Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гриб Владислав Валерьевич
Должность: Ректор
Дата подписания: 23.09.2026 18:46:38
Уникальный программный ключ:
637517d24e103c3db032acf37e[illegible]

**Образовательное частное учреждение высшего образования**
**«МОСКОВСКИЙ УНИВЕРСИТЕТ ИМЕНИ А.С. ГРИБОЕДОВА»**
(ИМПЭ им. А.С. Грибоедова)

**МЕЖДУНАРОДНЫЙ ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И БИЗНЕС-ИНФОРМАТИКИ**

**УТВЕРЖДАЮ**
Директор Международного
института информационных
технологий и бизнес-информатики
_____ Т.В. Новикова
«17» декабря 2025г.

**Рабочая программа дисциплины**

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

**Направление подготовки**
**09.03.03 Прикладная информатика**
**(уровень бакалавриат)**

**Направленность (профиль):**
**«Анализ данных»**

**Форма обучения**: **очная, заочная**

**Москва**

Рабочая программа дисциплины «Информационная безопасность». Направление подготовки 09.03.03 Прикладная информатика, направленность (профиль): «Анализ данных» / О.А. Левичев – М.: ИМПЭ им. А.С. Грибоедова.

Рабочая программа дисциплины составлена на основании федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 09.03.03 Прикладная информатика, утвержденного приказом Министерства образования и науки Российской Федерации от «19» сентября 2017 № 922 (с изменениями и дополнениями) и Профессиональным стандартом «Программист», Утверждённым приказом Министерства труда и социальной защиты Российской Федерации от 20 июля 2022 № 424н (регистрационный номер 4).

Разработчики: О.А. Левичев, к. в. н., доцент

Ответственный рецензент: Е.В. Михалёва, к. ф.-м. н.
исполнительный директор института информационных систем и инженерно- компьютерных технологий

Рабочая программа дисциплины рассмотрена и одобрена на заседании кафедры информационных технологий и прикладной информатики 17.12.2025г., протокол №6

Заведующий кафедрой _____/Н.Н. Загускин, к.ю.н, доцент

Согласовано от библиотеки _____/ О. Е. Степкина

## Раздел 1. Цели и задачи освоения дисциплины

Целью освоения дисциплины является формирование обучающимися основных принципов, моделей и методов защиты информации; овладение методами организационного и правового обеспечения безопасности информационных систем и данных; приобретение навыков и основных приемов защиты информации от утечки и несанкционированного доступа, антивирусной борьбы; применение криптографических методов защиты.

Задачи дисциплины:

- изучить характерные свойства защищаемой информации, основные информационные угрозы, существующие направления защиты;
- получить теоретические знания в области защиты информации;
- ознакомиться с требованиями российских и международных стандартов в области информационной безопасности;
- научиться применять современные программно-аппаратные средства защиты на практике.

## Раздел 2. Планирование результатов обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

| Код компетенции | Формулировка компетенции | Индикаторы достижения компетенции |
|---|---|---|
| УК-10 | Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности | ИУК-10.1. Знать природу экстремизма, терроризма, коррупционного поведения как социально-правового явления. Понимать общественную опасность экстремизма, терроризма, коррупционного поведения во всех их проявлениях, последствия и необходимость противодействия им<br>ИУК-10.2. Уметь реализовывать средства обеспечения законности и правопорядка в сфере противодействия экстремизма, терроризма, коррупционному поведению |
| ОПК-3 | Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | ИОПК-3.1. Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне<br>ИОПК-3.2. Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне |

## Раздел 3. Место дисциплины в структуре образовательной программы бакалавриата

Дисциплина «Информационная безопасность» изучается в 5 семестре очной и в 6 семестре заочной форм обучения, относится к Блоку 1 «Дисциплины (модули)», «Обязательная часть», образовательной программы по направлению подготовки 09.03.03 Прикладная информатика (уровень бакалавриат), направленность (профиль): «Анализ данных».

## Раздел 4. Объем (трудоемкость) дисциплины (общая, по видам учебной работы, видам промежуточной аттестации)

### Трудоемкость дисциплины и виды учебной нагрузки

**на очной форме обучения**

| з.е. | Итого | Лекции | Практические занятия | Курсовое проектирование | Самостоятельная работа | Текущий контроль | Контроль, промежуточная аттестация |
|---|---|---|---|---|---|---|---|
| 5 семестр | | | | | | | |
| 3 | 108 | 16 | 16 | | 72 | | 4 Зачет |

**на заочной форме обучения**

| з.е. | Итого | Лекции | Практические занятия | Курсовое проектирование | Самостоятельная работа | Текущий контроль | Контроль, промежуточная аттестация |
|---|---|---|---|---|---|---|---|
| 6 семестр | | | | | | | |
| 3 | 108 | 4 | 4 | | 96 | | 4 Зачет |

### Тематический план дисциплины

**Очная форма обучения**

| Разделы / Темы | Лекции | Практические занятия | Самостоятельная работа | Текущий контроль | Контроль, промежуточная аттестация | Всего часов |
|---|---|---|---|---|---|---|
| 5 семестр | | | | | | |
| Тема. 1 Введение в информационную безопасность | 3 | 2 | 7 | | | 12 |
| Тема. 2 Законодательный уровень информационной безопасности | 3 | 2 | 7 | | | 12 |
| Тема. 3 Стандарты и спецификации в области информационной безопасности | 2 | 2 | 7 | | | 11 |
| Тема. 4 Административный уровень информационной безопасности | 1 | 2 | 7 | | | 10 |
| Тема. 5 Процедурный уровень информационной безопасности | 1 | 2 | 7 | | | 10 |
| Тема. 6 Идентификация и аутентификация | 1 | 1 | 7 | | | 9 |
| Тема. 7 Управление доступом. Протоколирование и аудит | 1 | 1 | 7 | | | 9 |
| Тема. 8 Криптографические методы защиты | 1 | 1 | 7 | | | 9 |
| Тема. 9 Контроль целостности | 1 | 1 | 6 | | | 8 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Тема. 10 Экранирование. Тунелирование | 1 | 1 | 5 | | | 7 |
| Тема. 11 Анализ защищенности | 1 | 1 | 5 | | | 7 |
| Зачет | | | | | **4** | **4** |
| Итого по дисциплине | **16** | **16** | **72** | | **4** | **108** |

**Заочная форма обучения**

| Разделы / Темы | Лекции | Практические занятия | Самостоятельная работа | Текущий контроль | Контроль, промежуточная аттестация | Всего часов |
|---|---|---|---|---|---|---|
| 6 семестр | | | | | | |
| Тема. 1 Введение в информационную безопасность | 1 | | 9 | | | 10 |
| Тема. 2 Законодательный уровень информационной безопасности | | 1 | 9 | | | 10 |
| Тема. 3 Стандарты и спецификации в области информационной безопасности | 1 | | 8 | | | 9 |
| Тема. 4 Административный уровень информационной безопасности | | 1 | 9 | | | 10 |
| Тема. 5 Процедурный уровень информационной безопасности | 1 | | 9 | | | 10 |
| Тема. 6 Идентификация и аутентификация | | | 9 | | | 9 |
| Тема. 7 Управление доступом. Протоколирование и аудит | | 1 | 9 | | | 10 |
| Тема. 8 Криптографические методы защиты | 1 | | 9 | | | 10 |
| Тема. 9 Контроль целостности | | | 8 | | | 8 |
| Тема. 10 Экранирование. Тунелирование | | | 8 | | | 8 |
| Тема. 11 Анализ защищенности | | 1 | 9 | | | 10 |
| Зачет | | | | | 4 | 4 |
| Итого по дисциплине | **4** | **4** | **96** | | **4** | **108** |

**Структура и содержание дисциплины**

| Наименование разделов/тем | Содержание темы |
|---|---|
| Тема 1. Введение в информационную безопасность | Понятие информационной безопасности. Основные составляющие информационной безопасности: доступность, целостность и конфиденциальность. Угрозы информационной безопасности. Задачи системы информационной безопасности.<br>Меры противодействия угрозам безопасности.<br>Основные принципы построения систем защиты АИС. Информационная безопасность на уровне государства. Концепция безопасности РФ. Важность проблемы информационной безопасности. Примеры нарушений информационной безопасности. |

| Наименование разделов/тем | Содержание темы |
|---|---|
| Тема 2. Законодательный уровень информационной безопасности | Понятие и важность законодательного уровня информационной безопасности. Обзор российского законодательства в области информационной безопасности. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности. Закон `Об информации, информационных технологиях и о защите информации`. Закон `Об электронной подписи`. Закон `О персональных данных`. Защита авторского права на программные продукты. Обзор международного законодательства в области информационной безопасности. Федеральный закон `О государственной тайне`. |
| Тема 3. Стандарты и спецификации в области информационной безопасности | Оценочные стандарты и технические спецификации. Оценочный стандарт ГОСТ Р ИСО/МЭК 15408 `Общие критерии оценки безопасности информационных технологий`. Введение и общая модель. Функциональные компоненты безопасности. Компоненты доверия к безопасности. Сопутствующие документы. Управленческие стандарты информационной безопасности. ГОСТ Р ИСО/МЭК 17799 `Информационные технологии. Практические правила управления информационной безопасностью`. ГОСТ Р ИСО/МЭК 27001 `Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования`. Руководящие документы Гостехкомиссии России. |
| Тема 4. Административный уровень информационной безопасности | Основные понятия. Политика безопасности. Программа безопасности. Синхронизация программы безопасности с жизненным циклом систем Примеры типовых политик безопасности организации. |
| Тема 5. Процедурный уровень информационной безопасности | Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Поддержка работоспособности<br>Реагирование на нарушение режима безопасности. Планирование восстановительных работ. План восстановительных работ. |
| Тема 6. Идентификация и аутентификация | Определение идентификации и аутентификации. Парольная аутентификация. Требования к паролям. Одноразовые пароли.<br>Сервер аутентификации Kerberos. Идентификация/аутентификация с помощью биометрических данных. Алгоритмы создания одноразовых паролей. Социальный инжиниринг. |
| Тема 7. Управление доступом. Протоколирование и аудит | Понятие управления доступом. Модели безопасности: модель дискреционного доступа; модель Белла-ЛаПадулы; ролевая модель управления доступом. Понятие протоколирования и аудита. Активный аудит. Системы разграничения доступа. Функциональные компоненты архитектуры. |
| Тема 8. Криптографические методы защиты | Введение в криптографию. Основные термины и понятия криптографии. Типы криптографических |

| Наименование разделов/тем | Содержание темы |
|---|---|
| | систем. Шифры подстановки и перестановки. Блочные шифры. Сеть Фейштеля.<br>Симметричные алгоритмы шифрования. Алгоритмы DES, ГОСТ 34.12-2015, AES. Асимметричные алгоритмы шифрования. Алгоритм RSA. Режимы шифрования блочных шифров. Потоковые шифры. Обмен ключами Диффи-Хелмана. Шифросистема Эль-Гамаля. Стандарт ГОСТ Р 34.10-2012. |
| Тема 9. Контроль целостности | Определение функции хеширования. Требования к хеш-фукнциям. Функции Хеширования. Электронная цифровая подпись. Цифровые сертификаты. Деятельность удостоверяющих центров. Функция хеширования MD5. |
| Тема 10. Экранирование. Тунелирование | Понятие экранирования. Межсетевые экраны. Классификация межсетевых экранов. Виды межсетевых экранов. Понятие тунелирования. Виртуальные частные сети. VPN IPsec, PPTP.<br>Разработка конфигурации межсетевого экрана. |
| Тема 11. Анализ защищенности | Понятие анализа защищенности. Сетевые сканеры. Антивирусная защита. Классификация вирусов. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ. Основы работы антивирусных программ.<br>Антивирусная защита компьютерной сети. |

**Занятия семинарского типа**
**(Практические занятия)**

Общие рекомендации по подготовке к практическим занятиям. При подготовке к работе во время проведения занятий практического типа следует обратить внимание на следующие моменты: на процесс предварительной подготовки, на работу во время занятия, обработку полученных результатов, исправление полученных замечаний. Предварительная подготовка к учебному занятию практического типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач занятия.

Работа во время проведения занятия практического типа включает несколько моментов: а) консультирование обучающихся преподавателями с целью предоставления исчерпывающей информации, необходимой для самостоятельного выполнения предложенных преподавателем задач, б) самостоятельное выполнение заданий согласно обозначенной учебной программой тематики.

Раздел №1 «Законодательный, процедурный и административный уровни информационной безопасности»

Практическая работа 1. Обзора российского законодательства в области информационной безопасности

1. Какие основные цели и принципы закреплены в Федеральном законе № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», и как он соотносится с другими нормативными актами в сфере ИБ?
2. Как Федеральный закон № 152-ФЗ «О персональных данных» регулирует обработку, хранение и защиту персональной информации, и какие обязательства он накладывает на операторов в контексте обеспечения информационной безопасности?

3. Какие полномочия в сфере информационной безопасности закреплены за уполномоченными органами власти (ФСБ, Роскомнадзор, Минцифры), и как их взаимодействие отражается на практике соблюдения законодательства организациями?

Практическая работа 2. Разработка политики безопасности организации

1. Какие основные разделы должна включать политика информационной безопасности организации, и как она соотносится с международными стандартами (например, ISO/IEC 27001)?
2. Как учитывать специфику предметной области (например, здравоохранение, образование, финансы) при разработке политики безопасности, чтобы обеспечить баланс между защитой данных и операционной эффективностью?
3. Какие механизмы используются для внедрения, коммуникации и контроля соблюдения политики безопасности сотрудниками, и почему формальное утверждение документа недостаточно для её эффективности?

Практическая работа 3. Анализ рисков информационной безопасности организации

1. Какие этапы включает процесс анализа рисков информационной безопасности согласно стандарту ISO/IEC 27005, и почему идентификация активов является отправной точкой этого процесса?
2. В чём различие между качественным и количественным подходами к оценке рисков, и в каких случаях целесообразно использовать каждый из них в деятельности организации?
3. Как результаты анализа рисков информационной безопасности влияют на выбор мер защиты, распределение бюджета и приоритеты в реализации программ по обеспечению ИБ?

Раздел №2 «Программно-технический уровень информационной безопасности»

Практическая работа 4. Защита информации в компьютерной системе от случайных угроз. Создание и управление учетными записями пользователей

1. Какие меры защиты позволяют минимизировать последствия случайных угроз (например, ошибок пользователей, сбоев оборудования) в компьютерной системе, и какую роль в этом играет корректная настройка прав доступа?
2. Какие принципы (например, принцип минимальных привилегий, разделение обязанностей) следует соблюдать при создании и настройке учетных записей пользователей, чтобы снизить риски как умышленных, так и случайных нарушений информационной безопасности?
3. Какие процедуры необходимо внедрить в организации для жизненного цикла учетной записи пользователя (создание, изменение прав, блокировка, удаление), чтобы обеспечить актуальность доступа и предотвратить появление «зомби-аккаунтов»?

Практическая работа 5. Обеспечение безопасности ресурсов с помощью разрешений файловой системы NTFS. Аудит ресурсов и событий системы защиты

1. Как разрешения NTFS позволяют реализовать гибкую модель управления доступом к файлам и папкам, и в чём состоит различие между разрешениями на уровне «разрешить» и «запретить» при наличии нескольких групповых членств?
2. Как наследование разрешений NTFS упрощает администрирование, и в каких случаях целесообразно его отключать или настраивать явным образом?
3. Как настройка аудита в NTFS и журналирование событий безопасности (через «Просмотр событий») помогают выявлять несанкционированные действия или нарушения политики безопасности, и какие типы событий наиболее критичны для мониторинга?

Практическая работа 6. Настройка системных параметров безопасности

1. Какие категории системных параметров безопасности (например, политики паролей, блокировка учётных записей, аудит входа в систему) наиболее критичны для защиты Windows-системы от несанкционированного доступа, и почему их настройка важнее установки антивируса?

2. Как инструмент «Локальная политика безопасности» (secpol.msc) или групповые политики (GPO) помогают централизованно управлять параметрами безопасности в корпоративной сети, и какие риски возникают при их некорректной конфигурации?
3. В чём заключается принцип «безопасности по умолчанию» (secure by default), и как настройка системных параметров (отключение ненужных служб, ограничение прав администратора, настройка UAC) способствует реализации этого принципа в современных операционных системах?

Практическая работа 7. Настройка параметров безопасности подключения к Интернет
1. Какие настройки безопасности веб-браузера (управление cookie, блокировка всплывающих окон, режим «не отслеживать», обновления) наиболее эффективно защищают пользователя от слежки, фишинга и вредоносного контента при подключении к Интернету?
2. Как настройка брандмауэра (межсетевого экрана) и параметров частной/публичной сети в операционной системе влияет на уровень защищённости устройства при подключении к различным типам интернет-соединений (домашний Wi-Fi, общественный hotspot, мобильная сеть)?
3. Какие дополнительные меры (использование HTTPS, DNS-over-HTTPS, VPN, двухфакторная аутентификация) следует применять при настройке подключения к Интернету для защиты конфиденциальности и целостности данных, особенно при работе с корпоративными или персональными ресурсами?

Практическая работа 8. Разработка алгоритмов криптографической защиты
1. Какие основные требования (стойкость к атакам, энтропия ключа, вычислительная сложность и др.) предъявляются к криптографическим алгоритмам при их разработке, и почему «секретность алгоритма» не является надёжной основой безопасности?
2. В чём заключаются различия между разработкой симметричных и асимметричных криптосистем, и какие математические проблемы лежат в основе их стойкости (например, факторизация, дискретный логарифм, эллиптические кривые)?
3. Как обеспечивается корректная реализация криптографического алгоритма на практике, и почему даже теоретически стойкий алгоритм может стать уязвимым из-за ошибок в программной реализации или управлении ключами?

## Раздел 5. Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине

Наряду с чтением лекций и проведением практических занятий неотъемлемым элементом учебного процесса является *самостоятельная работа.* При самостоятельной работе достигается конкретное усвоение учебного материала, развиваются теоретические способности, столь важные для успешной подготовки и защиты выпускной работы бакалавра. Формы самостоятельной работы, обучаемых могут быть разнообразными. Самостоятельная работа включает: изучение литературы, веб-ресурсов, оценку, обсуждение и рецензирование публикуемых статей; ответы на контрольные вопросы; решение задач; самотестирование. Выполнение всех видов самостоятельной работы увязывается с изучением конкретных тем.

Типовые задания для самостоятельной, представлены в фонде оценочных средств по дисциплине.

### 5.1. Индивидуальные задания для курсовых работ

Курсовая работа позволяет выявить степень владения базовыми знаниями, умениями необходимыми для обучения, и определить уровень владения новым материалом. Рекомендации по подготовке, оформлению и защите курсовой работы (курсового проекта), предусмотренной учебным планом, изложены в Методических указаниях по соответствующей дисциплине.

#### 5.1.1. Примерная тематика курсовых работ (проектов)

*Курсовая работа не предусмотрена учебным планом.*

## Раздел 6. Оценочные и методические материалы по образовательной программе (фонд оценочных средств) для проведения текущего контроля успеваемости и промежуточной аттестации

В процессе освоения учебной дисциплины для оценивания сформированности требуемых компетенций используются оценочные материалы (фонды оценочных средств).
Типовые тестовые задания, типовые практические задания, типовые задания для контрольных работ и материалы для диагностической работы представлены в фонде оценочных средств по дисциплине. Промежуточная аттестация проводится в форме зачета/ зачета с оценкой/экзамена.

### 6.1. Материалы для оценки результатов промежуточной аттестации

**Перечень вопросов для подготовки к промежуточной аттестации (зачёт)**

1. Основы информационной безопасности: понятие, цели и задачи.
2. Угрозы информационной безопасности и их классификация.
3. Методы и средства защиты информации.
4. Криптографические методы защиты информации.
5. Сетевые технологии и информационная безопасность.
6. Безопасность операционных систем и приложений.
7. Антивирусная защита и её роль в обеспечении информационной безопасности.
8. Управление доступом и аутентификация пользователей.
9. Резервное копирование и восстановление данных.
10. Законодательство и стандарты в области информационной безопасности.
11. Социальная инженерия как метод реализации угроз информационной безопасности.
12. Модели безопасности: дискреционная (DAC), мандатная (MAC), ролевая (RBAC) и атрибутная (ABAC).
13. Обнаружение и предотвращение вторжений (IDS/IPS): принципы работы и применение.
14. Безопасность беспроводных сетей (Wi-Fi, Bluetooth, мобильные сети).
15. Защита персональных данных: принципы, методы и требования законодательства (на примере ФЗ-152).
16. Инциденты информационной безопасности: классификация, расследование и реагирование.
17. Аудит и мониторинг информационных систем: цели, методы и инструменты.
18. Безопасность облачных вычислений (IaaS, PaaS, SaaS): риски и модели ответственности.
19. Проблемы безопасности в Интернете вещей (IoT) и встроенных системах.
20. Цифровая подпись и электронная аутентификация: технологии и применение.
21. Средства обеспечения конфиденциальности: шифрование данных на диске, в транзите и в памяти.
22. Политики информационной безопасности организации: разработка, внедрение и контроль.
23. Безопасность веб-приложений: типичные уязвимости (OWASP Top 10) и методы защиты.
24. Фишинг, спуфинг и другие виды мошенничества в цифровой среде.
25. Этический хакинг и тестирование на проникновение (penetration testing).
26. Защита корпоративной сети: межсетевые экраны, шлюзы, сегментация и DMZ.
27. Управление уязвимостями и патч-менеджмент в ИТ-инфраструктуре.
28. Кибербезопасность критически важных информационных инфраструктур (КИИ).
29. Международные стандарты информационной безопасности (ISO/IEC 27001, NIST, COBIT).
30. Будущие вызовы информационной безопасности: квантовые вычисления, ИИ и децентрализованные технологии.

### 6.2. Оценивание ответов на вопросы и выполнения заданий промежуточной аттестации

При оценке знаний учитывается уровень сформированности компетенций:
1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.

2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

**Шкала оценивания на экзамене, зачете с оценкой**

| Оценка | Критерии выставления оценки |
|---|---|
| Отлично | Обучающийся должен:<br>- продемонстрировать глубокое и прочное усвоение знаний программного материала;<br>- исчерпывающе, последовательно, грамотно и логически стройно изложить теоретический материал;<br>- правильно формулировать определения;<br>- продемонстрировать умения самостоятельной работы с литературой;<br>- уметь сделать выводы по излагаемому материалу. |
| Хорошо | Обучающийся должен:<br>- продемонстрировать достаточно полное знание программного материала;<br>- продемонстрировать знание основных теоретических понятий;<br>- достаточно последовательно, грамотно и логически стройно излагать материал;<br>- продемонстрировать умение ориентироваться в литературе;<br>- уметь сделать достаточно обоснованные выводы по излагаемому материалу. |
| Удовлетворительно | Обучающийся должен:<br>- продемонстрировать общее знание изучаемого материала;<br>- показать общее владение понятийным аппаратом дисциплины;<br>- уметь строить ответ в соответствии со структурой излагаемого вопроса;<br>- знать основную рекомендуемую программой учебную литературу. |
| Неудовлетворительно | Обучающийся демонстрирует:<br>- незнание значительной части программного материала;<br>- не владение понятийным аппаратом дисциплины;<br>- существенные ошибки при изложении учебного материала;<br>- неумение строить ответ в соответствии со структурой излагаемого вопроса;<br>- неумение делать выводы по излагаемому материалу. |

**Шкала оценивания на зачете**

| Оценка | Критерии выставления оценки |
|---|---|
| «Зачтено» | Обучающийся должен: уметь строить ответ в соответствии со структурой излагаемого вопроса; продемонстрировать прочное, достаточно полное усвоение знаний программного материала; продемонстрировать знание основных теоретических понятий; правильно формулировать определения; последовательно, грамотно и логически стройно изложить теоретический материал; продемонстрировать умения самостоятельной работы с литературой; уметь сделать достаточно обоснованные выводы по излагаемому материалу. |
| «Не зачтено» | Обучающийся демонстрирует: незнание значительной части программного материала; не владение понятийным аппаратом |

| | |
|---|---|
| | дисциплины; существенные ошибки при изложении учебного материала; неумение строить ответ в соответствии со структурой излагаемого вопроса; неумение делать выводы по излагаемому материалу. |

**Методические материалы, определяющие процедуру оценивания сформированных компетенций в соответствии с ООП**

***Качество знаний*** характеризуется способностью обучающегося точно, структурированно и уместно воспроизводить информацию, полученную в процессе освоения дисциплины, в том виде, в котором она была изложена в учебном издании или преподавателем.

Умения, как правило, формируются на занятиях семинарского типа. Задания, направленные на оценку умений, в значительной степени требуют от обучающегося проявления стереотипности мышления, т.е. способности выполнить работу по образцам, с которыми он работал в процессе обучения. Преподаватель же оценивает своевременность и правильность выполнения задания.

***Навыки*** можно трактовать как автоматизированные умения, развитые и закрепленные осознанным самостоятельным трудом. Навыки формируются при самостоятельном выполнении обучающимися практико ориентированных заданий, моделирующих решение им производственных и социокультурных задач в соответствующей области профессиональной деятельности, как правило, при выполнении домашних заданий, курсовых проектов (работ), научно-исследовательских работ, прохождении практик, при работе индивидуально или в составе группы и т.д.

***Устный опрос*** – это процедура, организованная как специальная беседа преподавателя с группой обучающихся (фронтальный опрос) или с отдельными обучающимися (индивидуальный опрос) с целью оценки сформированности у них основных понятий и усвоения учебного материала. Устный опрос может использоваться как вид контроля и метод оценивания формируемых компетенций (как и качества их формирования) в рамках самых разных форм контроля, таких как: собеседование, коллоквиум, зачет, экзамен по дисциплине. Устный опрос (УО) позволяет оценить знания и кругозор обучающегося, умение логически построить ответ, владение монологической речью и иные коммуникативные навыки. УО обладает большими возможностями воспитательного воздействия преподавателя. Воспитательная функция УО имеет ряд важных аспектов: профессионально-этический и нравственный аспекты, дидактический (систематизация материала при ответе, лучшее запоминание материала при интеллектуальной концентрации), эмоциональный (радость от успешного прохождения собеседования) и др. Обучающая функция УО состоит в выявлении деталей, которые по каким-то причинам оказались недостаточно осмысленными в ходе учебных занятий и при подготовке к зачёту или экзамену. УО обладает также мотивирующей функцией: правильно организованные собеседование, коллоквиум, зачёт и экзамен могут стимулировать учебную деятельность студента, его участие в научной работе.

***Тесты*** являются простейшей формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин. Тест может предоставлять возможность выбора из перечня ответов (один или несколько правильных ответов).

***Семинарские занятия***. Основное назначение семинарских занятий по дисциплине – обеспечить глубокое усвоение обучающимися материалов лекций, прививать навыки самостоятельной работы с литературой, воспитывать умение находить оптимальные решения в условиях изменяющихся отношений, формировать современное профессиональное мышление обучающихся. На семинарских занятиях преподаватель проверяет выполнение самостоятельных заданий и качество усвоения знаний, умений, определяет уровень сформированности компетенций.

## Раздел 7. Методические указания для обучающихся по основанию дисциплины

Освоение обучающимся учебной дисциплины предполагает изучение материалов дисциплины на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проходят в форме лекций, семинаров и практических занятий. Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся.

Для успешного освоения учебной дисциплины и достижения поставленных целей необходимо внимательно ознакомиться с настоящей рабочей программы учебной дисциплины. Следует обратить внимание на список основной и дополнительной литературы, которая имеется в электронной библиотечной системе Университета. Эта информация необходима для самостоятельной работы обучающегося.

При подготовке к аудиторным занятиям необходимо помнить особенности каждой формы его проведения.

Подготовка к учебному занятию лекционного типа. С целью обеспечения успешного обучения обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку: знакомит с новым учебным материалом; разъясняет учебные элементы, трудные для понимания; систематизирует учебный материал; ориентирует в учебном процессе.

С этой целью: внимательно прочитайте материал предыдущей лекции; ознакомьтесь с учебным материалом по учебнику и учебным пособиям с темой прочитанной лекции; внесите дополнения к полученным ранее знаниям по теме лекции на полях лекционной тетради; запишите возможные вопросы, которые вы зададите лектору на лекции по материалу изученной лекции; постарайтесь уяснить место изучаемой темы в своей подготовке; узнайте тему предстоящей лекции (по тематическому плану, по информации лектора) и запишите информацию, которой вы владеете по данному вопросу

Предварительная подготовка к учебному занятию семинарского типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач занятия.

Самостоятельная работа. Для более углубленного изучения темы задания для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темы. При выполнении заданий по возможности используйте наглядное представление материала.

Подготовка к зачету, экзамену. К зачету, экзамену необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить учебную дисциплину в период зачетно-экзаменационной сессии, как правило, приносят не слишком удовлетворительные результаты. При подготовке к зачету обратите внимание на защиту практических заданий на основе теоретического материала. При подготовке к экзамену по теоретической части выделите в вопросе главное, существенное (понятия, признаки, классификации и пр.), приведите примеры, иллюстрирующие теоретические положения.

## Раздел 8. Учебно-методическое и информационное обеспечение дисциплины

### *Основная литература*

1. Бондаренко, И. С. Информационная безопасность: учебник / И. С. Бондаренко. — Москва: Издательский Дом МИСиС, 2023. — 254 с. — ISBN 978-5-907560-71-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/137525.html

2. Галатенко, В. А. Основы информационной безопасности: учебное пособие / В. А. Галатенко. - 3-е изд. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. - 266 с. - ISBN 978-5-4497-0675-1. - Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. - URL: https://www.IPRsmart hop.ru/97562.html

3. Фомин, Д. В. Информационная безопасность: учебник / Д. В. Фомин. — Москва: Ай Пи Ар Медиа, 2022. — 222 с. — ISBN 978-5-4497-1548-7. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/118876.html

***Дополнительная литература***

1. Суворова, Г. М. Информационная безопасность: учебное пособие / Г. М. Суворова. — 2-е изд. — Саратов: Вузовское образование, 2024. — 214 c. — ISBN 978-5-4487-1026-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/142805.html

2. Овчинникова, Е. А. Информационная безопасность: учебное пособие для СПО / Е. А. Овчинникова. — Саратов: Профобразование, 2024. — 166 c. — ISBN 978-5-4488-1872-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/139028.html

**8.1 Требования к материально-техническому и учебно-методическому обеспечению**

8.1.1. Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой магистратуры, оснащенные оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей).

В Университете имеются специализированные аудитории для проведения занятий по информационным технологиям.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде Университета.

**Электронная информационно-образовательная среда Университета включает:**

1. Официальный сайт Университета (https://www.iile.ru/)
2. Электронная информационно-образовательная среда «1С: Университет» договор от 10.09.2018 г. №ПРКТ-18281 (бессрочно)
3. Программы для ЭВМ. Система дистанционного обучения «Mirapolis» - Лицензионный договор №107/06/24-к от 27.06.2024 (Спецификация к Лицензионному договору №107/06/24-к от 27.06.2024, срок действия с 01.07.2026 по 30.06.2027 г.) https://impe.lms.mirapolis.ru/mira/
4. Программа для ЭВМ. Виртуальная комната «Mirapolis» - Лицензионный договор №107/06/24-к от 27.06.2024 (Спецификация к Лицензионному договору №107/06/24-к от 27.06.2024, срок действия с 01.07.2026 по 30.06.2027 г.) https://impe.lms.mirapolis.ru/mira/
5. Система тестирования INDIGO лицензионное соглашение (Договор от 07.11.2018 г. №Д-54792, бессрочно) http://212.48.35.211:85/

8.1.2. Университет обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства (состав определяется в рабочих программах дисциплин (модулей) и подлежит обновлению при необходимости).

**Перечень лицензионного программного обеспечения, в том числе отечественного производства:**

1. Операционная система «Атлант» - Atlant Academ от 24.01.2024 г. (бессрочно)
2. Антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition договор-оферта № Tr000941765 от 16.10.2025 г.

8.1.3. Обучающимся обеспечен доступ (удаленный доступ) к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в рабочих программах дисциплин (модулей) и обновляется при необходимости, но не реже одного раз в год.

**Перечень современных профессиональных баз данных и информационных справочных систем:**

1. Информационно-поисковая система «Консультант Плюс» - Договор №МИ-ВИП-79717-56/2022 (бессрочно)
2. Электронно-библиотечная система IPRsmart лицензионный договор от 01.09.2024 г. №11652/24С (срок действия до 31.08.2027 г.) https://www.iprbookshop.ru/
3. Научная электронная библиотека eLIBRARY лицензионный договор SCIENC INDEX № SIO - 3079/2026 от 30.01.2026 г. (срок действия до 29.01.2027г.) https://elibrary.ru

8.1.4. Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

**Раздел 9. Материально-техническое обеспечение образовательного процесса**

| | |
|---|---|
| Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации | Оборудование: специализированная мебель (мебель аудиторная (столы, стулья, доска аудиторная навесная), стол преподавателя, стул преподавателя.<br>Технические средства обучения: персональный компьютер; мультимедийное оборудование (проектор, экран). |
| Помещение для самостоятельной работы | Специализированная мебель (столы, стулья), персональные компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета |