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

Основы информационной безопасности
(наименование дисциплины)

02.03.01 Математика и компьютерные науки
(код, наименование направления/специальности)

09.03.01 Информатика и вычислительная техника
(код, наименование направления/специальности)

10.05.03 Информационная безопасность автоматизированных систем
(код, наименование направления/специальности)

38.03.05 Бизнес-информатика
(код, наименование направления/специальности)

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

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

Алчевск, 2024

1 Цели и задачи изучения дисциплины

Цели дисциплины. Целью изучения дисциплины «Основы информационной безопасности» является формирование у обучающихся знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

Задачи изучения дисциплины:

– понимание сущности информационной безопасности и принципов организации защиты информации на предприятиях;

– выявление основных видов угроз информационной безопасности;

– применение программно-аппаратных средств для обеспечения информационной безопасности.

2 Место дисциплины в структуре ОПОП ВО

Логико-структурный анализ дисциплины – курс входит в обязательную часть БЛОКА 1 «Дисциплины (модули)» по направлениям 02.03.01 Математика и компьютерные науки, 09.03.01 Информатика и вычислительная техника, 38.03.05 Бизнес-информатика, и специальности 10.05.03 Информационная безопасность автоматизированных систем.

Дисциплина реализуется кафедрой интеллектуальных систем и информационной безопасности.

Основывается на базе дисциплин: «Информатика».

Является основой для изучения следующих дисциплин: «Физические основы построения технических средств защиты информации», «Безопасность систем баз данных», «Безопасность операционных систем», «Безопасность сетей ЭВМ», а также, приобретенные знания, могут быть использованы при подготовке и защите выпускной квалификационной работы, при прохождении преддипломной практики, а также в профессиональной деятельности.

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения профессиональных задач деятельности, связанных с дисциплинами: «Физика», «Информатика», «Основы программирования».

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

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

Дисциплина изучается на 2 курсе в 3 семестре. Форма промежуточной аттестации – зачет.

3 Перечень результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП ВО

Процесс изучения дисциплины «Основы информационной безопасности» направлен на формирование компетенции, представленной в таблице 1.

Таблица 1 – Компетенции, обязательные к освоению

Код	Наименование специальности, направления подготовки	Компетенция (код, содержание)	Индикатор (код, наименование)
02.03.01	Математика и компьютерные науки	ОПК-5 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-5.1. Знает основные принципы работы современных информационных технологий.
09.03.01	Информатика и вычислительная техника	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.3. Применяет знания в области безопасности баз данных и программных комплексов
10.05.03	Информационная безопасность автоматизированных систем	ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-1.4. Оценивает значение информационной безопасности для обеспечения объективных потребностей личности, общества и государства ОПК-5.1. Применяет нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации
38.03.05	Бизнес-информатика	ОПК-2 Способен проводить исследование и анализ рынка информационных систем и информационно-коммуникационных технологий, выбирать рациональные решения для управления бизнесом	ОПК-2.1. Осуществляет анализ рынка информационно-коммуникационных технологий

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
		3
Аудиторная работа, в том числе:	36	36
Лекции (Л)	18	18
Практические занятия (ПЗ)	18	18
Лабораторные работы (ЛР)	–	–
Курсовая работа/курсовой проект	–	–
Самостоятельная работа студентов (СРС), в том числе:	36	36
Подготовка к лекциям	5	5
Подготовка к лабораторным работам	–	–
Подготовка к практическим занятиям / семинарам	9	9
Выполнение курсовой работы / проекта	–	–
Расчетно-графическая работа (РГР)	–	–
Реферат (индивидуальное задание)	–	–
Домашнее задание	6	6
Подготовка к контрольным работам	–	–
Подготовка к коллоквиуму	–	–
Аналитический информационный поиск	4	4
Работа в библиотеке	4	4
Подготовка к экзамену (зачету)	8	8
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 6 тем:

– тема 1 (Основные понятия информационной безопасности);

– тема 2 (Организационно-правовая защита информации);

– тема 3 (Общеметодологические принципы теории информационной безопасности);

– тема 4 (Уязвимости и угрозы информационной безопасности);

– тема 5 (Техническая защита информации);

– тема 6 (Защита информации в компьютерных сетях).

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	Основные понятия информационной безопасности	Исторические аспекты возникновения и развития информационной безопасности. Актуальность проблем информационной безопасности. Основные термины и определения в области информационной безопасности. Аспекты информационной безопасности. Понятие комплексной защиты информации	2	Основные термины и определения в области информационной безопасности. Понятие комплексной защиты информации	2	–	–
2	Организационно-правовая защита информации	Государственная система защиты информации. Основные законодательные акты в области информационной безопасности. Меры ответственности за нарушения в области информационной безопасности. Основные регуляторы в области информационной безопасности. Основные нормативные и методических документы ФСТЭК и ФСБ РФ в области обеспечения защиты конфиденциальной информации, в том числе персональных данных. Организационные методы защиты информации. Понятие политики информационной безопасности. Понятие объекта информатизации и его аттестации. Понятие лицензирования, стандартизации и сертификации в области информационной безопасности	4	Основные законодательные акты в области информационной безопасности. Примеры нормативных и методических документов ФСТЭК и ФСБ РФ в области обеспечения защиты конфиденциальной информации, в том числе персональных данных. Понятие аттестации объекта информатизации. Понятие лицензирования, стандартизации и сертификации в области информационной безопасности.	4	–	–

Продолжение таблицы 3

1	2	3	4	5	6	7	8
3	Общеметодологические принципы теории информационной безопасности	Комплексность. Этапы развития информационной безопасности: Системы безопасности ресурса; Этап развитой защиты; Этап комплексной защиты. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Комплексность: целевая, инструментальная, структурная, функциональная, временная	2	Комплексность. Этапы развития информационной безопасности: Системы безопасности ресурса. Этап развитой защиты. Этап комплексной защиты. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Комплексность: целевая, инструментальная, структурная, функциональная, временная.	2	–	–
4	Уязвимости и угрозы информационной безопасности	Уязвимости информационной безопасности. Угрозы информационной безопасности. Понятие защиты информации от несанкционированного доступа. Понятие риск-ориентированного подхода к обеспечению информационной безопасности. Понятие моделирования угроз информационной безопасности	2	Уязвимости информационной безопасности. Угрозы информационной безопасности. Понятие защиты информации от несанкционированного доступа. Понятие риск-ориентированного подхода к обеспечению информационной безопасности. Понятие моделирования угроз информационной безопасности	4	–	–

Завершение таблицы 3

1	2	3	4	5	6	7	8
5	Техническая защита информации	Понятие инженерно-технической защиты информации. Технические каналы утечки информации. Понятие и классификация визуально-оптических каналов утечки информации. Понятие и классификация каналов утечки акустической (речевой) информации. Понятие материально-вещественных каналов утечки информации. Понятие и классификация радиоэлектронных каналов утечки информации. Криптографические методы защиты информации. Системы шифрования. Понятие симметричной системы шифрования. Понятие асимметричной системы шифрования. Понятие электронной подписи	4	Понятие и классификация визуально-оптических каналов утечки информации, каналов утечки акустической (речевой) информации. Понятие и классификация радиоэлектронных каналов утечки информации. Понятие симметричной системы шифрования. Понятие асимметричной системы шифрования. Понятие электронной подписи	4	–	–
6	Защита информации в компьютерных сетях	Понятие компьютерных сетей. Защита информации на компьютерах. Защита информации в локальных и глобальных сетях. Понятие системы защиты информации. Основные принципы построения систем защиты информации. Основные подсистемы обеспечения информационной безопасности. Понятие программно-аппаратных средств обеспечения информационной безопасности. Понятие критической информационной инфраструктуры. Понятие центров мониторинга и управления безопасностью	4	Понятие СЗИ. Основные принципы построения систем ЗИ. Основные подсистемы обеспечения ИБ. Понятие программно-аппаратных средств обеспечения ИБ. Понятие центров мониторинга и управления безопасностью	2	–	–
Всего аудиторных часов		18		18		–	

6 Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины

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 работ по дисциплине и способы оценивания знаний приведены в таблице 4.

Таблица 4 – Перечень работ по дисциплине и способы оценивания знаний

Вид учебной работы	Способ оценивания	Количество баллов
Домашнее задание	Предоставление отчета	24 - 40
Работа на практических занятиях	Предоставление рабочих записей	18 - 30
Итоговое тестирование	Проверка тестов	18 - 30
Итого	–	60 - 100

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 «Основы информационной безопасности» 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. 6.5), 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 Домашние задания

Индивидуальное домашнее задание имеет целью более углубленное изучение одного из направлений в рамках информационной безопасности.

Оформляется в виде реферата. Перечень тем, для выполнения ИДЗ представлен ниже.

1. Порядок подготовки документов к открытой печати, с учетом требований к информации ограниченного доступа.

2. Электронная подпись. Технология ЭЦП.

3. Международные документы и стандарты в области информационной безопасности.

4. Методы борьбы с утечкой информации по визуально-оптическим каналам.

5. Методы борьбы с утечкой информации по акустическим (речевым) каналам.

6. Методы борьбы с утечкой информации по радиоэлектронным (электромагнитным) каналам.

7. Методы борьбы с утечкой информации по радиоэлектронным (электрическим) каналам.

8. Основные свойства информации. Важность, полнота, адекватность, релевантность.

9. Физическая защита информационных систем.

10. Характеристика программно-аппаратных средств защиты информации (не рассматриваемых в курсе дисциплины).

11. Этапы создания систем защиты информации.

12. Защита информации. Основные принципы обеспечения информационной безопасности.

13. Информация. Виды информации, свойства и понятие информации в контексте информационной безопасности.

14. Антивирусы и антивирусная защита. Классификация вредоносных программ.

15. Межсетевые экраны и методы создания защищенных систем, включающих межсетевые экраны.

16. Особенности защиты различных операционных систем.

17. Аппаратные средства защиты информации.

18. Протоколы PPP, SMTP, FTP и методы создания защищенного обмена.

19. Обеспечение безопасности при работе с электронной почтой.

20. Резервирование информации. Средства создания резервных копий.

21. Применение криптографических методов для защиты информации.

22. Физическое разрушение информационных систем и методы защиты от физического воздействия.

23. Троянские кони, люки и технология салями.

24. Технология VPN. Построение защищенных каналов связи.

25. Сертификаты. Протокол HTTPS. Центры сертификации.

26. Социальная инженерия как способ мошенничества в киберпространстве.

27. Популярные способы мошенничества в киберпространстве.

6.3 Темы для рефератов (презентаций) – индивидуальное задание

Не предусмотрены.

6.4 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Не предусмотрены.

6.5 Вопросы для подготовки к зачету

1) Что такое информация, информационная безопасность, защита информации, конфиденциальная информация?

2) Как классифицируется информация?

3) Что такое утечка информации?

4) Каким образом классифицируются каналы утечки информации?

5) В чем состоит актуальность проблем информационной безопасности?

6) Каковы правовые понятия в области защиты информации?

7) Какие методы защиты информации, использовавшиеся в древнее время и в Средние века Вам известны?

8) В чем, на Ваш взгляд, заключаются основные трудности обеспечения информационной безопасности в настоящее время?

9) В каких направлениях идет развитие теории информационной безопасности в настоящее время?

10) С чем связан возросший интерес к проблемам защиты информации?

11) Каков вклад российских ученых в теорию информационной безопасности?

12) Что такое конфиденциальность, целостность, доступность?

13) Что такое информационная система? Телекоммуникационная система? Автоматизированная система?

14) Каковы основные принципы построения систем защиты информации?

15) Что такое комплексный подход к обеспечению информационной безопасности?

16) Каковы основные задачи защиты информации?

17) Каковы основные средства реализации комплексной системы защиты информации?

18) Что такое морально-этические средства защиты информации?

19) Что такое центры информационной безопасности и какова их роль в развитии теории и практики защиты информации?

20) Перечислите основные носители информации, особенности их использования и защиты.

21) Какими свойствами определяется ценность информации?

22) Что понимается под информационными ресурсами?

23) Какие существуют виды тайны?

24) Какое назначение имеет перечень конфиденциальных сведений предприятия?

25) Что не разрешается относить к информации ограниченного доступа?

26) Каково место информационной безопасности в системе национальной безопасности Российской Федерации?

27) Какова структура государственной системы защиты информации?

28) Кто несет ответственность за нарушение режима защиты информации?

29) Каковы функции руководителей предприятий при организации защиты информации?

30) Каковы основные функции ФСТЭК?

31) Какие основные положения Доктрины информационной безопасности приняты в РФ?

32) Для каких систем (приведите примеры) наибольшую опасность представляет нарушение целостности информации?

33) В каких системах на первом месте стоит обеспечение доступности информации?

34) В чем различие понятий «нарушение конфиденциальности информации», «несанкционированный доступ к информации», «утечка информации»?

35) В чем отличие терминов «НСД» и «Нарушение конфиденциальности информации»?

36) Каким образом следует выбирать меры защиты конфиденциальности информации?

37) В чем разница между понятиями идентификации и аутентификации пользователя?

38) Какой из способов аутентификации Вы считаете наиболее эффективным? Почему?

39) Какие основные методы контроля доступа используются в известных вам информационных системах? В чем их достоинства и недостатки?

40) Почему аутентификация с использованием пароля считается в настоящее время ненадежной?

41) Каковы методы аутентификации с использованием предметов заданного типа?

42) Поясните, что понимается под понятием – совершенный шифр?

43) Почему большинство современных шифрограмм могут быть однозначно дешифрованы?

44) Каким образом государство регулирует использование средств криптозащиты?

45) Каковы способы контроля целостности потока сообщений?

46) Какие существуют способы контроля целостности сообщений при взаимном доверии сторон?

47) Как контролировать целостность сообщений при высоком уровне помех в каналах связи?

48) Как организован обмен документами, заверенными цифровой подписью?

49) В чем отличие и сходство обычной и цифровой подписей?

50) Какими принципами нужно руководствоваться для сохранения целостности данных при их обработке?

51) Почему проблемы контроля целостности данных относятся к проблемам информационной безопасности?

52) Что означает контроль целостности данных на уровне содержания?

53) Как обеспечить целостность данных при их хранении?

54) Что такое надежность и чем отличается надежность аппаратуры от надежности программного обеспечения?

55) Следует ли различать защиту от случайных угроз и от действий злоумышленника при обеспечении беспрепятственного доступа к информации?

56) Как защитить программное обеспечение от изучения логики его работы?

57) Как изменяется надежность аппаратуры с течением времени?

58) Каковы способы повышения надежности аппаратуры и линий связи?

59) Что из себя представляет матрица доступа?

60) Что из себя представляет граф доступа?

61) Что такое политика безопасности, кто ее разрабатывает и где она применяется?

62) Приведите классификацию моделей разграничения доступа. Какова их роль в теории информационной безопасности?

63) Каковы основные достоинства и недостатки дискреционных моделей?

64) Что такое монитор безопасности и какие требования к нему предъявляются?

65) Перечислите основные положения субъектно-объектного подхода к разграничению доступа? В чем достоинства и недостатки такого подхода?

66) В чем суть мандатной политики разграничения доступа?

67) Каковы основные достоинства и недостатки мандатной политики?

68) Что такое скрытые каналы утечки информации и как их обнаружить?

69) Почему ролевая политика получила большое распространение?

70) В чем суть моделей группового доступа?

71) Что такое информационная невыводимость и информационное невмешательство?

72) Как и зачем строятся многоуровненвые схемы разграничения доступа?

73) Чем отличаются понятия «информационная война» и «информационное противоборство»?

74) Какие виды информационных войн Вы можете выделить?

75) Можно ли рассматривать рекламу как средство ведения информационной борьбы?

76) Что такое информационное оружие?

77) Какие виды оружия применяются в ходе ведения информационной войны?

78) Каковы цели информационной войны?

79) Каковы средства и методы защиты от информационно-технического оружия?

80) Каковы особенности информационно-психологической войны?

81) Что такое аттестация объекта автоматизации?

82) Что такое сертификация средств защиты информации?

83) Что такое лицензирование деятельности в области защиты информации?

84) Что представляет из себя риск-ориентированный подход при обеспечении информационной безопасности?

85) Какие технические каналы утечки информации Вы знаете?

86) Какие криптографические методы обработки информации используются в области информационной безопасности?

87) Что такое симметричная система шифрования, ее достоинства и недостатки?

88) Что такое асимметричная система шифрования, ее достоинства и недостатки?

89) Какие известны основные принципы построения систем защиты информации?

90) Какие известны подсистемы обеспечения информационной безопасности?

91) Что такое центр мониторинга и управления безопасностью?

6.6 Примерная тематика курсовых работ

Не предусмотрено учебным планом.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. 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. – 15 экз.

2. Сухостат В.В. Основы информационной безопасности: учебное пособие / В.В. Сухостат, И.Н. Васильева. – СПб. : Изд-во СПбГЭУ, 2019. – 103 с. Режим доступа: https://infosec.spb.ru/wp-content/uploads/2020/06/osnovy-informaczionnoj-bezopasnosti.pdf (Дата обращения 10.05.2024).

3. Родичев Ю.А. Информационная безопасность. Национальные стандарты Российской Федерации: учебное пособие для студентов, обучающихся по программам высшего образования / Ю. А. Родичев. – Москва [и др.] : Питер, 2019. – 304 с. Режим доступа: https://chitat-online.org/str/informacionnaya-bezopasnost-nacionalnye-standarty-rossiyskoy (Дата обращения 10.05.2024).

4. Вострецова Е.В. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова. – Екатеринбург : Изд-во Урал. ун-та, 2019. – 204 с. Режим доступа: https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf (Дата обращения 10.05.2024).

5. Гродзенский Я.С. Информационная безопасность: учебное пособие / Я. С. Гродзенский. - Москва : Проспект, 2021. - 142 с. Режим доступа: https://knigogid.ru/books/1582163-informacionnaya-bezopasnost-nacionalnye-standarty-rossiyskoy-federacii/toread/fragment (Дата обращения 10.05.2024).

Дополнительная литература

1. Михнев И.П. Информационная безопасность: учебное пособие / И.П. Михнев. – Волгоградский институт управления – филиал ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации». – Волгоград: Изд-во Волгоградского института управления – филиала РАНХиГС, 2019. Режим доступа: https://docs.vlgr.ranepa.ru/podr/ipc/elizd/Михнев.pdf (Дата обращения 10.05.2024).

2. Карасева Э.М. Основы информационной безопасности: Учебное пособие /Э.М. Карасева, О.В. Рак.– Костанайский филиал «ЧелГУ», Костанай, 2019.–90 с. Режим доступа: https://csukz.ru/nir/nui/2019/Учебное%20пособие%20Карасевой%20Э.М.,%20Рак%20О.В..pdf (Дата обращения 10.05.2024).

Учебно-методическое обеспечение

Проходит апробацию. Режим доступа: https://moodle.dstu.education/course/view.php?id=2357

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: Аудитория 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.	ауд. *207* корп.*4*
Компьютерные классы (22 посадочных места), оборудованный учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС: ПК – 11шт.; Интерактивная доска– 1 шт. ПК - 11 шт.; Доска– 1 шт.	ауд. *208* корп. *4* 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 ИСИБ от 27.08.2024г.

И.о. декана факультета
информационных технологий и
автоматизации производственных
процессов

(подпись) В.В Дьячкова
Ф.И.О.)

Согласовано

Председатель методической
комиссии по направлению подготовки
02.03.01 Математика и
компьютерные науки

(подпись) А.Н. Баранов
(Ф.И.О.)

Председатель методической
комиссии по направлению подготовки
09.03.01 Информатика и
вычислительная техника

(подпись) Е.Е. Бизянов
(Ф.И.О.)

Председатель методической
комиссии по специальности
10.05.03 Информационная безопасность
автоматизированных систем

(подпись) Е.Е. Бизянов
(Ф.И.О.)

Председатель методической
комиссии по направлению подготовки
38.03.05 Бизнес-информатика

(подпись) Н.Н. Лепило
(Ф.И.О.)

Начальник учебно-методического центра

(подпись О.А.Коваленко
Ф.И.О.)

Лист изменений и дополнений

Номер изменения, дата внесения изменения, номер страницы для внесения изменений	
ДО ВНЕСЕНИЯ ИЗМЕНЕНИЙ:	ПОСЛЕ ВНЕСЕНИЯ ИЗМЕНЕНИЙ:
Основание:	
Подпись лица, ответственного за внесение изменений	