

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Вишневский Дмитрий Александрович
Должность: Ректор
Дата подписания: 30.04.2025 11:55:50
Уникальный программный ключ:
03474917c4d012283e5ad996a48a5e70bf8da057

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



Д.В. Мулов

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Управление информационной безопасностью

(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 «Управление информационной безопасностью» является изучение методов и средств управления информационной безопасностью (ИБ) в организации, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью (СУИБ) определенного объекта.

Задачи изучения дисциплины. Привитие обучающимся основ культуры обеспечения информационной безопасности, формирование понимания роли процессов управления в обеспечении информационной безопасности организаций, объектов и систем, ознакомление с основными методами управления информационной безопасностью организаций, объектов и систем, обучение различным методам реализации процессов управления информационной безопасностью, направленных на эффективное управление ИБ конкретной организации.

Дисциплина направлена на формирование общепрофессиональных (ОПК-15) 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 операционных систем», «Безопасность сетей ЭВМ», «Программно-аппаратные средства защиты информации», «Информационная безопасность открытых информационных систем».

Является основой для изучения следующих дисциплин: «Интеллектуальные системы информационной безопасности». 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 информационной безопасностью.

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

Общая трудоемкость освоения дисциплины составляет 5 зачетных единиц, 180 ак.ч. Программой дисциплины предусмотрены лекционные (18 ак.ч.), лабораторные (36 ак.ч.), практические (36 ак.ч) занятия в том числе курсовая работа, самостоятельная работа студента (90 ак.ч.).

Дисциплина изучается на 5 курсе в 10 семестре. Форма промежуточной аттестации – экзамен, курсовая работа – дифференцированный зачет.

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

Процесс изучения дисциплины «Управление информационной безопасностью» 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 администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ОПК-15	ОПК-15.2 Осуществляет администрирование и контроль функционирования систем защиты информации автоматизированных систем

4 Объём и виды занятий по дисциплине

Общая трудоёмкость учебной дисциплины составляет 5 зачётных единиц, 180 ак.ч.

Самостоятельная работа студента (СРС) включает проработку материалов лекций, подготовку к практическим занятиям, текущему контролю, выполнение индивидуального задания, самостоятельное изучение материала, подготовку к экзамену и дифференцированному 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
		10
Аудиторная работа, в том числе:	90	90
Лекции (Л)	18	18
Практические занятия (ПЗ)	18	18
Лабораторные работы (ЛР)	36	36
Курсовая работа/курсовой проект	18	18
Самостоятельная работа студентов (СРС), в том числе:	90	90
Подготовка к лекциям	4	4
Подготовка к лабораторным работам	14	14
Подготовка к практическим занятиям / семинарам	18	18
Выполнение курсовой работы / проекта	18	18
Расчетно-графическая работа (РГР)	-	-
Реферат (индивидуальное задание)	-	-
Домашнее задание	-	-
Подготовка к контрольным работам	-	-
Подготовка к коллоквиуму	-	-
Аналитический информационный поиск	-	-
Работа в библиотеке	-	-
Подготовка к экзамену (диф.зачету)	36	36
Промежуточная аттестация – экзамен (Э), диф.зачет (ДЗ)	Э, ДЗ	Э, ДЗ
Общая трудоемкость дисциплины		
ак.ч.	180	180
з.е.	5	5

5 Содержание дисциплины

С целью освоения компетенций, приведенных в п.3 дисциплина разбита на такие темы:

- тема 1 (Введение. Стандартизация в сфере управления ИБ);
- тема 2 (Политика ИБ);
- тема 3 (Аудит ИБ АС);
- тема 4 (Программные средства поддержки процессов управления ИБ).

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	Введение. Стандартизация в сфере управления ИБ	Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Основные понятия и определения. Содержание и задачи процесса управления ИБ АС и предприятия в целом. Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии. Стандартизация в сфере управления ИБ. Ресурсы предприятия, подлежащие защите с точки зрения ИБ. Комплекс методов и средств защиты информации как объект управления ИБ.	4	Концептуальная модель информационной безопасности организации. Построение подсистемы информационной безопасности	2	Инвентаризация активов, подлежащих защите. Составление регламента работ по созданию комплексной системы защиты информации в информационно-телекоммуникационных системах организации.	4

Продолжение таблицы 3

	2	3	4	5	6	7	8
2	Политика ИБ	Назначение и содержание политики ИБ предприятия в целом, его структурных подразделений, частных политик безопасности. Средства их реализации.. Состав, роль, место и особенности взаимодействия субъектов процесса управления ИБ АС. Планирование, мотивация и контроль выполнения персоналом требований документов по защите информации в организации.	4	Организационная структура системы обеспечения безопасности информации. Служба защиты информации (СЗИ). Функции, задача, ответственность, штатная структура СЗИ	4	Организация защиты компьютерной сети от несанкционированного доступа.	4
3	Аудит ИБ АС	Назначение, цели и виды аудита ИБ АС. Требования к аудитору ИБ, особенности взаимодействия между аудитором и заказчиком. Оценка работы аудитора. Стандартизация в сфере аудита ИБ. Содержание и организация процесса аудита ИБ. Оценка рисков ИБ. Отчетные документы по результатам аудита. Выполнение рекомендаций по итогам проведения аудита ИБ.	4	Политики управления защитой информации в информационно-телекоммуникационных системах. Стандарты в области управления, оценки и аудита ИБ. Процессная модель управления ИБ	2 2	Аудиторская проверка информационной безопасности в организации. Использование инструментов оценки рисков и управления рисками информационной безопасности.	8 4

Завершение таблицы 3

1	2	3	4	5	6	7	8
4	Программные средства поддержки процессов управления ИБ	Выбор необходимых программных и программно-аппаратных средств защиты информации в АС, проектирование комплексной системы защиты информации предприятия эффективной с точки зрения решаемых задач и необходимых для этого ресурсов. Программные средства автоматизации процедур проведения аудита ИБ и анализа политики ИБ. Программные средства поддержки процессов управления ИБ.	6	Методы оценки рисков информационной безопасности. Оценка информационных рисков с использованием методов системного анализа. Средства анализа защищенности информационно-телекоммуникационных систем. Выявление атак и управление информационным и рисками.	6 2	Использование инструментальных средств для выявления уязвимостей и отражения атак Организация проведения экспертизы систем защиты информации в информационно-телекоммуникационных системах	4 8
Всего аудиторных часов		18		18		36	

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

6.1 Критерии оценивания

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

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

Таблица 4 – Перечень компетенций по дисциплине и способы оценивания знаний

Код и наименование компетенции	Способ оценивания	Оценочное средство
ОПК-15	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.

По курсовой работе в семестре студент может набрать 100 баллов, в том числе:

- выполнение курсовой работы – 40 баллов;
- оформление курсовой работы – 10 баллов;
- защита курсовой работы – 50 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 «Управление информационной безопасностью» 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. 6.4), 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 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Тема 1 (Введение. Стандартизация в сфере управления ИБ)

- 1) Какие задачи ставятся для процесса управления ИБ АС и предприятия в целом?
- 2) В чем заключается системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии?
- 3) С какой целью производится стандартизация в сфере управления ИБ?
- 4) Какие ресурсы предприятия, подлежат защите с точки зрения ИБ?
- 5) Какие комплексы методов и средств защиты информации могут быть определены как объект управления ИБ?

Тема 2 (Политика ИБ)

- 1) В чем заключается политика ИБ предприятия в целом?
- 2) В чем заключается политика ИБ структурных подразделений предприятия?
- 3) Какие средства реализации политик информационной безопасности предприятия и его структурных подразделений Вы можете назвать?
- 4) Определите состав, роль, место и особенности взаимодействия субъектов процесса управления ИБ АС?
- 5) С какой целью производится планирование, мотивация и контроль выполнения персоналом требований документов по защите информации в организации?

Тема 3 (Аудит ИБ АС)

- 1) В чем заключается цели аудита ИБ АС?
- 2) Какие виды аудита ИБ АС Вы знаете?
- 3) Какие требования предъявляются к аудитору ИБ?
- 4) В чем заключаются особенности взаимодействия между аудитором и заказчиком?
- 5) Как производится оценка рисков ИБ?

Тема 4 (Программные средства поддержки процессов управления ИБ)

- 1) На основании каких критериев производится выбор необходимых программных средств защиты информации в АС?
- 2) На основании каких критериев производится выбор необходимых программно-аппаратных средств защиты информации в АС?
- 3) В соответствии с какими требованиями производится проектирование комплексной системы защиты информации предприятия, эффективной с точки зрения решаемых задач и необходимых для этого ресурсов?
- 4) Какие программные средства автоматизации процедур проведения аудита ИБ и анализа политики ИБ Вы знаете?
- 5) Какие программные средства поддержки процессов управления ИБ Вы знаете?

6.4 Вопросы для подготовки к экзамену

- 1) Почему информационная безопасность - одна из важнейших проблем современной жизни?
- 2) Что понимается под системой безопасности?
- 3) Какие вопросы, касающиеся информационной безопасности, содержатся в Конституции РФ?
- 4) Что такое информационная система?
- 5) Какие структурные компоненты информационных систем Вы знаете?
- 6) Что понимают под информационными ресурсами и процессами?
- 7) Какие основные компоненты концептуальной модели ИБ Вы знаете?
- 8) Как выглядит графическая схема концептуальной модели системы ИБ?
- 9) Какие вопросы, касающиеся информационной безопасности, содержатся в Гражданском кодексе РФ?
- 10) Какая информация является предметом защиты?
- 11) Какие основные свойства информации как предмета защиты Вы знаете?
- 12) По каким критериям определяется секретная и конфиденциальная информация?
- 13) Что такое объекты угроз ИБ?
- 14) В чем выражаются угрозы информации?
- 15) Каковы основные источники угроз защищаемой информации?
- 16) Каковы цели угроз информации со стороны злоумышленников?
- 17) Какие статьи Уголовного кодекса напрямую касаются информационной безопасности?
- 18) Что такое признаковая информация?

- 19) Почему семантическая информация по отношению к признаковой является вторичной?
- 20) Какие признаки объектов являются демаскирующими?
- 21) Какие основные способы неправомерного овладения конфиденциальной информацией Вы знаете?
- 22) Какие основные понятия рассматриваются в Законе РФ "Об информации, информатизации и защите информации"?
- 23) Что такое «источник конфиденциальной информации»?
- 24) Какие основные источники конфиденциальной информации Вы знаете?
- 25) Какие основные способы НСД к конфиденциальной информации Вы знаете?
- 26) Что из себя представляет обобщенная модель взаимодействия способов НСД источников конфиденциальной информации?
- 27) Для чего проводится лицензирование?
- 28) Кто такие лицензиат и лицензирующие органы?
- 29) Почему лицензирование и сертификация выступают в качестве средства защиты информации?
- 30) На какие виды деятельности, касающихся ИБ, на осуществление которых требуются лицензии?
- 31) Что такое утечка конфиденциальной информации?
- 32) Как осуществляется утечка конфиденциальной информации?
- 33) Какие Вам известны американские законы, напрямую связанные с ИБ?
- 34) Что можно сказать о законодательстве ФРГ по вопросам ИБ?
- 35) Что такое защита информации?
- 36) Определите понятие «несанкционированный доступ» к конфиденциальной информации, как он реализуется?
- 37) Какие недостатки российского законодательства, на Ваш взгляд, необходимо устранять в первую очередь?
- 38) Какие действия определяют угрозы конфиденциальной информации?
- 39) Что такое атака? Что такое окно опасности? Какие события происходят во время существования окна опасности?
- 40) Что понимается под политикой безопасности?
- 41) Что такое угрозы утечки информации?
- 42) Какие угрозы называются преднамеренными и случайными?
- 43) Что такое программа безопасности, ее уровни?
- 44) Что такое канал НСД?
- 45) Что такое управление рисками?

46) Почему управление рисками рассматривается на административном уровне ИБ?

47) В чем заключается суть мероприятий по управлению рисками?

48) В чем заключается основная специфика процедурного уровня ИБ?

49) Почему вопросы поддержания работоспособности ИС являются принципиальными на процедурном уровне ИБ?

50) В чем специфика деятельности Межведомственной комиссии по защите государственной тайны?

51) Что такое канал утечки информации?

52) Что такое технический канал утечки информации?

53) В чем специфика деятельности ФСТЭК России?

54) Что такое источник угроз безопасности информации?

55) Почему уровень ИБ в России в настоящее время не соответствует жизненно важным потребностям личности, общества и государства и какие ключевые проблемы необходимо решить безотлагательно, чтобы обеспечить достаточный уровень ИБ в России?

56) Какие аспекты современных ИС с точки зрения безопасности наиболее существенны?

57) Что такое вредоносное программное обеспечение? Дайте определение «бомбы», «червя», «вируса». Какие негативные последствия в функционировании ИС вызывает вредоносное ПО?

58) Что такое идентификация?

59) Какие меры позволяют повысить надежность парольной защиты?

60) Что такое государственная тайна?

61) В чем заключается основная задача логического управления доступом?

62) Что такое матрица доступа?

63) Какая информация анализируется при принятии решения о предоставлении доступа?

64) Каким требованиям должна отвечать коммерческая тайна?

65) Какая информация не может быть отнесена к коммерческой тайне?

66) Что такое защита от разглашения?

67) Что такое протоколирование?

68) Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к профессиональной тайне?

69) В чем заключается основная задача аудита, как сервиса безопасности?

70) Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к служебной тайне?

71) Что такое firewall и как он функционирует?

- 72) Какие сведения могут быть отнесены к персональным данным?
- 73) Кто является держателем персональных данных?
- 74) Для каких целей служит сервис анализа защищенности?
- 75) В чем заключается специфика управления, как сервиса безопасности?

6.5 Тематика и содержание курсовой работы

Для обеспечения эффективного управления информационной безопасностью, спроектировать систему защиты информации. При проектировании системы защиты информации необходимо:

- изучить вопросы оценки классификации информационных систем и средств защиты информации требованиям безопасности;
- изучить подходы, методы и средства, необходимые для реализации и использования защиты информации;
- изучить теоретические основы анализа и синтеза систем защиты информации (СЗИ) корпоративных информационных систем и сетей;
- определить приемлемый для учреждения уровень риска, обеспечивающий ему выполнение своих задач;
- определить защищенность каждого ценного ресурса при помощи анализа угроз, действующих на конкретный ресурс, и уязвимостей, через которые данные угрозы могут быть реализованы;
- оценить вероятность реализации актуальных для ценного ресурса угроз и степень влияния реализации угрозы на ресурсы;
- научиться анализировать информационные риски ресурсов организации;
- научиться на заключительном этапе проводить анализ эффективности предложенных мероприятий по устранению выявленных уязвимостей.

При выполнении задания курсовой работы (согласно своего варианта) необходимо получить следующие данные:

- риск реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса;
- риск реализации суммарно по всем угрозам для ресурса;
- риск реализации по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы;
- риск реализации по всем угрозам для информационной системы;
- риск реализации по всем угрозам для информационной системы после проведения контрмер;
- эффективность контрмеры;
- эффективность комплекса контрмер.

Примерные темы курсовых работ:

- 1) Информационная система для обеспечения деятельности судоходной компании "Балтика".
- 2) Информационная система для Учреждения юстиции.
- 3) Информационная система для обеспечения деятельности малого научно-внедренческого предприятия "Квадро".
- 4) Информационная система для обеспечения деятельности ООО "Киновидеопрокат".
- 5) Информационная система для обеспечения деятельности предприятия LADA-сервис.
- 6) Информационная система для торгово-закупочной фирмы "Столица".
- 7) Информационная система для обеспечения деятельности отдела гарантийного ремонта товаров фирмы "Народная торговая компания".
- 8) Информационная система для обеспечения деятельности отдела учета домовладений Бюро технической инвентаризации.
- 9) Информационная система для обеспечения деятельности отдела учета квартир Бюро технической инвентаризации.
- 10) Информационная система для обеспечения деятельности отдела учета нежилых помещений Бюро технической инвентаризации.
- 11) Информационная система для обеспечения деятельности отдела учета налогообложения физических лиц городской налоговой инспекции.
- 12) Информационная система для обеспечения деятельности телеателье "Спектр".
- 13) Информационная система для обеспечения деятельности Государственной автомобильной инспекции по безопасности дорожного движения города.
- 14) Информационная система для ведения реестра имущества университетского городка.
- 15) Информационная система для обеспечения деятельности туристической компании "Вояж".
- 16) Информационная система для обеспечения деятельности регистратуры ведомственной поликлиники "Эскулап".
- 17) Информационная система для обеспечения деятельности рекламного агентства "Rapid".
- 18) Информационная система для обеспечения деятельности ООО "Центр оценки и продажи недвижимости".
- 19) Информационная система для обеспечения деятельности отдела вневедомственной охраны квартир.

20) Информационная система для обеспечения деятельности отдела приватизации жилья администрации города.

21) Информационная система для обеспечения деятельности Бюро технической инвентаризации по изготовлению и выдаче технических паспортов на объекты недвижимости.

22) Информационная система для обеспечения деятельности отдела аренды ЗАО "Сириус".

23) Информационная система для обеспечения деятельности телефонной компании.

24) Информационная система для обеспечения деятельности мелкооптового книжного магазина.

25) Информационная система для обеспечения деятельности ОАО "Автовокзал".

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. Чекулаева Е.Н. Управление информационной безопасностью: учебное пособие / Е.Н. Чекулаева, Е.С. Кубашева. — Йошкар-Ола: ПГТУ, 2020. — 154 с. — [Электронный ресурс]. — URL: <https://e.lanbook.com/book/157473> Режим доступа: для авториз. пользователей. (Дата обращения 26.08.2024).

2. Зырянова Т.Ю. Управление информационной безопасностью: учебное пособие / Т.Ю. Зырянова. — Екатеринбург: , 2023. — 96 с. — Текст: электронный // Лань : электронно-библиотечная система. — [Электронный ресурс] URL: <https://e.lanbook.com/book/369482> — Режим доступа: для авториз. пользователей. (Дата обращения 26.08.2024).

3. Давыдов А.И. Управление информационной безопасностью: учебное пособие / А.И. Давыдов, Д.А. Елизаров. — Омск: ОмГУПС, 2023. — 91 с. — — Текст : электронный // Лань : электронно-библиотечная система. — [Электронный ресурс] URL: <https://e.lanbook.com/book/419255> — Режим доступа: для авториз. Пользователей (Дата обращения 26.08.2024).

Дополнительная литература

1. Поздняк И.С. Управление информационной безопасностью: методические указания / И.С. Поздняк, И.С. Макаров. — Самара : ПГУТИ, 2019. — 43 с. — Текст : электронный // Лань : электронно-библиотечная система. — [Электронный ресурс] URL: <https://e.lanbook.com/book/223313> — Режим доступа: для авториз. пользователей (Дата обращения 26.08.2024).

2. Елизаров Д.А. Методы выявления нарушений информационной безопасности объектов информатизации: учебно-методическое пособие / Д.А. Елизаров, А.И. Давыдов, Т.А. Мызникова. — Омск: ОмГУПС, 2023. — 20 с. — Текст: электронный // Лань: электронно-библиотечная система. — [Электронный ресурс] URL: <https://e.lanbook.com/book/419261> — Режим доступа: для авториз. пользователей. (Дата обращения 26.08.2024).

3. Киреева Н.В. Практическое применение мер по защите конфиденциальной информации в работе с гражданами в учреждении по предоставлению и обработке персональных данных: учебное пособие / Н.В. Киреева, Л.Р. Чупахина, О.А. Караулова. — Самара: ПГУТИ, 2020. — 50 с. — Текст: электронный // Лань: электронно-библиотечная система. — [Электронный ресурс] URL: <https://e.lanbook.com/book/255440> — Режим доступа: для авториз. 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>.

Материально-техническое обеспечение представлено в таблице 6.

Наименование оборудованных учебных кабинетов	Адрес (местоположение) учебных кабинетов
Специальные помещения: <i>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.</i> Аудитории для проведения лекций: <i>Компьютерные классы (22 посадочных места), оборудованный учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС:</i>	ауд. <u>207</u> корп. <u>4</u> ауд. <u>217</u> корп. <u>3</u> ауд. <u>211</u> корп. <u>4</u>

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 кафедрыот 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
Информационная безопасность
автоматизированных систем


(подпись)

Е.Е. Бизянов
(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	