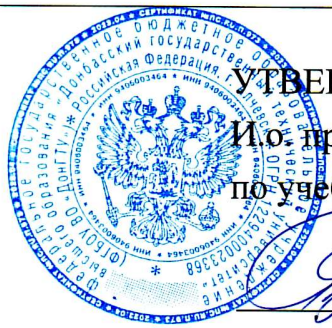
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБРНАУКИ РОССИИ)

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

Анализ рисков информационной безопасности
(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 «Анализ рисков информационной безопасности» является формирование у будущих специалистов теоретических знаний и практических навыков для решения научно-исследовательских и прикладных задач.

Задачи изучения дисциплины. Приобретение студентами знаний, умений и практических навыков, необходимых для понимания обеспечения информационной безопасности открытых информационных систем, освоения методов анализа и оценки рисков нарушения информационной безопасности, а также методов снижения уровня рисков и повышения уровня защищенности объекта защиты.

Дисциплина направлена на формирование общепрофессиональных (ОПК-6) компетенций выпускника.

2 Место дисциплины в структуре образовательной программы

Логико-структурный анализ дисциплины – курс входит в элективные дисциплины 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: «Сети и системы передачи информации», «Защита информации от утечки по техническим каналам», «Безопасность сетей ЭВМ».

Является основой для изучения следующих дисциплин: «Информационная безопасность открытых информационных систем», «Интеллектуальные системы информационной безопасности».

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения профессиональных задач деятельности, связанных с применением знаний в области информационной безопасности.

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

Общая трудоемкость освоения дисциплины составляет 5 зачетных единицы, 180 ак.ч. Программой дисциплины предусмотрены лекционные (36 ак.ч.), лабораторные (36 ак.ч.) занятия, самостоятельная работа студента (108 ак.ч.).

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

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

Процесс изучения дисциплины «Анализ рисков информационной безопасности» 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 при решении профессиональных задач организовать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6	ОПК-6.1 Решает профессиональные задачи по защите информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами

4 Объём и виды занятий по дисциплине

Общая трудоёмкость учебной дисциплины составляет 5 зачётных единицы, 180 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:	72	72
Лекции (Л)	36	36
Практические занятия (ПЗ)	-	-
Лабораторные работы (ЛР)	36	36
Курсовая работа/курсовой проект	-	-
Самостоятельная работа студентов (СРС), в том числе:	108	108
Подготовка к лекциям	9	9
Подготовка к лабораторным работам	18	18
Подготовка к практическим занятиям / семинарам	-	-
Выполнение курсовой работы / проекта	-	-
Расчетно-графическая работа (РГР)	30	30
Реферат (индивидуальное задание)	-	-
Домашнее задание	-	-
Подготовка к контрольным работам	-	-
Подготовка к коллоквиуму	-	-
Аналитический информационный поиск	18	18
Работа в библиотеке	18	18
Подготовка к зачету	15	15
Промежуточная аттестация – зачет (З)	З	З
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 5 тем:

– тема 1 (Анализ рисков в области информационной безопасности);

– тема 2 (Стандарты управления рисками);

– тема 3 (Технологии анализа рисков);

– тема 4 (Средства анализа рисков);

– тема 5 (Управление информационными рисками).

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	Анализ рисков в области информационной безопасности	Информационная безопасность. Проблемы обоснования стоимости корпоративной системы защиты информации. Службы информационной безопасности. Основные функции специалистов, ответственных за информационную безопасность. Основные этапы работы по обеспечению режима информационной безопасности. Постановка задачи анализа рисков. Национальные особенности защиты информации.		-	-	Табличные методы оценки и анализа информационных рисков Расчет рисков информационной безопасности	4 4
2	Стандарты управления рисками	Национальные стандарты управления рисками ИБ: ГОСТ Р ИСО/МЭК семейств 17799, 27000, 13335, 13569, 18044, 18045. Международные стандарты управления рисками: CobiT, ITIL, BSI, COSO, SAS70, NIST-800. Обзор основных стандартов. Ведомственные и корпоративные стандарты управления рисками ИБ		-	-	Исследование современных информационных рисков и их особенностей Исследование рисков различных информационных систем	4 4

Завершение таблицы 3

1	2	3	4	5	6	7	8
3	Технологии анализа рисков	Вопросы анализа рисков и управления ими. Идентификация рисков. Оценивание рисков. Качественные и количественные методики оценки рисков. Выбор допустимого уровня рисков. Выбор контрмер и оценка их эффективности. Разработка корпоративной методики анализа рисков.		-	-	Оценка угроз безопасности информации в технологии оценки рисков Применение технологий обработки рисков информационной безопасности	4 4
4	Средства анализа рисков	Инструментарии базового уровня. Средства полного анализа рисков. Комплекс оценки рисков «ГРИФ». Методики и инструменты CORAS, CRAMM, Babel Enterprise, RiskWatch. Экспертная система «АванГард».		-	-	Комплекс оценки рисков «ГРИФ» Экспертная система «АванГард»	4 4
5	Управление информационными рисками	Основные элементы управления рисками информационных систем. Система управления информационными рисками.		-		Методы и инструментальные средства управления рисками	4
Всего аудиторных часов		36		-		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-6	Зачет	Комплект контролирующих материалов для зачета

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

– расчетно-графическая работа (РГР) – всего 10 баллов;

– лабораторные работы – всего 90 баллов.

Оценка по зачету 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 «Анализ рисков информационной безопасности» 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 6 – 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) – индивидуальное задание

Тема: Разработка рекомендаций по информационной безопасности организации.

Цель: Разработать рекомендации по аудиту информационной безопасности предприятия.

Расчетно-графическая работа №1.
Тема: Аудиторский отчёт.

Расчетно-графическая работа №2.
Тема: Рекомендации по технической составляющей ИБ.

Расчетно-графическая работа №3.
Тема: Рекомендации по организационной составляющей ИБ.

Варианты организаций:

1) Компания имеет 5 представительств, все пять в разных странах (.ua, .ru и тд). Имеет 5 представительств в каждом от 50-100 чел. Головная компания 1000 чел в России. Отдел продаж в региональное представительство, административный отдел и отдел обработки данных. Направление деятельности компании - транснациональные грузовые перевозки.
2) Компания имеет одно представительство в России, которое является компанией, купленной годом ранее, занимающееся разработкой ПО. Головная компания до 500 чел. Представительство - до 300 чел. (Разные бренды). 2 домена – 2 бренда
3) Компания имеет головной офис со штатом 300 чел. Занимается продажей сотовых телефонов. По всей России 2000-3000 представительств – магазинах, есть упр. менеджер (локальный отд. продаж) и тарифный отдел и отд. логистики.
4) Компания – 100 чел. Сфера деятельности аутсорсинг, услуги администрирования различных систем на базе Microsoft. Клиенты в большинстве стран мира. Компания обеспечивает полную поддержку инфраструктуры клиента.
5) Компания состоит из 3-х филиалов на территории РФ. ЦО в Хабаровске. Численность ЦО 100 чел., в филиалах 20 чел. Занимается производством и разработкой средств аутентификации. Производство в филиалах, ЦО выполняет только административные действия.
6) Компания - холдинг с центральным офисом в г. Владивостоке. Занимается созданием и разработкой интернет сайтов и в неё входит ещё 4 компании, находящиеся в 4 странах мира. В каждой компании до 50 человек.

7) Компания имеет 10 представительств, пять в одной стране, пять в разных странах (.ua, .ru и тд). В каждом от 50-100 чел. Головная компания 1000 чел в России. Отдел продаж в региональное представительство, административный отдел и отдел обработки данных. Направление деятельности компании - транснациональные грузовые перевозки.

8) Компания имеет два представительства в России, которые являются компанией, купленной годом ранее, занимающееся разработкой ПО. Головная компания до 800 чел. Представительство - до 500 чел. (Разные бренды). 3 домена – 2 бренда.

9) Компания имеет головной офис со штатом 400 чел. Занимается продажей сотовых телефонов. По всей России 2000-3000 представительств – магазинах, есть упр. менеджер (локальный отд. продаж) и тарифный отдел и отд. логистики.

10) Компания – 200 чел. Сфера деятельности аутсорсинг, услуги администрирования различных систем на базе Microsoft. Клиенты в большинстве стран мира. Компания обеспечивает полную поддержку инфраструктуры клиента.

11) Компания состоит из 5-х филиалов на территории РФ. ЦО в Волгограде. Численность ЦО 100 чел., в филиалах 20 чел. Занимается производством и разработкой средств аутентификации. Производство в филиалах, ЦО выполняет только административные действия.

12) Компания - холдинг с центральным офисом в г. Воронеже. Занимается созданием и разработкой интернет сайтов и в неё входит ещё 3 компании, находящиеся в 3 странах мира. В каждой компании до 50 человек.

Изучить теоретические материалы. Сформировать матрицу рисков ИБ для ИС. Количественно оценить риски Предложить набор контрмер. Оформить отчет о проделанной работе. Исследовать методику оценки затрат на ЗИ в организации.

6.4 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Тема 1 (Анализ рисков в области информационной безопасности)

1) В чем заключается особенность корпоративной системы защиты информации?

2) Какие службы обеспечивают информационную безопасность организаций?

3) Какие задачи должны решать специалисты, ответственные за информационную безопасность?

4) Какие основные этапы работы по обеспечению режима информационной безопасности Вы знаете?

5) В чем заключаются национальные особенности защиты информации?

Тема 2 (Стандарты управления рисками)

1) О чем идет речь в национальных стандартах управления рисками информационной безопасности: ГОСТ Р ИСО/МЭК семейств 17799, 27000, 13335, 13569, 18044, 18045?

2) О чем идет речь в международных стандартах управления рисками: CobiT, ITIL, BSI, COSO, SAS70, NIST-800?

3) В чем отличие национальных и международных стандартов управления рисками информационной безопасности?

4) Какие основные стандарты управления рисками Вам известны?

5) В чем отличие ведомственных и корпоративных стандартов управления рисками информационной безопасности?

Тема 3 (Технологии анализа рисков)

1) В чем заключается процесс идентификации рисков?

2) В чем заключается процесс оценивания рисков?

3) Какие качественные и количественные методики оценки рисков Вы знаете?

4) Как производится выбор допустимого уровня рисков?

5) Как производится выбор контрмер и оценка их эффективности?

Тема 4 (Средства анализа рисков)

1) Какие инструментарии базового уровня Вы знаете?

2) Какие средства полного анализа рисков Вы знаете?

3) Какие задачи решает комплекс оценки рисков «ГРИФ»?

4) Чем отличаются методики и инструменты CORAS, CRAMM, Babel Enterprise и RiskWatch?

5) Какие задачи решает экспертная система «АванГард»?

Тема 5 (Управление информационными рисками)

1) Какие основные элементы управления рисками информационных систем Вам известны?

2) Что такое система управления информационными рисками?

3) Что содержит план управления рисками?

4) Из скольких уровней, в основном, состоит система управления информационными рисками?

5) Из каких уровней, в основном, состоит система управления информационными рисками?

6.5 Вопросы для подготовки к зачету

1) Что представляет собой менеджмент риска информационной безопасности?

2) В чем заключаются задачи менеджмента риска информационной безопасности?

3) Как взаимосвязаны основные этапы менеджмента риска информационной безопасности?

4) Что включает в себя этап установление контента?

5) Какие основные критерии, необходимы для менеджмента риска ИБ?

6) В чем заключается и какие этапы включает в себя оценка риска ИБ?

7) В чем заключается и какие этапы включает в себя анализ риска ИБ?

8) В чем заключается идентификация риска ИБ?

9) Из каких этапов состоит идентификация риска ИБ?

10) Что включает в себя идентификация активов?

11) Какие основные виды активов Вы знаете?

12) Что представляют собой требования безопасности для активов?

13) Что включает в себя реестр информационных активов?

14) Каким образом может быть определена ценность активов?

15) По каким критериям и соответствующим шкалам производится оценка возможного ущерба?

16) Что такое профиль и жизненный цикл угрозы?

17) По каким признакам классифицируются угрозы информационной безопасности?

18) Какими способами может быть выполнена оценка вероятности угроз информационной безопасности?

19) Какими способами может быть выполнена оценка уязвимостей?

20) Каким образом может быть получена количественная оценка риска информационной безопасности?

21) Что включает в себя реестр рисков информационной безопасности?

22) В чем заключается оценивание рисков информационной безопасности?

23) Какие существуют варианты обработки рисков информационной безопасности?

24) В чем заключается снижение риска информационной безопасности?

25) Какие способы снижения рисков Вы знаете?

26) Какие типичные ограничения должны быть учтены?

27) В чем заключается сохранение риска информационной безопасности?

28) Какие факторы влияют на решение о принятии рисков?

29) В чем заключается предотвращение риска информационной безопасности?

30) Какие основные способы предотвращения риска Вы знаете?

31) Что такое перенос риска информационной безопасности?

32) Какие задачи решаются в процессе коммуникации риска информационной безопасности?

33) Какие факторы подлежат мониторингу в процессе переоценки риска информационной безопасности?

34) Какова роль лица, принимающего решения, экспертов, консультантов в задачах принятия решений?

35) В чем заключается общая схема алгоритма экспертизы?

36) Каковы основные этапы экспертизы?

37) Каковы основные формы опроса экспертов, взаимодействия экспертов при опросе?

38) Каков алгоритм оценивания согласованности мнений экспертов?

39) Каковы методы формирования исходного множества альтернатив?

40) Что такое область компромиссов?

41) Что такое область согласия?

42) Что такое множество Парето?

43) Что такое множество эффективных решений?

44) Как выделяют область компромиссов?

45) Каковы признаки и свойства методов решения многокритериальных задач принятия решений?

46) Как производится классификация методов многокритериальной оценки альтернатив и методов решения многокритериальных задач принятия решений?

47) Что такое аксиоматические методы многокритериальной оценки альтернатив?

48) Какие принципы оптимальности используются в прямых методах многокритериальной оценки альтернатив?

49) Каковы основные приемы нормализации критериев?

50) Как определяется важность критериев?

51) Как выглядят структурные схемы методов порогов несравнимости?

52) К каким решениям могут приводить методов порогов несравнимости?

53) Как выглядит структурная схему метода аналитической иерархии?

54) Чем различаются задачи принятия решений при риске и при определенности?

55) В чем состоит неопределенность задачи принятия решений при риске?

56) В чем заключаются основные особенности однокритериальной модели принятия решений при риске?

57) В чем заключаются основные особенности многокритериальной модели принятия решений при риске?

58) В чем заключается неопределенность задачи принятия решений при риске?

59) Как преодолевается неопределенность задачи принятия решений при риске?

60) Возможно ли применение метода RA Software Tool для описание рисков в системах, обрабатывающих гостайну и почему?

61) Какой из методов управления рисками наиболее предпочтителен в национальной системе стандартов информационной безопасности и почему?

62) Какие существуют способы снижения рисков?

63) Что такое система управления рисками, её назначение?

64) Кто выполняет оценку риска?

65) Что такое профиль угрозы?

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. Аверченков В.И. Аудит информационной безопасности : учебное пособие для вузов // В.И. Аверченков. Москва: Издательство «Флинта», 2021. – 269с. – [Электронный ресурс]: – Режим доступа: https://biblioclub.ru/index.php?page=book_red&id=93245&sr=1 (Дата обращения 26.08.2024).

2. Тихомиров Н.П. Теория риска: учебник / Н.П. Тихомиров, Т.М. Тихомирова; Российский экономический университет им. Г.В. Плеханова. – Москва : Юнити-Дана, 2020. – 308 с.: ил., табл., граф. [Электронный ресурс]: – URL: https://biblioclub.ru/index.php?page=book&id=615777 – Режим доступа: для авторизованных пользователей (дата обращения: 26.08.2024).

Дополнительная литература

1. Ожиганова М.И. Организация и управление службой защиты информации: учеб. пособие / Сост. М.И. Ожиганова, А.Ю. Мордвинова. – Севастополь: СевГУ, 2019. – 156 с. [Электронный ресурс]: https://lib.sevsu.ru/xmlui/bitstream/handle/123456789/8887/%D1%80_190185.pdf?sequence=1&isAllowed=y (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 9.

Таблица 9 – Материально-техническое обеспечение

Наименование оборудованных учебных кабинетов	Адрес (местоположение) учебных кабинетов
Специальные помещения: *Мультимедийная аудитория. (60 посадочных мест)*, оборудованная специализированной (учебной) мебелью (скамья учебная –20 шт., стол– 1 шт., доска аудиторная– 1 шт.), учебное ПК (монитор + системный блок), мультимедийная стойка с оборудованием – 1 шт., широкоформатный экран. Аудитории для проведения лекций: *Компьютерные классы (22 посадочных места),* оборудованный учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС:	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 _____ Е.Е. Бизянов
(наименование кафедры) (подпись) (Ф.И.О.)

Протокол № 1 заседания кафедры от 27.08. 2024г.

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

Согласовано

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

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