (Контроль доступа к ресурсам).

1) Что из себя представляет технология DCOM?
2) В чем отличие между технологиями CORBA и DCOM?
3) Каковы основные возможности и компоненты технологии J2EE?
4) Каковы особенности работы с базой данных с JDBC?
5) Что из себя представляет архитектура Web приложений J2EE?

6.5 Вопросы для подготовки к экзамену

1) Организация защищенного канала связи между клиентом и сервером. Какие основные сетевые механизмы безопасности Вы знаете?
2) Какие компоненты и возможности конфигурации и сборки у архитектура Web приложений J2EE Вы знаете?
3) Чем определяется целостность и конфиденциальность сообщений?
4) Каковы типичные характеристики ИС организации?
5) Какие требования выдвигаются к идеальным открытым системам?
6) Какие основные свойства открытых систем Вы знаете?
7) Какова роль стандартов в концепции открытых систем?
8) Какие международные организации по стандартизации, виды разрабатываемых ими стандартов Вы знаете?
9) Какие формы логической организации стандартов вы знаете?
10) Что означают понятия переносимости и способности к взаимодействию?
11) Используя базовую модель ИС, поясните, как осуществляется взаимодействие платформы приложений с ПП и объектами внешней среды?
12) В чем заключается системный подход к описанию функциональности на основе модельного представления ИС?

13) Какие функциональные блоки выделяют в открытых системах?

14) Каковы способы их взаимодействия?

15) Как обеспечивается переносимость ПП между открытыми системами?

16) Как обеспечивается переносимость пользователей и данных между открытыми системами?

17) Как обеспечивается способность к взаимодействию открытых систем?

18) Что такое коммуникационный интерфейс и стеки протоколов?

19) Какие свойства распределенной вычислительной среды обеспечивают формирование образа единой системы?

20) Каковы характерные особенности функционирования ПП в распределенной вычислительной среде?

21) Чем характеризуются модели организации распределенных вычислений: хостовая, клиент-серверная, иерархическая, master-slave, одноранговая, объектная?

22) Дайте определение интранету. Каковы его основные отличия от локальной сети?

23) Какие преимущества для организации предоставляет интранет?

24) Из каких элементов состоит архитектура интранета?

25) Какие базовые механизмы выделяют для интранета? Каковы их функции?

26) Какие базовые сервисы интранета вам известны? В чем их назначение?

27) Что такое сетевая инфраструктура интранета? Какие элементы в нее входят?

28) Из чего складывается информационное наполнение интранета?

29) Какие типы приложений используются в интранете?

30) Какие функции и какими средствами выполняет система публикации информации для интранета?

31) Каковы особенности управления интранетом?

32) Какой новый персонал требуется для поддержки функционирования интранет? Каковы его примерные обязанности?

33) Какие виды интранета вам известны?

34) Каково место внутренней информационной среды предприятия в модели глобальной коммуникационной инфраструктуры?

35) Для каких целей в модели TOGAF вводится понятие организационного континуума? Из каких составляющих оно слагается?

36) Что такое экстранет?

37) Рассмотрите известные классификации порталов. В чем особенности КП?

38) Какова логическая структура и компоненты КП?

39) Какие типы злоумышленников в открытых сетях вам известны?

40) Какие угрозы ИБ интранета вам известны? Какие у них источники?

41) В чем проблемы с неправильной конфигурацией систем?

42) Верно ли, что основной задачей защиты встроенных в ОС средств является защита системной информации?

43) Достаточно ли в общем случае встроенных в ОС средств защиты?

44) Какие проблемы с обеспечением информационной безопасности обнаружены на Windows-платформах?

45) Каковы основные причины уязвимости хостов интранета?

46) Какие уязвимости в различных типах серверов являются основными (рассмотрите на ряде примеров)?

47) Какие основные угрозы информации в СУБД вам известны?

48) Каковы основные сценарии атак на СУБД?

49) Каким несанкционированным действиям может подвергнуться рабочая станция?

50) В чем заключаются основные уязвимости каналов связи?

51) Как осуществляются различные типы перехватов данных в каналах связи?

52) Какие уязвимости каналообразующего оборудования нужно учитывать при создании системы защиты для интранета?

53) С чем связаны уязвимости системных утилит, команд и сервисов?

54) Какими возможностями для несанкционированного доступа к информации обладает злоумышленник при работе с сервисом Telnet?

55) Каковы последствия при получении доступа злоумышленником к неправильно сконфигурированному FTP-серверу?

56) В чем проблемы с системой безопасности при работе с сетевой файловой системой?

57) Каково назначение системы доменных имен и в чем заключается DNS-алгоритм удаленного поиска IP-адреса по имени?

58) Чем опасна подстановка ложных доменных имен?

59) Какие злоупотребления возможны при работе с сетевой информационной системой?

60) Что такое скрипты CGI? Какие проблемы для обеспечения информационной безопасности могут возникнуть при их использовании?

61) Какая специальная информация в системе WWW может помочь злоумышленникам получить несанкционированный доступ к информации?

62) Как осуществляется защита веб-узла от "фальшивых" запросов?

63) Какие проблемы возникают при использовании команды удаленного выполнения?

64) Каковы потенциальные проблемы с электронной почтой? Как можно вывести из строя почтовый сервер?

65) Какие утилиты могут помочь узнать злоумышленникам больше информации об интранете?

66) Каковы характерные признаки УА на интранет и что понимают под "типовыми удаленными атаками"?

67) По каким основным критериям можно классифицировать УА?

68) Рассмотрите типовую атаку "анализ сетевого трафика".

69) Каким образом может осуществляться перехват паролей в интранете? Какие объективные причины этому способствуют?

70) Что такое программа-sniffer? Как она работает и при каких условиях?

71) Где в интранете злоумышленник может перехватить незащищенный трафик?

72) В чем суть распределенных атак "отказ в обслуживании"? Какие рекомендации по защите от них вы можете дать для Unix- и Windows-платформ?

73) Как реализуется типовая атака получения удаленного контроля над станцией в сети?

74) В чем проявляются атаки, возникающие из-за недостатков ОС и стека протоколов TCP/IP?

75) Для чего предназначены "программные закладки", внедряемые злоумышленниками в ПО?

76) Как осуществляется перехват информации 1) при ее перемещении в интранете по каналам связи и 2) непосредственно при вводе с клавиатуры?

77) Какие средства используются злоумышленниками для исследования системы, выбранной ими в качестве жертвы для атаки?

78) Каковы этапы реализации атак?

79) Какие средства используются при этом злоумышленниками?

80) Что знает и может злоумышленник на каждом этапе реализации удаленной атаки?

81) На какие уровни можно подразделить атаки в зависимости от серьезности последствий от их реализации?

82) Какие методы и средства, применяемые злоумышленниками при вторжении в интранет, вам известны?

83) Какие виды нападений с использованием сетевых протоколов наиболее часто применяются злоумышленниками в отношении интранет?

84) Что такое спуффинг?

85) Какие проблемы с информационной безопасностью возникают при использовании графических интерфейсов?

86) Как осуществляется перехват сеансов злоумышленниками и по каким причинам?

87) Какие проблемы с электронной почтой могут возникнуть при вмешательстве в почтовый сервис злоумышленником?

88) Какие методы и средства обнаружения прослушивающих приложений в Windows вам известны?

89) Какие еще методы вторжений в интранет могут предприниматься злоумышленниками и для каких систем они характерны?

90) Сколько уровней выделяют в модели ИС при организации доступа в другие сети?

91) На каком уровне модели ИС организация определяет сервисы, которые станут доступными для пользователей из Интернета внутри сети организации?

92) На каком уровне модели ИС организация определяет сервисы и службы, которые будут открыты ее сотрудникам в сети Интернета?

93) На каком уровне модели ИС организация определяет правила разграничения доступа к информационным ресурсам своей сети?

94) На каком уровне модели ИС организация определяет правила доступа к ресурсам ОС?

95) На каком уровне модели ИС организация определяет правила работы с прикладными программами?

96) На каком уровне модели ИС организация определяет правила взаимодействия с удаленными пользователями своей сети?

97) На каком этапе производится поиск уязвимых мест в сети организации?

98) Осуществление каких мероприятий предполагает управление безопасностью интранета?

99) Какие выделяют основные виды топологии интранета при подключении к Интернету?

100) В чем преимущества и недостатки физической изоляции?

101) Как осуществляется изоляция протоколов при подключении к Интернету?

102) Как реализуется топология на основе использования маршрутизаторов?

103) Что такое ПБ интранета? Каковы ее основные компоненты? Зачем она нужна?

104) Каковы этапы выработки ПБ?

105) Какие предъявляются требования к ПБ?

106) Какие два вида категорий ПБ вам известны?

107) Каковы в общем случае две задачи защиты информационного взаимодействия в открытых системах? Применением каких средств защиты они могут быть решены?

108) Для чего используются в интранете зоны безопасности?

109) Что такое эшелонированная защита интранета?

110) Каково содержание документа, описывающего ПБ интранета?

111) Что такое анализ рисков и для чего он нужен?

112) По каким признакам можно определить, что произошел взлом интранета?

113) Что делать в случае взлома интранета?

114) Какова в общих чертах процедура документирования факта взлома интранета?

115) Как предотвратить посягательства злоумышленников на интранет?

116) Как проследить за работой пользователей в интранете и Интернете? На основе каких подходов работают эти средства?

117) Каковы краткие рекомендации администраторам ИБ интранета?

6.6 Тематика и содержание курсового проекта

Курсовой проект не предусмотрен.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. Карпухин Е.О. Технологии и методы защиты инфокоммуникационных систем и сетей: учебное пособие для вузов / Е.О. Карпухин - М. : Горячая линия - Телеком, 2021 - 120 с. – [Электронный ресурс]: Режим доступа: https://znanium.ru/read?id=419370. (дата обращения: 26.08.2024).

2. Зенков А.В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — [Электронный ресурс]: Режим доступа: Текст: электронный // Образовательная платформа Юрайт [сайт]. https://urait.ru/bcode/544290 (дата обращения: 26.08.2024).

3. Сычев Ю.Н. Защита информации и информационная безопасность: учебное пособие для студентов высших учебных заведений, обучающихся по направлению подготовки 10.03.01 "Информационная безопасность" (квалификация (степень) "бакалавр") / Ю.Н. Сычев. – Москва : ИНФРА-М, 2023 . – 199 с. : ил. + табл. – (Высшее образование: Бакалавриат). – 15 экз.

Дополнительная литература

1. Мельников Д.А. Информационная безопасность открытых систем: учебник / Д.А. Мельников. — М.: ФЛИНТА : Наука, 2019. — 448 с. – [Электронный ресурс]: Режим доступа: https://znanium.ru/read?id=344453. (Дата обращения 26.08.2024).

2. Запечников С.В. Информационная безопасность открытых систем: Учебник для вузов. В 2-х томах. Том 1 - Угрозы, уязвимости, атаки и подходы к защите / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. - М.: Горячая линия-Телеком, 2006. - 536 е.: ил. –[Электронный ресурс]. – URL: https://openbooks.itmo.ru/ru/lib_book/7450/7450.pdf (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: Аудитории для проведения лекций: *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. *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) _____ Р.Н. Погорелов
(подпись) (Ф.И.О.)

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

Протокол №__1__ заседания кафедры от __27.08. 2024г.

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

Согласовано

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

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>