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 информационных технологий

УТВЕРЖДАЮ
и.о. проректора по учебной работе
Д.В. Мулов

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Управление информационной безопасностью
(наименование дисциплины)

38.04.05 Бизнес-информатика
(код, наименование направления)

Бизнес-аналитика
(профиль подготовки)

Квалификация магистр
(бакалавр/специалист/магистр)

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

Алчевск, 2024

1 Цели и задачи изучения дисциплины

Цели дисциплины. Целями изучения дисциплины «Управление информационной безопасностью» является: формирование навыков организации и методологии обеспечения информационной безопасности в коммерческих организациях и организациях банковской системы РФ; создание представления о функциях, структурах и штатах подразделения информационной безопасности; об организационных основах, принципах, методах и технологиях и управлении информационной безопасностью в коммерческих организациях и организациях банковской системы РФ; развитие способностей по использованию существующей системы управления информационной безопасности.

Задачи изучения дисциплины:

– приобретение теоретических знания и практических навыков в методике построения и оценки уровня системы защиты информации;

– разработке стратегии обеспечения информационной безопасности и политики ее реализации, разграничении ответственности между подразделениями критически важных объектов,

– получение практических навыков управления информационной безопасностью в процессе мониторинга, реагирования на инциденты, аудите системы информационной безопасности на предприятии

Дисциплина направлена на формирование профессиональной компетенции (ПК-4) выпускника.

2 Место дисциплины в структуре ОПОП ВО

Логико-структурный анализ дисциплины – курс входит в БЛОК 1 «Дисциплины (модули)», обязательную часть подготовки студентов по направлению 38.04.05 Бизнес-информатика (профиль «Бизнес-аналитика»).

Дисциплина реализуется кафедрой информационной технологии. Основывается на базе дисциплин: «Технологии анализа данных и машинное обучение», «Управление информационной безопасностью», «Теория принятия решений», «Математические методы и модели рыночной экономики», «Актуарные расчеты», «Системно-динамическое моделирование», «Эффективность информационных систем», «Инженерия знаний и проектирование баз знаний», «Проектирование информационных систем».

Является основой для изучения следующих дисциплин: «Архитектура предприятия (продвинутый уровень), «Бизнес-анализ», «Производственная (технологическая) практика», «Производственная (преддипломная) практика», выпускная квалификационная работа.

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения профессиональных задач деятельности, связанных с управлением бизнес-процессами на предприятии.

Курс является фундаментом для ориентации студентов в сфере правового регулирования деятельности предприятий в сфере моделирования бизнес-процессов, электронный бизнес.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 ак.ч. Программой дисциплины предусмотрены лекционные (20 ак.ч.), практические (30 ак.ч.) занятия и самостоятельная работа студента (58 ак.ч.).

Дисциплина изучается на 1 курсе в 1 семестре. Форма промежуточной аттестации – экзамен.

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

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 управлять стратегией изменений в организациях, в том числе в информационной среде	ПК-4	ПК-4.1. Способен анализировать и определять направление развития организации, проектировать архитектуру предприятия ПК-4.2.Разрабатывает стратегию управления изменениями в организации ПК-4.3. Способен планировать интеграцию новых информационных технологий в существующую архитектуру предприятия ПК-4.4. Способен управлять процессом интеграции информационных технологий в существующую информационную среду ПК-4.5. Способен формировать показатели оценки эффективности ИТ

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
		11
Аудиторная работа, в том числе:	50	50
Лекции (Л)	20	20
Практические занятия (ПЗ)	30	30
Лабораторные работы (ЛР)	-	-
Курсовая работа/курсовой проект	-	-
Самостоятельная работа студентов (СРС), в том числе:	58	58
Подготовка к лекциям	5	5
Подготовка к лабораторным работам	-	-
Подготовка к практическим занятиям / семинарам	30	30
Выполнение курсовой работы / проекта	-	-
Расчетно-графическая работа (РГР)	-	-
Реферат (индивидуальное задание)		
Домашнее задание		
Подготовка к контрольной работе		
Подготовка к коллоквиуму	-	-
Аналитический информационный поиск	5	5
Работа в библиотеке	5	5
Подготовка к экзамену	13	13
Промежуточная аттестация – экзамен (Э)	Э	Э
Общая трудоемкость дисциплины		
ак.ч.	108	108
з.е.	3	3

5 Содержание дисциплины

С целью освоения компетенции, приведенной в п.3 дисциплина разбита на 4 темы:

– тема 1 (Основы управления ИБ);

– тема 2 (Системы управления ИБ);

– тема 3 (Основы управления рисками ИБ);

– тема 4 (Процессы управления ИБ);

Виды занятий по дисциплине и распределение аудиторных часов для очной и заочной формы приведены в таблице 3 и 4 соответственно.

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	Основы управления ИБ	Тема№ 1. Введение Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальности. Содержание дисциплины. Виды контроля знаний. Тема № 2. Базовые вопросы управления ИБ Тема № 3. Стандартизация в области управления ИБ	2	Выбор области действия СУИБ Разработка Политики ИБ	2 2	–	–
2	Системы управления ИБ	Тема№ 4. Процессный подход Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Понятие процессного подхода. Тема № 5. Область деятельности СУИБ Тема № 6. Ролевая структура СУИБ. Тема № 7. Политика СУИБ	4	Разработка методики оценки рисков ИБ Проведение оценки рисков ИБ системы	3 3		–
3	Основы управления рисками ИБ	Тема № 8. Рискология ИБ ИБ. Тема № 9. Анализ рисков ИБ.	6	Разработка плана проведения внутреннего аудита ИБ Проведение внутреннего аудита ИБ Планирование работы службы безопасности предприятия	10		

Продолжение таблицы 3

№ 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.
4	Процессы управления ИБ	Тема№ 10. Основные процессы СУИБ. Обязательная документация СУИБ Тема № 11. Внедрение разработанных процессов. Тема№ 12. Внедрение мер (контрольных процедур) по обеспечению ИБ Категории контрольных процедур. Тема№ 13. Процесс «Управление инцидентами ИБ» Тема№ 14. Процесс «Обеспечение непрерывности ведения бизнеса» Тема№ 15. Эксплуатация и независимый аудит СУИБ	8	Организация работы службы безопасности предприятия Контроль за работой службы безопасности предприятия	10		
Всего аудиторных часов			20		30	–	

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 компетенций по дисциплине и способы оценивания знаний приведены в таблице 5.

Таблица 5 – Перечень компетенций по дисциплине и способы оценивания знаний

Код и наименование компетенции	Способ оценивания	Оценочное средство
ПК-4	Экзамен	Комплект контролирующих материалов для экзамена

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

– тестовый контроль или устный опрос на коллоквиумах (2 работы) – всего 40 баллов;

– практические работы – всего 40 баллов;

– за выполнение индивидуального и домашнего задания – всего 20 баллов.

Экзамен 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 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 6.

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

6.3 Темы для рефератов (презентаций) – индивидуальное задание

1.Безопасность и правовое регулирование электронной коммерции

2. Обзор деятельности центров реагирования на инциденты в РФ

3. Обзор деятельности МСЭТ по управлению информационной безопасности

4.Обзор материалов Гост Р ИСО/МЭК 18044 -2007 Менеджмент инцидентов информационной безопасности

5. Обзор материалов Гост ISO/IEC 27005-2012 Методы обеспечение безопасности. Менеджмент рисков безопасности

6. Менеджмент непрерывности бизнеса

7. Менеджмент оказание услуг третьим лицам и клиентам

8. Направления организационной работы в области безопасности, связанной с персоналом.

9. Оценка эффективности передачи риска информационной безопасности третьим лицам

10 Мониторинг безопасности

11 Задачи департамента информационной безопасности

12 Аудит безопасности информационных технологий

6.4 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Тема 1 – Основы управления ИБ

1) Приведите убедительные доводы того, что 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) Дайте определение информационной системы. Перечислите структурные компоненты информационных систем. Что понимают под информационными ресурсами и процессами?

5) Перечислите основные компоненты концептуальной модели ИБ. Изобразите графически схему концептуальной модели системы ИБ.

6) Какие вопросы, касающиеся информационной безопасности, содержатся в Гражданском кодексе РФ?

7) Какая информация является предметом защиты? Перечислите основные свойства информации как предмета защиты. Охарактеризуйте секретную и конфиденциальную информацию.

8) Что такое объекты угроз ИБ? В чем выражаются угрозы информации? Каковы основные источники угроз защищаемой информации? Каковы цели угроз информации со стороны злоумышленников?

9) Какие статьи Уголовного кодекса напрямую касаются информационной безопасности?

10) Охарактеризуйте свойства информации. Что такое признаковая информация? Почему семантическая информация по отношению к признаковой является вторичной? Какие признаки объектов являются демаскирующими?

11) Назовите основные способы неправомерного овладения конфиденциальной информацией.

12) Какие основные понятия рассматриваются в Законе РФ "Об информации, информатизации и защите информации"?

13) Что такое «источник конфиденциальной информации»? Перечислите основные источники конфиденциальной информации.

14) Дайте определение и перечислите основные с пособы НСД к конфиденциальной информации. Охарактеризуйте обобщенную модель взаимодействия способов НСД источников конфиденциальной информации.

15) Дайте определение лицензирования. Кто такие лицензиат и лицензирующие органы? Почему лицензирование и сертификация выступают в качестве средства защиты информации? Перечислите перечень видов деятельности, касающихся ИБ, на осуществление которых требуются лицензии.

16) Дайте определение информационной безопасности, прокомментируйте его составляющие. Перечислите основные категории информационной безопасности.

17) Что такое утечка конфиденциальной информации? Как осуществляется утечка конфиденциальной информации?

18) Какие Вам известны американские законы, напрямую связанные с ИБ? Что можно сказать о законодательстве ФРГ по вопросам ИБ?

19) Что такое защита информации?

20) Определите понятие «несанкционированный доступ» к конфиденциальной информации, как он реализуется?

21) Какие недостатки российского законодательства, на Ваш взгляд, необходимо устранять в первую очередь?

Тема 2 – Системы управления ИБ

22) Охарактеризуйте понятия доступности, целостности и конфиденциальности информации.

23) Дайте определение угроз конфиденциальной информации. Какие действия определяют угрозы конфиденциальной информации?

24) Приведите основные направления деятельности по вопросам ИБ на законодательном уровне.

25) Прокомментируйте основные составляющие информационной безопасности РФ.

26) Что такое атака? Что такое окно опасности? Какие события происходят во время существования окна опасности?

27) Назовите главную цель мер административного уровня ИБ. Что понимается под политикой безопасности? Приведите примерный список решений верхнего уровня политики безопасности.

28) Перечислите важнейшие задачи обеспечения информационной безопасности РФ.

29) Что такое угрозы утечки информации? Какие угрозы называются преднамеренными и случайными?

30) Что такое программа безопасности, ее уровни.

31) Классифицируйте угрозы ИБ РФ для личности, для общества, для Государства по общей направленности.

32) Что такое канал НСД? Назовите типовые причины их возникновения.

33) Что такое управление рисками? Почему управление рисками рассматривается на административном уровне ИБ? В чем заключается суть мероприятий по управлению рисками?

34) Охарактеризуйте государственную структуру органов, обеспечивающих информационную безопасность.

35) Назовите основные способы добывания конфиденциальной информации злоумышленником.

36) В чем заключается основная специфика процедурного уровня ИБ? Перечислите основные классы мер процедурного уровня ИБ. Почему вопросы поддержания работоспособности ИС являются принципиальными на процедурном уровне ИБ?

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

38) Что такое канал утечки информации? Что такое технический канал утечки информации? Охарактеризуйте случайный и организованный канал утечки информации.

39) Перечислите направления повседневной деятельности системного администратора, обеспечивающие поддержание работоспособности ИС.

40) В чем специфика деятельности ФСТЭК России?

41) Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз.

42) Перечислите основные причины важности программно-технического уровня ИБ. Назовите основные сервисы ИБ программно-технического уровня.

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

Тема 3 – Основы управления рисками ИБ

44) Прокомментируйте наиболее распространенные угрозы доступности. Охарактеризуйте программные атаки на доступность.

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

46) Раскройте содержание политических, Экономических и организационно-технических факторов, влияющих на состояние информационной безопасности РФ.

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

48) Что такое идентификация? Дайте толкование понятия «аутентификация». Из-за каких причин затруднена надежная идентификация?

49) Дайте определение защищаемой информации и охарактеризуйте ее основные признаки.

50) Охарактеризуйте основные угрозы целостности конфиденциальной информации.

51) Прокомментируйте парольную идентификацию. Какие меры позволяют повысить надежность парольной защиты?

52) Что такое государственная тайна? Перечислите сведения, которые могут быть отнесены к государственной тайне. Приведите классификацию сведений, составляющих государственную тайну, по степеням секретности

53) Перечислите основные угрозы конфиденциальности информации.

54) Прокомментируйте возможности биометрической идентификации (аутентификации).

55) Перечислите основные виды конфиденциальной информации, нуждающейся в защите.

56) Дайте определение способа защиты информации. Охарактеризуйте основные способы защиты. Перечислите основные защитные действия при реализации способов ЗИ.

57) В чем заключается основная задача логического управления доступом? Что такое матрица доступа? Какая информация анализируется при принятии решения о предоставлении доступа?

Тема 4 – Процессы управления ИБ

58) Каким требованиям должна отвечать коммерческая тайна? Охарактеризуйте основные субъекты права на коммерческую тайну. Какая информация не может быть отнесена к коммерческой тайне?

59) Что такое защита от разглашения?

60) Что такое протоколирование? Прокомментируйте особенности применения данного сервиса безопасности.

61) Перечислите и охарактеризуйте основные объекты профессиональной тайны. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к профессиональной тайне?

62) Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации.

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

64) Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к служебной тайне? Приведите перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения.

65) Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации.

66) Охарактеризуйте экранирование в качестве основного сервиса безопасности ИС. Что такое firewall и как он функционирует?

6.5. Вопросы для подготовки к экзамену (тесты)

1) К правовым методам, обеспечивающим информационную безопасность, относятся

~Разработка аппаратных средств обеспечения правовых данных

~Разработка и установка во всех компьютерных правовых сетях журналов учета действий

=Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке

~Хищение жестких дисков, подключение к сети, инсайдерство

=Перехват данных, хищение данных, изменение архитектуры системы

~Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности

=Персональная, корпоративная, государственная

~Клиентская, серверная, сетевая

~Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение

=Несанкционированного доступа, воздействия в сети

~Инсайдерства в организации

~Чрезвычайных ситуаций

5) Основные объекты информационной безопасности

=Компьютерные сети, базы данных
~Информационные системы, психологическое состояние пользователей
~Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются
~Искажение, уменьшение объема, перекодировка информации
~Техническое вмешательство, выведение из строя оборудования сети
=Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится
=Экономической эффективности системы безопасности
~Многоплатформенной реализации системы
~Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются
~Руководители, менеджеры, администраторы компаний
=Органы права, государства, бизнеса
~Сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное
=Установление регламента, аудит системы, выявление рисков
~Установка новых офисных приложений, смена хостинг-компании
~Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения
=Неоправданных ограничений при работе в сети (системе)
~Рисков безопасности сети, системы
~Презумпции секретности

11) Принципом политики информационной безопасности является принцип
=Невозможности миновать защитные средства сети (системы)
~Усиления основного звена сети, системы
~Полного блокирования доступа при риск-ситуациях

12) К основным типам средств воздействия на компьютерную сеть относится
~Компьютерный сбой
=Логические закладки («мины»)
~Аварийное отключение питания

13) Когда получен спам по e-mail с приложенным файлом, следует

~Прочитать приложение, если оно не содержит ничего ценного – удалить

~Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама

=Удалить письмо с приложением, не раскрывая (не читая) его

14) Принцип Кирхгофа

~Секретность ключа определена секретностью открытого сообщения

~Секретность информации определена скоростью передачи данных

=Секретность закрытого сообщения определяется секретностью ключа

15) ЭЦП – это

~Электронно-цифровой преобразователь

=Электронно-цифровая подпись

~Электронно-цифровой процессор

16) Наиболее распространены угрозы информационной безопасности корпоративной системы

~Покупка нелицензионного ПО

=Ошибки эксплуатации и неумышленного изменения режима работы системы

~Сознательного внедрения сетевых вирусов

17) Наиболее распространены угрозы информационной безопасности сети

~Распределенный доступ клиент, отказ оборудования

~Моральный износ сети, инсайдерство

=Сбой (отказ) оборудования, нелегальное копирование данных

18) Наиболее распространены средства воздействия на сеть офиса

~Слабый трафик, информационный обман, вирусы в интернет

=Вирусы в сети, логические мины (закладки), информационный перехват

~Компьютерные сбои, изменение администрирования, топологии

19) Утечкой информации в системе называется ситуация, характеризуемая

=Потерей данных в системе

~Изменением формы информации

~Изменением содержания информации

20) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются

=Целостность

~Доступность

~Актуальность

21) Угроза информационной системе (компьютерной сети) – это

=Вероятное событие

~Детерминированное (всегда определенное) событие

~Событие, происходящее периодически

22) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется

~Регламентированной

~Правовой

=Защищаемой

23) Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке

=Программные, технические, организационные, технологические

~Серверные, клиентские, спутниковые, наземные

~Личные, корпоративные, социальные, национальные

24) Окончательно, ответственность за защищенность данных в компьютерной сети несет

=Владелец сети

~Администратор сети

~Пользователь сети

25) Политика безопасности в системе (сети) – это комплекс

=Руководств, требований обеспечения необходимого уровня безопасности

~Инструкций, алгоритмов поведения пользователя в сети

~Нормы информационного права, соблюдаемые в сети

26) Наиболее важным при реализации защитных мер политики безопасности является

~Аудит, анализ затрат на проведение защитных мер

~Аудит, анализ безопасности

=Аудит, анализ уязвимостей, риск-ситуаций

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература:

1. Баланов, А. Н. Комплексная информационная безопасность: полный справочник специалиста : практическое пособие / А. Н. Баланов. - Москва ; Вологда : Инфра-Инженерия, 2024. - 156 с. - ISBN 978-5-9729-1771-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2169705 (дата обращения: 19.07.2024). – Режим доступа: по подписке.

2. Царегородцев, А. В. Анализ рисков в процессах обеспечения информационной безопасности жизненного цикла финансовых автоматизированных информационных систем : монография / А.В. Царегородцев, С.В. Романовский, С.Д. Волков. — Москва : ИНФРА-М, 2024. — 198 с. — (Научная мысль). — DOI 10.12737/2049718. - ISBN 978-5-16-018719-8. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2049718 (дата обращения: 19.07.2024). – Режим доступа: по подписке.

Дополнительная литература:

1. Вопросы управления информационной безопасностью: Учебное пособие для вузов. Основы управления информационной безопасностью / Курило А.П., Милославская Н.Г., Сенаторов М.Ю. - Москва :Гор. линия-Телеком, 2013. - 244 с. (Вопросы управления информационной безопасностью)ISBN 978-5-9912-0271-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/560780 (дата обращения: 19.07.2024). – Режим доступа: по подписке.

2. Милославская, Н. Г. Проверка и оценка деятельности по управлению информационной безопасностью: Уч.пос./ Н.Г. Милославская и др. - Москва : Гор. линия-Телеком, 2012. - 166 с.: ил. - (Вопросы управления информационной безопасностью; Кн.5). ISBN 978-5-9912-0275-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/560784 (дата обращения: 19.07.2024). – Режим доступа: по подписке.

3. Милославская, Н. Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И., - 2-е изд. - Москва :Гор. линия-Телеком, 2016. - 170 с.ISBN 978-5-9912-0363-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/560782 (дата обращения: 19.07.2024). – Режим доступа: по подписке.

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.

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 7.

Таблица 7 – Материально-техническое обеспечение

Наименование оборудованных учебных кабинетов	Адрес (местоположение) учебных кабинетов
Специальные помещения: Аудитория для проведения практики, для самостоятельной работы: *Компьютерный класс с мультимедийным оборудованием (14 посадочных мест), оборудованный ознакомительная мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС.* *Персональный компьютер Intel Core 2 Duo E2180 / Biostar 945G / DDR2 2GB / HDD Maxtor 160 GB / TFT Монитор Belinea 17" — 10;* *Персональный компьютер Semptron 2,8 / DDR2 2GB/160/CD52/3,5/KMP/1705G1 — 4;* *Сканер Canon Lide 25 — 1; Принтер Canon LBP-810 — 1, Принтер Epson LX-300 — 1;Коммутатор Suricom EP808X-R 8 port — 3; Проектор LG DS 125 — 1, Мультимедийный экран — 1; Столы компьютерные — 27; столы — 6; стулья — 30; доска ученическая — 1.*	ауд. *412* корп. *2*

Лист согласования РПД

Доцент кафедры
информационных технологий _____ И.С.Зайцев
(должность) (подпись) (Ф.И.О.)

И.о. заведующего кафедрой
информационных технологий _____ А.Н.Баранов
(наименование кафедры) (подпись) (Ф.И.О.)

Протокол №__1___ заседания кафедры от _26.08. 2024 г.

И.о. декана факультета _____ В.В.Дьячкова
(подпись) (Ф.И.О.)

Согласовано

Председатель методической
комиссии по направлению подготовки
38.04.05 Бизнес-информатика
(профиль «Бизнес-аналитика») _____ Н.Н. Лепило
(подпись) (Ф.И.О.)

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>БЫЛО:</td><td>СТАЛО:</td></tr>
<tr><td colspan="2">Основание:</td></tr>
<tr><td colspan="2">Подпись лица, ответственного за внесение изменений</td></tr>
</table>