

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Узунов Федор Владимирович

Должность: Ректор

Дата подписания: 30.09.2026 09:20:02

Уникальный программный ключ: fd935d10451b860e912264c0378f8448452b603f94388008e29877a6bcb55

**АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ  
«ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ»  
«УНИВЕРСИТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ»  
Факультет экономики, управления и юриспруденции  
Кафедра «Управление и бизнес-информатика»**



**УТВЕРЖДАЮ**

Проректор по учебно-методической работе

*Г.П. Узунова*

«02» февраля 2026 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Методы оценки безопасности компьютерных систем**

Направление подготовки

**10.03.01 «Информационная безопасность»**

Профиль

**Безопасность компьютерных систем**

Квалификация выпускника

*Бакалавр*

Для всех

форм обучения

Симферополь, 2026

Рабочая программа составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки 10.03.01 «Информационная безопасность» профиль Безопасность компьютерных систем, утвержденным приказом Министерства образования и науки Российской Федерации от 17.11.2020 г. № 1427 (зарегистрировано в Министерстве юстиции РФ 18.02.2021 №62548) с изменениями и дополнениями.

Программу составил Л. В. Яковенко, старший преподаватель

Рабочая программа дисциплины «Методы оценки безопасности компьютерных систем» утверждена на заседании кафедры «Управление и бизнес-информатика».

Протокол № 6 от 29.01.2026 г.

Заведующий кафедрой  Д.В. Моторина  
(подпись)

| <b>АННОТАЦИЯ</b>                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Индекс дисциплины по учебному плану                       | Наименование дисциплины                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Б1.О.33</b>                                            | <b>Методы оценки безопасности компьютерных систем</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Цель изучения дисциплины                                  | формирование у студентов профессиональных компетенций, необходимых для разработки, анализа безопасности и практического внедрения комплексных мер по защите программного обеспечения (ПО) и обрабатываемой им информации от несанкционированного доступа, исследования, модификации и тиражирования.                                                                                                                                                                                                                                                                                                                                                                  |
| Место дисциплины в структуре ОПОП                         | Дисциплина относится к обязательной части блока 1. «Дисциплины (модули)» программы бакалавриата                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Компетенции, формируемые в результате освоения дисциплины | ОПК-12                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Содержание дисциплины                                     | <p>Тема 1. Теоретические модели безопасности и формальные методы верификации.</p> <p>Тема 2. Международные стандарты оценки безопасности: Критерии Common Criteria (ISO/IEC 15408) Детально рассматривается универсальный методологический аппарат для.</p> <p>Тема 3. Методы анализа защищенности исходного кода: статический (SAST) и динамический (DAST).</p> <p>Тема 4. Методология количественной и качественной оценки рисков информационной безопасности.</p> <p>Тема 5. Тестирование на проникновение (Penetration Testing) и аудит соответствия техническим требованиям</p> <p>Тема 6. Оценка надежности компьютерных систем и теория отказоустойчивости</p> |
| Общая трудоемкость дисциплины                             | Общая трудоемкость дисциплины составляет 5 зачетные единицы (180часов)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Форма промежуточной аттестации                            | Экзамен/                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## Содержание

|                                                                                                                                                                                                                 |    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 1. Цель и перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы бакалавриата                                                                     | 5  |
| 2. Место дисциплины в структуре ОПОП бакалавриата                                                                                                                                                               | 5  |
| 3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся     | 5  |
| 4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий                                                           | 6  |
| 5. Контроль качества освоения дисциплины                                                                                                                                                                        | 11 |
| 6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины                                                                                                                   | 11 |
| 7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины                                                                                                    | 12 |
| 8. Методические указания для обучающихся по освоению дисциплины                                                                                                                                                 | 13 |
| 9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости) | 13 |
| 10. Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине                                                                                       | 14 |
|                                                                                                                                                                                                                 | 15 |

## 1. Цель и перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы бакалавриата

Цель изучения дисциплины «Методы оценки безопасности компьютерных систем» – формирование у студентов профессиональных компетенций, необходимых для разработки, анализа безопасности и практического внедрения комплексных мер по защите программного обеспечения (ПО) и обрабатываемой им информации от несанкционированного доступа, исследования, модификации и тиражирования.

В результате освоения ОПОП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине:

| Коды компетенции | Результаты освоения ОПОП                                                                                                                                                                     | Перечень планируемых результатов обучения по дисциплине                                                                                                                                                                               |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ОПК-12</b>    | Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений | ОПК-12.1. Формирует требования и разрабатывает внешние спецификации для разрабатываемого программного обеспечения<br>ОПК-12.2. Разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений |

## 2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина Б1.О.33 «Методы оценки безопасности компьютерных систем» относится к обязательной части блока 1. «Дисциплины (модули)» учебного плана ОПОП бакалавриата по направлению подготовки 10.03.02 «Информационная безопасность». Дисциплина «Информационные технологии в профессиональной деятельности» изучается обучающимися очной формы обучения в 7 семестре, очно-заочной формы обучения – в 7 семестре.

Знания, умения и навыки, полученные при изучении дисциплины «Методы оценки безопасности компьютерных систем», будут необходимы для углубленного и осмысленного восприятия дисциплин: Операционные системы и др.

## 3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 5 зачетных единицы (з.е.), 180 академических часа.

### 3.1. Объём дисциплины по видам учебных занятий (в часах)

Для очной формы обучения

Общая трудоёмкость дисциплины составляет 5 зачётных единицы 180 часа

| Объём дисциплины                           | Всего часов |
|--------------------------------------------|-------------|
| Общая трудоёмкость дисциплины              | 180         |
| Контактная работа                          | 52          |
| Аудиторная работа (всего):                 | 52          |
| Лекции                                     | 18          |
| Семинары, практические занятия             | 34          |
| Самостоятельная работа обучающихся (всего) | 92          |
| Курсовая работа                            | -           |
| Зачет                                      | -           |
| Экзамен                                    | 36          |

#### Для очно-заочной формы обучения

Общая трудоёмкость дисциплины составляет 5 зачётных единицы 180 часа

| Объём дисциплины                           | Всего часов |
|--------------------------------------------|-------------|
| Общая трудоёмкость дисциплины              | 180         |
| Контактная работа                          | 40          |
| Аудиторная работа (всего):                 | 40          |
| Лекции                                     | 20          |
| Семинары, практические занятия             | 20          |
| Самостоятельная работа обучающихся (всего) | 104         |
| Курсовая работа                            | -           |
| Зачет                                      | -           |
| Экзамен                                    | 36          |

#### 4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

##### 4.1. Разделы дисциплины и трудоёмкость по видам учебных занятий (в академических часах)

| № темы | Наименование темы                                                                                      | Всего |      | Количество часов  |      |              |      |                  |      |
|--------|--------------------------------------------------------------------------------------------------------|-------|------|-------------------|------|--------------|------|------------------|------|
|        |                                                                                                        | ОФО   | ОЗФО | Контактная работа |      |              |      | Внеаудит. работа |      |
|        |                                                                                                        |       |      | Лекции            |      | Практические |      | Самост. работа   |      |
|        |                                                                                                        |       |      | ОФО               | ОЗФО | ОФО          | ОЗФО | ОФО              | ОЗФО |
| 1.     | Тема 1. Теоретические модели безопасности и формальные методы верификации.                             | 34    | 34   | 2                 | 2    | 4            | 2    | 28               | 30   |
| 2.     | Тема 2. Международные стандарты оценки безопасности: Критерии Common Criteria (ISO/IEC 15408) Детально | 34    | 34   | 4                 | 2    | 4            | 2    | 28               | 30   |

|    |                                                                                                          |            |            |    |    |    |    |    |     |
|----|----------------------------------------------------------------------------------------------------------|------------|------------|----|----|----|----|----|-----|
|    | рассматривается универсальный методологический аппарат для.                                              |            |            |    |    |    |    |    |     |
| 3. | Тема 3. Методы анализа защищенности исходного кода: статический (SAST) и динамический (DAST).            | 34         | 34         | 4  | 2  | 4  | 2  | 28 | 30  |
| 4. | Тема 4. Методология количественной и качественной оценки рисков информационной безопасности.             | 34         | 32         | 4  | 1  | 4  | 1  | 28 | 30  |
| 5. | Тема 5. Тестирование на проникновение (Penetration Testing) и аудит соответствия техническим требованиям | 32         | 32         | 4  | 1  | 4  | 1  | 28 | 30  |
| 6. | Тема 6. Оценка надежности компьютерных систем и теория отказоустойчивости                                | 36         | 30         | 6  | 2  | 6  | 2  | 24 | 26  |
|    | Всего по дисциплине                                                                                      | 144        | 144        | 18 | 20 | 34 | 20 | 92 | 104 |
|    | Контроль                                                                                                 | 36         | 36         |    |    |    |    |    |     |
|    | <b>Итого</b>                                                                                             | <b>180</b> | <b>180</b> |    |    |    |    |    |     |

#### 4.2. Содержание дисциплины, структурированное по темам (разделам)

**Тема 1. Теоретические модели безопасности и формальные методы верификации** Раскрывается математический фундамент оценки защищенности систем. Изучаются классические политики управления доступом: дискреционная (DAC), мандатная (MAC, модель Белла-ЛаПадулы для конфиденциальности, модель Биба для целостности) и ролевая (RBAC). Рассматривается использование теории решеток для построения иерархий уровней секретности. Практическая часть посвящена анализу состояния системы через переходы состояний (State Transition Models) и применению формальных языков спецификаций (Z-notation, B-Method) для доказательства отсутствия логических уязвимостей в архитектуре программного обеспечения до начала его написания.

**Тема 2. Международные стандарты оценки безопасности: Критерии Common Criteria (ISO/IEC 15408)** Детально рассматривается универсальный методологический аппарат для сертификации средств защиты информации. Раскрывается структура профиля защиты (Protection Profile — PP) и задания по безопасности (Security Target — ST). Изучается система оценочных уровней доверия (EAL1–EAL7): от простого функционального тестирования до полуформальное проектирования и верификации. Анализируется процесс проведения испытаний независимой аккредитованной лабораторией, определение объектов оценки (Target of Evaluation — TOE) и описание среды безопасности. Тема включает разбор российских интерпретаций стандарта в рамках требований ФСТЭК России.

**Тема 3. Методы анализа защищенности исходного кода: статический (SAST) и динамический (DAST) анализ** Изучаются технологии поиска программных закладок и ошибок реализации на уровне кода. *Статический анализ (SAST)*: исследование абстрактного синтаксического дерева программы без ее запуска. Рассматриваются алгоритмы taint-анализа (отслеживание потока данных от недоверенных источников к

чувствительным функциям), символьное выполнение (*Symbolic Execution*) и поиск типовых паттернов уязвимостей из перечня *CWE*. *Динамический анализ (DAST)*: тестирование работающего приложения. Включает фаззинг (*Fuzzing*) — подачу случайных или некорректных входных данных для вызова сбоев, а также инструменты интерактивного анализа приложений (*IAST*). Сравниваются преимущества гибридных методов (*Гибридный анализ*) для снижения количества ложноположительных срабатываний сканеров.

**Тема 4. Методология количественной и качественной оценки рисков информационной безопасности** Раскрываются подходы к измерению уровня опасности для бизнес-процессов организации. Изучаются качественные методы: матрицы вероятности и последствий, опросы экспертов, построение диаграмм Исикавы («рыбья кость»). Детально разбираются количественные методики: *FAIR (Factor Analysis of Information Risk)*: расчет ожидаемых годовых потерь (*ALE*) через оценку частоты возникновения событий (*ARO*) и величины потери (*SLE*). *CVSS (Common Vulnerability Scoring System)*: алгоритм вычисления метрики опасности конкретной уязвимости на основе базовых, временных и контекстных показателей. Цель темы — научить переводить технические недостатки ИТ-инфраструктуры на язык финансовых и операционных рисков руководства компании.

**Тема 5. Тестирование на проникновение (Penetration Testing) и аудит соответствия техническим требованиям** Рассматривается активный метод оценки, имитирующий действия злоумышленника. Раскрывается стандарт проведения тестов *PTES (Penetration Testing Execution Standard)*. Изучаются этапы жизненного цикла теста: сбор разведданных (*OSINT*), сканирование сети, эксплуатация уязвимостей, закрепление в системе (*Post-Exploitation*) и составление отчета. Особое внимание уделяется правилам взаимодействия (*RoE — Rules of Engagement*) во избежание нарушения работы критически важных систем. Параллельно изучается технический аудит конфигураций на соответствие «твердым» стандартам (*CIS Benchmarks, DISA STIGs*).

**Тема 6. Оценка надежности компьютерных систем и теория отказоустойчивости** Тема фокусируется не только на защите от атак, но и на оценке способности системы сохранять работоспособность при сбоях. Изучаются основные показатели надежности: среднее время наработки на отказ (*MTBF*), среднее время восстановления (*MTTR*) и коэффициент готовности ( $Availability = MTBF / (MTBF + MTTR)$ ). Рассматриваются инженерные методы повышения надежности: резервирование компонентов (*N+1, 2N*), кластеризация серверов, механизмы контрольных точек (*checkpointing*) и изоляция отказов (*fault isolation*). Проводится граница между надежностью (случайные отказы оборудования/софта) и безопасностью (целенаправленные действия нарушителя), показывая их взаимозависимость в рамках единой модели доступности сервиса.

#### 4.3. Содержание практических занятий (очная форма обучения)

**Тема 1. Теоретические модели безопасности и формальные методы верификации** Раскрывается математический фундамент оценки защищенности систем. Изучаются классические политики управления доступом: дискреционная (*DAC*), мандатная (*MAC*, модель Белла-ЛаПадуды для конфиденциальности, модель Биба для целостности) и ролевая (*RBAC*). Рассматривается использование теории решеток для построения иерархий уровней секретности.

**Тема 2. Международные стандарты оценки безопасности: Критерии Common Criteria (ISO/IEC 15408)** Детально рассматривается универсальный методологический аппарат для сертификации средств защиты информации. Раскрывается структура

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>профиля защиты (<i>Protection Profile — PP</i>) и задания по безопасности (<i>Security Target — ST</i>). Изучается система оценочных уровней доверия (<i>EAL1–EAL7</i>): от простого функционального тестирования до полуформального проектирования и верификации.</p>                                                                                                                                                                                                                                                                                                                                                             |
| <p><b>Тема 3. Методы анализа защищенности исходного кода: статический (SAST) и динамический (DAST) анализ</b> Изучаются технологии поиска программных закладок и ошибок реализации на уровне кода. <i>Статический анализ (SAST)</i>: исследование абстрактного синтаксического дерева программы без ее запуска. Рассматриваются алгоритмы taint-анализа (отслеживание потока данных от недоверенных источников к чувствительным функциям), символьное выполнение (<i>Symbolic Execution</i>) и поиск типовых паттернов уязвимостей из перечня <i>CWE</i>. <i>Динамический анализ (DAST)</i>: тестирование работающего приложения.</p> |
| <p><b>Тема 4. Методология количественной и качественной оценки рисков информационной безопасности</b> Раскрываются подходы к измерению уровня опасности для бизнес-процессов организации. Изучаются качественные методы: матрицы вероятности и последствий, опросы экспертов, построение диаграмм Исикавы («рыбья кость»). Детально разбираются количественные методики: <i>FAIR (Factor Analysis of Information Risk)</i>: расчет ожидаемых годовых потерь (<i>ALE</i>) через оценку частоты возникновения событий (<i>ARO</i>) и величины потери (<i>SLE</i>).</p>                                                                  |
| <p><b>Тема 5. Тестирование на проникновение (Penetration Testing) и аудит соответствия техническим требованиям</b> Рассматривается активный метод оценки, имитирующий действия злоумышленника. Раскрывается стандарт проведения тестов <i>PTES (Penetration Testing Execution Standard)</i>. Изучаются этапы жизненного цикла теста: сбор разведанных (<i>OSINT</i>), сканирование сети, эксплуатация уязвимостей, закрепление в системе (<i>Post-Exploitation</i>) и составление отчета.</p>                                                                                                                                         |
| <p><b>Тема 6. Оценка надежности компьютерных систем и теория отказоустойчивости</b> Тема фокусируется не только на защите от атак, но и на оценке способности системы сохранять работоспособность при сбоях. Изучаются основные показатели надежности: среднее время наработки на отказ (<i>MTBF</i>), среднее время восстановления (<i>MTTR</i>) и коэффициент готовности (<math>Availability = MTBF / (MTBF + MTTR)</math>).</p>                                                                                                                                                                                                    |

#### 4.4. Содержание самостоятельной работы

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Тема 1. Теоретические модели безопасности и формальные методы верификации</b> Практическая часть посвящена анализу состояния системы через переходы состояний (<i>State Transition Models</i>) и применению формальных языков спецификаций (<i>Z-notation</i>, <i>B-Method</i>) для доказательства отсутствия логических уязвимостей в архитектуре программного обеспечения до начала его написания.</p>                                                                                                |
| <p><b>Тема 2. Международные стандарты оценки безопасности: Критерии Common Criteria (ISO/IEC 15408)</b> Анализируется процесс проведения испытаний независимой аккредитованной лабораторией, определение объектов оценки (<i>Target of Evaluation — TOE</i>) и описание среды безопасности. Тема включает разбор российских интерпретаций стандарта в рамках требований ФСТЭК России.</p>                                                                                                                     |
| <p><b>Тема 3. Методы анализа защищенности исходного кода: статический (SAST) и динамический (DAST) анализ</b> <i>Динамический анализ (DAST)</i>: тестирование работающего приложения. Включает фаззинг (<i>Fuzzing</i>) — подачу случайных или некорректных входных данных для вызова сбоев, а также инструменты интерактивного анализа приложений (<i>IAST</i>). Сравниваются преимущества гибридных методов (<i>Гибридный анализ</i>) для снижения количества ложноположительных срабатываний сканеров.</p> |

**Тема 4. Методология количественной и качественной оценки рисков информационной безопасности CVSS (Common Vulnerability Scoring System):** алгоритм вычисления метрики опасности конкретной уязвимости на основе базовых, временных и контекстных показателей. Цель темы — научить переводить технические недостатки ИТ-инфраструктуры на язык финансовых и операционных рисков руководства компании.

**Тема 5. Тестирование на проникновение (Penetration Testing) и аудит соответствия техническим требованиям** Особое внимание уделяется правилам взаимодействия (RoE — Rules of Engagement) во избежание нарушения работы критически важных систем. Параллельно изучается технический аудит конфигураций на соответствие «твердым» стандартам (CIS Benchmarks, DISA STIGs).

**Тема 6. Оценка надежности компьютерных систем и теория отказоустойчивости** Граница между надежностью (случайные отказы оборудования/софта) и безопасностью (целенаправленные действия нарушителя), показывая их взаимозависимость в рамках единой модели доступности сервиса.

## 5. Контроль качества освоения дисциплины

Текущий контроль и промежуточная аттестация осуществляются в соответствии с «Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся в Автономной некоммерческой организации «Образовательная организация высшего образования» «Университет экономики и управления».

Вид промежуточной аттестации – экзамен. Форма проведения промежуточной аттестации – письменный экзамен.

Фонд оценочных средств по дисциплине приведен в приложении к РПД.

## 6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

### а) основная литература:

1. Батуро, А. Н. Конфигурирование ИТ-инфраструктуры. Прикладное программное обеспечение под ОС Astra Linux Special Edition : учебное пособие для СПО / А. Н. Батуро, Г. М. Бойко. — Москва : Ай Пи Ар Медиа, 2026. — 344 с. — ISBN 978-5-4497-5384-7. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/161012/details> (дата обращения: 27.01.2026). — Режим доступа: для авторизир. пользователей

2. Мельников, А. В. Основы информационной безопасности : учебное пособие / А. В. Мельников, С. В. Зарубин. — Москва : Российский государственный университет правосудия имени В.М. Лебедева, 2025. — 220 с. — ISBN 978-5-00209-188-1. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/152309/details> (дата обращения: 27.01.2026). — Режим доступа: для авторизир. пользователей

### б) дополнительная литература:

3. Баженова, И. Ю. Введение в программирование : учебное пособие / И. Ю. Баженова, В. А. Сухомлин. — 5-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2026. — 326 с. — ISBN 978-5-4497-3298-9. — Текст : электронный // Образовательная платформа IPR SMART : [сайт].

— URL: <https://www.iprbookshop.ru/books/162502/details> (дата обращения: 27.01.2026). — Режим доступа: для авторизир. пользователей

4. Основы информационных технологий : учебное пособие / С. В. Назаров, С. Н. Белоусова, И. А. Бессонова [и др.]. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 530 с. — ISBN 978-5-4497-0339-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/89454.html> (дата обращения: 16.01.2026). — Режим доступа: для авторизир. пользователей.

## **7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**

1. Информационно-правовой портал «Гарант»: официальный сайт. — URL: <http://www.garant.ru> — Текст: электронный.

2. Цифровой образовательный ресурс «IPRsmart»: официальный сайт. — URL: <http://www.iprbookshop.ru/> — Текст: электронный.

3. Научная электронная библиотека «КиберЛенинка»: официальный сайт. — URL: <https://cyberleninka.ru/> — Текст: электронный.

4. Российский интернет-портал и аналитическое агентство TAdviser: официальный сайт. — URL: <https://www.tadviser.ru/> — Текст: электронный.

## **8. Методические указания для обучающихся по освоению дисциплины**

При проведении лекций, семинарских (практических) занятий, самостоятельной работе обучающихся применяются интерактивные формы проведения занятий с целью погружения обучающихся в реальную атмосферу профессионального сотрудничества по разрешению проблем, оптимальной выработки навыков и качеств будущего специалиста. Интерактивные формы проведения занятий предполагают обучение в сотрудничестве. Все участники образовательного процесса (преподаватель и обучающиеся) взаимодействуют друг с другом, обмениваются информацией, совместно решают проблемы, моделируют ситуацию.

В учебном процессе используются интерактивные формы занятий:

- творческое задание. Выполнение творческих заданий требует от обучающегося воспроизведение полученной ранее информации в форме, определяемой преподавателем, и требующей творческого подхода;

- групповое обсуждение. Групповое обсуждение кого-либо вопроса направлено на достижение лучшего взаимопонимания и способствует лучшему усвоению изучаемого материала.

В ходе освоения дисциплины при проведении контактных занятий используются следующие формы обучения, способствующие формированию компетенций: лекции-дискуссии; кейс-метод; решение задач; ситуационный анализ; обсуждение рефератов и докладов; разработка групповых проектов; встречи с представителями государственных и общественных организаций.

## **9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)**

В процессе лекционных и практических занятий используется следующее программное обеспечение:

- \*программы, обеспечивающие доступ в сеть «Интернет» (например, «Microsoft Edge», «Google Chrome»);
- \*программы, демонстрации видео материалов (например, проигрыватель «Windows Media Player»);
- \*текстовые редакторы и процессоры (например, «Microsoft Office Word»);
- \*табличные процессоры (например, «Microsoft Office Excel»);
- \*системы управления базами данных (например, «Microsoft Office Access»);
- \*программы для демонстрации и создания презентаций (например, «Microsoft PowerPoint»);
- \*проблемно-ориентированные пакеты прикладных программ по отраслям и сферам деятельности (например, «1С: Управление нашей фирмой», «Loginom Community Edition»).

#### **10. Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине**

##### **Учебная аудитория**

###### Оборудование учебной аудитории:

рабочее место преподавателя; посадочные места по количеству обучающихся;

доска классная;

стенды информационные;

Учебно-наглядные пособия: компьютеры с лицензионным программным обеспечением и возможностью подключения к информационно-телекоммуникационной сети Интернет; мультимедийная установка.

###### **Помещение для самостоятельной работы обучающихся**

оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.