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

Информационная безопасность
(шифр, наименование дисциплины)

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

Цифровые технологии в бизнесе
(профиль подготовки)

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

Электронный бизнес
(профиль подготовки)

Квалификация бакалавр
(бакалавр/специалист/магистр)

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

Алчевск 2024

## 1 Цели и задачи изучения дисциплины

Дисциплина «Информационная безопасность» посвящена изучению основ информационной безопасности. Рассматриваются основные понятия информационной безопасности, структура мер в области информационной безопасности, кратко описываются меры законодательного, административного, процедурного и программно-технического уровней. Излагаются взгляды на информацию, как объект защиты с выделением характерных свойств защищаемой информации. Рассматриваются виды угроз информационной безопасности; методы и средства борьбы с угрозами информационной безопасности; понятие политики безопасности, существующие типы политик безопасности; действующие стандарты информационной безопасности; нормативные руководящие документы.

Цель дисциплины – формирование у будущих специалистов и руководителей системных знаний по проблеме обеспечения комплексной защиты информационных ресурсов и управлению информационными рисками, а также практических навыков безопасной работы в информационных системах.

Задачи дисциплины:

– формирование системных представлений об управлении информационными рисками;

– изучение методов и средств комплексной защиты информации в информационных системах коммерческих предприятий и государственных учреждений;

– формирование практических навыков анализа защищенности информационных систем, использования встроенных возможностей ОС, MS Office, Брандмауэра Windows, Internet Explorer, а также антивирусных и криптографических средств для обеспечения безопасности информации;

– получение теоретических знаний и практических навыков при решении типовых задач по обеспечению информационной безопасности;

– изучение проблем защиты информации, стоящих перед современной вычислительной техникой;

– формирование навыков использования полученных знаний для правильного выбора решений при разработке криптографических, организационных, технических средств защиты информации.

Дисциплина нацелена на формирование общепрофессиональных (ОПК-2, ОПК-5, ОПК-8), профессиональных компетенций (ПК-1) выпускника.

## 2 Место дисциплины в структуре ОПОП ВО

Логико-структурный анализ дисциплины — входит в *обязательную часть Блока 1* подготовки студентов по направлению подготовки 02.03.01 Математика и компьютерные науки (профиль «Цифровые технологии в бизнесе») и в часть БЛОКА 1 «Дисциплины (модули)», формируемую участниками образовательных отношений по направлению подготовки 38.03.05 Бизнес-информатика (профиль «Электронный бизнес»).

Дисциплина реализуется кафедрой информационных технологий.

Основывается на базе дисциплин: «Анализ данных», «Математические методы принятия решений» по направлению 02.03.01 «Математика и компьютерные науки»; «Анализ данных», «Теория систем и системный анализ» по направлению 38.03.05 Бизнес-информатика.

Является основой для изучения следующих дисциплин: «Электронный бизнес» по направлению подготовки 02.03.01 Математика и компьютерные науки; «Управление проектами», «Преддипломная (производственная) практика» по направлению 38.03.05 Бизнес-информатика.

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения профессиональных задач деятельности, связанных с использованием математических методов и информационных технологий.

Курс является фундаментом для формирования у студентов навыков по использованию в практической деятельности инструментов оценки бизнеса.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы, 108 ак.ч.

Программой дисциплины предусмотрены:

– *при очной форме обучения* для всех направлений — лекционные (18 ак.ч.), практические (36 ак.ч.) занятия и самостоятельная работа студента (54 ак.ч.).

Дисциплина изучается при очной форме обучения для всех направлений на 2 курсе в 4-м семестре.

Форма промежуточной аттестации — зачет.

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

*Процесс изучения дисциплины* «Информационная безопасность» направлен на формирование компетенций, представленных 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.<br>ОПК-5.2. Умеет использовать их в профессиональной деятельности.<br>ОПК-5.3. Имеет практические навыки использования современных информационных технологий для решения задач профессиональной деятельности. |
| | | ОПК-8. Способен использовать основы правовых знаний в различных сферах жизнедеятельности | ОПК-8.1. Знает базовые основы правовых знаний<br>ОПК-8.2. Умеет использовать их в профессиональной деятельности<br>ОПК-8.3. Имеет практические навыки применения правовых знаний |
| 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<br>ОПК-2.2. Выявляет бизнес-потребности в информационном обеспечении и формализует требования к ИТ-решениям.<br>ОПК-2.3. Анализирует и документирует различные альтернативные варианты решений для удовлетворения потребностей бизнеса<br>ОПК-2.4. Оценивает альтернативные решения в контексте их использования |
| | | ПК-1 Способен выявлять бизнес-проблемы и бизнес-возможности организации, анализировать их, обосновывать и выбирать решения | ПК-1.1 Осуществляет сбор информации и выявляет бизнес-проблемы и бизнес-возможности предприятия<br>ПК-1.2 Использует инструментальные средства для анализа и визуализации бизнес-информации<br>ПК-1.3 Способен применять экономико-математический инструментарий при анализе проблемных ситуаций и поиске возможных решений |

## 4 Объём и виды занятий по дисциплине

Общая трудоёмкость учебной дисциплины составляет 3 зачётных единиц, 108 ак.ч.

Самостоятельная работа студента (СРС) включает проработку материалов лекций, выполнение домашнего задания, подготовку к лабораторным занятиям, устному опросу, текущему контролю, 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 для направления подготовки 02.03.01 Математика и компьютерные науки и для направления подготовки 38.03.05 Бизнес-информатика.

Таблица 2 — Распределение бюджета времени на СРС для направления подготовки 02.03.01 Математика и компьютерные науки, 38.03.05 Бизнес-информатика

| Вид учебной работы | Всего ак.ч. | Ак.ч. по семестрам |
|---|---|---|
| | | 4 |
| Аудиторная работа, в том числе: | 54 | 54 |
| Лекции (Л) | 18 | 18 |
| Практические занятия (ПЗ) | - | - |
| Лабораторные работы (ЛР) | 36 | 36 |
| Курсовая работа/курсовой проект | - | - |
| Самостоятельная работа студентов (СРС), в том числе: | 54 | 54 |
| Подготовка к лекциям | 4 | 4 |
| Подготовка к лабораторным работам | 36 | 36 |
| Подготовка к практическим занятиям / семинарам | - | - |
| Выполнение курсовой работы / проекта | - | - |
| Расчетно-графическая работа (РГР) | - | - |
| Реферат (индивидуальное задание) | - | - |
| Домашнее задание | - | - |
| Подготовка к контрольной работе | - | - |
| Подготовка к коллоквиуму | - | - |
| Аналитический информационный поиск | 6 | 6 |
| Работа в библиотеке | 2 | 2 |
| Подготовка к зачету | 6 | 6 |
| Промежуточная аттестация – зачет (З) | З | З |
| Общая трудоемкость дисциплины | | |
| ак.ч. | 108 | 108 |
| з.е. | 3 | 3 |

## 5 Содержание дисциплины

С целью освоения компетенций, приведенных в п.3, дисциплина разбита на 7 тем:

– тема 1 (Введение. Общее понятие безопасности и система мер по её обеспечению);

– тема 2 (Правовые аспекты и диагностические параметры экономической безопасности);

– тема 3 (Экономическая безопасность предприятия и основные её критерии и показатели);

– тема 4 (Анализ уровня экономической безопасности предприятия(ЭБП) и основные направления её обеспечения);

– тема 5 (Методы информационно- аналитической работы (конкурентной разведки), применяемые для определения и оценки экономических рисков компании);

– тема 6 (Защита компании от экономических рисков, связанных с участием компании в гражданско- правовых отношениях);

– тема 7 (Зарубежный опыт обеспечения безопасности предпринимательской деятельности);

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

Таблица 4 — 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 | Введение. Общее понятие безопасности и система мер по её обеспечению | Категории «опасность» и «безопасность»: генезис и диалектика развития. Национальная безопасность государства. Основные определения экономической безопасности Роль и место экономической безопасности в системе национальной безопасности. Угрозы информации. Классификация угроз по видам, по природе происхождения, по предпосылкам появления, по источникам. Взаимодействие угроз информации . | 2 | - | - | Аудит паролей в Windows<br>Хранение паролей в Windows<br>Парольный hash<br>Перебор паролей (словари, брудфорс)<br>Программы lcp, saminside, pwdump | 4 |
| 2 | Правовые аспекты и диагностические параметры экономической безопасности | Основные положения, концепции и Государственной стратегии экономической безопасности России. Критерии и индикаторы экономической безопасности страны. Основные понятия и определения. Классификация показателей экономической безопасности. Методы оценки экономической безопасности страны. Критерии базовых показателей экономической безопасности. Методы экспертной оценки. Доктрина информационной безопасности РФ. Закон о Государственной Тайне. Закон об информации, информационных технологиях и защите информации. | 2 | - | - | Симуляция перехвата клавиатурного ввода с сокрытием следов в системе и автоматической пересылкой полученного ввода с атакованного ПК<br>создание скрипта и задания в шедулере для пересылки файла с захваченным логом | 4 |

| № 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. |
|---|---|---|---|---|---|---|---|
| 3 | Экономическая безопасность предприятия и основные её критерии и показатели | Необходимость обеспечения экономической безопасности предприятия. «Экономическая безопасность предприятия» как экономическая категория. Основные направления и принципы обеспечения экономической безопасности предприятия. Стратегическое планирование и прогнозирование экономической безопасности предприятия. | 2 | - | - | Анализ IP-трафика (атака на ftp, http, SMB, MySQL) Wireshark сведения о структуре сетевых пакетов, протоколов, служб перехват паролей ftp, данных web-форм, содержимого файлов при передаче через SMB, перехват парольных хэшей MySQL и данных сервера БД | 4 |
| 4 | Анализ уровня экономической безопасности предприятия(ЭБП) и основные направления её обеспечения | Функциональный анализ. Алгоритм анализа. Основные направления обеспечения экономической безопасности предприятия. Финансовая составляющая и её сущность. Основные индикаторы состояния финансовой составляющей экономической безопасности предприятия. Интеллектуальная и кадровая составляющая(ИКС) экономической безопасности предприятия. Технико-технологическая составляющая(ТТС) экономической безопасности предприятия. | 2 | - | - | Брендмауэр Windows (настройка, логика разграничения групп компьютеров, создание правил) | 4 |

| № 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. |
|---|---|---|---|---|---|---|---|
| 5 | Методы информационно- аналитической работы (конкурентной разведки), применяемые для определения и оценки экономических рисков компании | Классификация информации и информационных ресурсов, применяемые информационные технологии, способы оценки информации, виды оперативного представления информационных услуг. Методы сбора информации, оценка информации и перевод её в сведения. Получение информации из «открытых источников» (из ресурсов Интернета, баз данных, средств массовой информации и т.д.). Методы анализа информации (SWOT-анализ, анализ конкурентной среды методом 5 сил Майкла Портера, диверсионный анализ, метод аналогии, метод исключения, анализ причинно-следственных связей, экспертные методы анализа и т.д.) Обзор автоматизированных информационно- аналитических систем, представленных на рынке | 4 | - | - | Брендмауэр Windows (настройка, логика разграничения групп компьютеров, создание правил) | 4 |

| № 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. |
|---|---|---|---|---|---|---|---|
| 6 | Защита компании от экономических рисков, связанных с участием компании в гражданско- правовых отношениях | Проверка надёжности организации перед заключением гражданско-правовых отношений. Направления анализа предполагаемого контрагента. Определение безопасности предложений и коммерческих проектов. Растровые признаки опасности при определении надёжности контрагентов и коммерческих проектов Защита компании от внешнего мошенничества. Защита компании от рейдерства. | 4 | - | - | Понятие Архитектура реализации стэка TCP архитектура WFP Фаервол Windows настройка, логика разграничения групп компьютеров, создание правил | 8 |
| 7 | Зарубежный опыт обеспечения безопасности предпринимательской деятельности | Частная правоохранительная деятельность в США. Проблемы взаимодействия правоохранительных органов с общественными организациями и частнопредпринимательскими структурами. Великобритания. Частные детективные агентства. Специфика законодательства и основные направления работы. Германия. Задачи и направления деятельности частных охранно-сыскных бюро. Особенности работы их сотрудников. Франция. Деятельность частных охранно-сыскных бюро. | 2 | - | | Разработка программы реализующей простой алгоритм симметричного шифрования Виды шифрования Симметричное шифрование обзор команд "полезных" для разработки алгоритмов шифрования Пример программы реализующей простой алгоритм симметричного шифрования | 8 |
| Всего аудиторных часов | | | 18 | - | | 36 | |

## 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 5.

Таблица 5 — Перечень работ по дисциплине и способы оценивания знаний

| Вид учебной работы | Способ оценивания | Количество баллов |
|---|---|---|
| Выполнение лабораторных работ | Предоставление отчетов | 50–80 |
| Выполнение тестового контроля или устного опроса | Более 50% правильных ответов | 10–20 |
| Итого | - | 60–100 |

Зачет проставляется автоматически, если студент набрал в течение 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 «Информационная безопасность» проводится по результатам работы в семестре. В случае, если полученная в семестре сумма баллов не устраивает студента, во время зачета студент имеет право повысить итоговую оценку в форме устного зачета по приведенным ниже вопросам (п.п. 6.3).

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 Оценочные средства для самостоятельной работы и текущего контроля успеваемости: тестовый контроль**

*1. Чтобы подписать сообщение электронной цифровой подписью, используются:*

а) открытый ключ отправителя;

б) открытый ключ получателя;

в) закрытый ключ отправителя;

г) закрытый ключ получателя.

*2. Какие утверждения о протоколе строгой двусторонней аутентификации на основе случайных чисел справедливы?*

а) в основе протокола лежит симметричный алгоритм шифрования;

б) на первом шаге проверяющий B отправляет проверяемому A случайное число;

в) на втором шаге проверяемый A отправляет проверяющему B зашифрованное сообщение, содержащее полученное на первом шаге случайное число, а также новое случайное число;

г) всего протокол требует отправки двух сообщений.

*3. Какова последовательность подписания сообщений с помощью ЭЦП?*

а) вычисляется хэш, затем хэш зашифровывается;

б) сообщение зашифровывается, после чего результат хэшируется;

в) при подписании сообщение зашифровывается, при проверке вычисляется хэш;

г) вычисляется хэш исходного сообщения, после чего оно зашифровывается.

*4. В чем заключается такое свойство функции хэширования как стойкость к коллизиям первого рода?*

а) Для любого хэша h должно быть практически невозможно вычислить или подобрать такое x, что H(x) = h.

б) Должно быть практически невозможно вычислить или подобрать любую пару различных сообщений x и y для которых H(x) = H(y);

в) Длина хэша должна быть фиксированной независимо от длины входного сообщения;

г) Для любого сообщения x должно быть практически невозможно вычислить или подобрать другое сообщение y, такое что H(x) = H(y).

*5. Доказательство корректности алгоритма RSA основано на:*

а) теореме Эйлера;

б) теореме о сумме эллиптических кривых;

в) китайской теореме об остатках;

г) расширенном алгоритме Евклида.

*6. Какими свойствами должен обладать генератор псевдослучайных чисел?*

а) недетерминированность;

б) непредсказуемость;

в) независимость очередного элемента от предыдущего;

г) равномерное распределение элементов последовательности;

д) неповторяемость элементов последовательности (в пределах периода).

*7. Чтобы расшифровать сообщение с помощью асимметричного алгоритма шифрования используются:*

а) открытый ключ отправителя;

б) открытый ключ получателя;

в) закрытый ключ отправителя;

г) закрытый ключ получателя.

*8. К какой разновидности протоколов относится протокол опознания пользователя на основе пароля?*

а) протокол аутентификации;

б) протокол обмена ключами;

в) протокол одновременной подписи;

г) протокол групповой подписи;

д) протокол голосования.

*9. Каким образом проникают в систему макровирусы?*

а) по электронной почте;

б) любым способом вместе с зараженными ими файлами;

в) злоумышленник должен вручную внести вирус в систему;

г) через Интернет, используя ошибки в сетевых программах;

д) через съемные носители данных при срабатывании автозагрузки с них.

*10. Какому требованию должен удовлетворять пароль для противодействия атаке по персональному словарю?*

а) при придумывании пароля не должны использоваться личные данные;

б) длина пароля должна составлять12 и более символов;

в) пароль нельзя открывать никому;

г) разные сервисы должны защищаться разными паролями;

д) пароль должен включать символы разных алфавитов и регистров, цифры, знаки препинания и т.д.

*11. Какие недостатки имеют системы обнаружения вторжений, работающие на основе обнаружения аномалий?*

а) высокий процент ложных срабатываний;

б) не способны контролировать ситуацию во всей сети;

в) неспособны анализировать степень проникновения;

г) работа затруднена при высокой загрузке сети; д) снижается эффективность работы сервера, на котором они установлены.

*12. Как называются вирусы, которые автоматически запускаются в момент старта операционной системы и, таким образом, постоянно функционируют в оперативной памяти?*

а) резидентные вирусы;

б) стелс-вирусы;

в) макровирусы;

г) полиморфные вирусы;

д) троянские кони.

*13. К какому классу относятся межсетевые экраны, которые отслеживают текущие соединения и пропускают только такие пакеты, которые удовлетворяют логике и алгоритмам работы соответствующих протоколов и приложений?*

а) Работающие на сетевом уровне;

б) Работающие на сеансовом уровне;

в) Работающие на уровне приложений;

г) Stateless;

д) Stateful.

*14. Как называются антивирусы, которые работают резидентно, предотвращая заражение файлов?*

а) детекторы;

б) фаги;

в) ревизоры;

г) вакцины;

д) фильтры.

*15. Какие вирусы заражают носители данных?*

а) файловые вирусы;

б) загрузочные вирусы;

в) макровирусы;

г) сетевые черви;

д) троянские кони.

*16. Как называются VPN, с помощью которых на основе не надёжной сети создается надежная и защищенная подсеть?*

а) Внутрикорпоративный;

б) Защищенные;

в) С удаленным доступом;

г) Доверительные;

д) Межкорпоративные.

*17. Какому требованию должен удовлетворять пароль для противодействия фишингу?*

а) пароль не должен быть производным от слов любого естественного языка;

б) длина пароля должна составлять12 и более символов;

в) пароль нельзя открывать никому;

г) разные сервисы должны защищаться разными паролями;

д) пароль должен включать символы разных алфавитов и регистров, цифры, знаки препинания и т.д.

*18. Что такое VPN?*

а) система обнаружения вторжений;

б) протокол обмена ключами;

в) трансляция сетевых адресов;

г) виртуальная частная сеть;

д) протокол защиты передаваемого потока.

*19. Каков основной недостаток обнаружения вирусов путем эвристического сканирования?*

а) значительная вероятность ложного срабатывания;
б) крайне медленная работа антивируса;
в) невозможность обнаружения новых вирусов;
г) необходимость трудоемкой ручной настройки антивируса

### 6.3 Вопросы для подготовки к зачету

1. Каковы четыре основные составляющие национальных интересов Российской Федерации (РФ) в информационной сфере?
2. Сформулируйте интересы государства, общества и личности в информационной сфере. Сформулируйте основные проблемы ИБ.
3. Дайте определение информационной безопасности РФ. Перечислите основные объекты и субъекты защиты процессов переработки информации.
4. Поясните значения основных аспектов информационной безопасности: конфиденциальности, целостности и доступности.
5. Приведите примеры средств, обеспечивающих конфиденциальность, но не гарантирующих целостность данных.
6. Приведите примеры действий воображаемого злоумышленника, направленных на нарушение доступности данных.
7. Предложите какой-нибудь способ обеспечения целостности данных. В чем заключается комплексное обеспечение ИБ?
8. Раскройте содержание основных принципов доктрины ИБ.
9. Каковы основные отечественные и зарубежные стандарты в области ИБ?
10. Дайте определения понятиям: «государственная тайна», «коммерческая тайна», «служебная тайна», «профессиональная тайна». Что такое персональные данные?
11. Что такое источники права на доступ к информации? Каковы уровни доступа к информации с точки зрения законодательства РФ?
12. Что такое информация ограниченного распространения? В чем может заключаться ответственность за нарушение законодательства РФ в информационной сфере?
13. Дайте общую характеристику международному стандарту ISO/IEC безопасности информационных технологий.
14. Чем вызвана необходимость разработки стандартов по защите информации в компьютерных системах? Назовите существующие стандарты и нормативов этой области.

15. На что направлены меры административного уровня информационной безопасности? Что такое политика безопасности?
16. Что такое программа безопасности? На основе чего строится политика безопасности?
17. Охарактеризуйте уровни политики безопасности.
18. Что понимается под угрозой информационной безопасности в компьютерной системе?
19. Каковы основные виды угроз ИБ? Как классифицируют организационные и правовые методы и средства предотвращения угроз ИБ?
20. Каким может быть статус злоумышленника, реализующего преднамеренные угрозы? Что представляют собой вредительские программы?
21. Каким образом классифицируют методы предотвращения угроз несанкционированного доступа в компьютерных системах?
22. Дайте классификацию методов предотвращения случайных угроз.
23. Какие криптографические методы предотвращения угроз вы знаете?

## 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. ─ ( Высшее образование: Бакалавриат ) . ─ ISBN 978-5-16-014976-9.– 15 экз.

2. Бабаш, А.В. Актуальные вопросы защиты информации : монография / А.В. Бабаш, Е.К. Баранова . ─ Москва : РИОР ; Москва : ИНФРА-М, 2022 . ─ 111 с. : ил. + табл. ─ ( Научная мысль ) . ─ ISBN 978-5-369-01680-0.– 10 экз.

**Дополнительная литература**

3. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2082642 (дата обращения: 05.07.2024). – Режим доступа: по подписке.

4. Скрипник, Д. А. Техническая защита информации. Организация защиты информации ограниченного доступа, несодержащей сведения, составляющие государственную тайну : краткий курс / Д. А. Скрипник. - Москва : ИНТУИТ, 2016. - 233 с. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2160980 (дата обращения: 05.07.2024). – Режим доступа: по подписке.

5. Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова. [и др.] ; - Москва : ИНТУИТ, 2016. - 276 с. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2160982 (дата обращения: 05.07.2024). – 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 8.

Таблица 8 — Материально-техническое обеспечение

| Наименование оборудованных учебных кабинетов | Адрес (местоположение) учебных кабинетов |
|---|---|
| Специальные помещения:<br>*Компьютерный класс с мультимедийным оборудованием (25 посадочных мест),* оборудованный учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС: компьютер – 14 шт., мультимедийный проектор, проекционный экран, веб-камера, колонки, микрофон, принтер Pantum P2516, доска для написания мелом | ауд. *412* корп. 2 |
| *Компьютерный класс кафедры ИТ (25 посадочных мест),* оборудованный учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС: компьютер – 14 шт., интерактивная панель, принтер Pantum P2516 | ауд. *314* корп. 2 |
| *Компьютерный класс кафедры ИТ (25 посадочных мест),* оборудованный учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС: персональный компьютер Intel Celeron 420 / ECS 945GCT-M2 / DDR2 2GB / HDD Hitachi 120 GB / TFT Монитор Hanns.G 18.5” – 14 шт., принтер Canon LBP-810 – 1 шт., принтер Epson LX300 – 1 шт., сканер A4 HP-400 – 1 шт., мультимедийная доска – 1 шт., столы компьютерные — 27 шт.; парты — 5 шт.; стулья — 30 шт. | ауд. *302* корп. 2 |

Лист согласования рабочей программы дисциплины

Разработал
к.э.н., доцент кафедры
информационных технологий _____ _____ И.С.Зайцев
(должность) (подпись) (Ф.И.О.)

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

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

Протокол № 1 заседания кафедры
информационных технологий от 26.08.2024г.

Согласовано

Председатель методической
комиссии по направлению подготовки:

02.03.01 Математика и компьютерные науки
38.03.05 Бизнес-информатика _____ 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>ДО ВНЕСЕНИЯ ИЗМЕНЕНИЙ:</td><td>ПОСЛЕ ВНЕСЕНИЯ ИЗМЕНЕНИЙ:</td></tr>
<tr><td colspan="2">Основание:</td></tr>
<tr><td colspan="2">Подпись лица, ответственного за внесение изменений</td></tr>
</table>