Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего

образования «Московский государственный технический университет имени

Н.Э. Баумана (национальный исследовательский университет)»

(МГТУ им. Н.Э. Баумана)

|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ  Первый проректор – проректор по учебной работе  МГТУ им. Н.Э. Баумана  \_\_\_\_\_\_\_\_\_\_\_\_ Б.В. Падалкин  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_ г. |

Факультет «Информатика и системы управления»

Кафедра ИУ5 «Системы обработки информации и управления»

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**«Защита информации»**

для направления подготовки (уровень бакалавриата):

09.03.01 «Информатика и вычислительная техника»

**Автор(ы) программы:**

Варламов О.О., профессор, дтн, с.н.с.

[varlamovoo@bmstu.ru](mailto:ovar@narod.ru)

Москва, 201\_

Автор(ы) программы:

Варламов О.О. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Рецензент:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Утверждена на заседании кафедры ИУ5 «Системы обработки информации и управления»

Протокол №\_\_\_ от «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_201\_ г.

Заведующий кафедрой ИУ5

Чёрненький В.М. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Декан факультета «Информатика и системы управления»

Пролетарский А.В. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Согласовано:

Декан факультета «Информатика и системы управления»

Пролетарский А.В. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Начальник Управления образовательных стандартов и программ

Гузева Т.А. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Оглавление

[1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 4](#_Toc524269566)

[2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 12](#_Toc524269567)

[3. ОБЪЕМ ДИСЦИПЛИНЫ 13](#_Toc524269568)

[4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО МОДУЛЯМ С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ИЛИ АСТРОНОМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ 14](#_Toc524269569)

[5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ 20](#_Toc524269570)

[6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ 21](#_Toc524269571)

[7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ 22](#_Toc524269572)

[8. ПЕРЕЧЕНЬ РЕСУРСОВ СЕТИ ИНТЕРНЕТ, РЕКОМЕНДУЕМЫХ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПРИ ОСВОЕНИИ ДИСЦИПЛИНЫ 24](#_Toc524269573)

[9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ СТУДЕНТОВ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ 25](#_Toc524269574)

[10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ 26](#_Toc524269575)

[11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ 27](#_Toc524269576)

# **1.** **ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

Настоящая рабочая программа дисциплины устанавливает требования к знаниям и умениям студента, а также определяет содержание и виды учебных занятий и отчетности.

Программа разработана в соответствии с основной профессиональной образовательной программой (ОПОП) и учебным планом МГТУ им. Н.Э. Баумана, составленными на основе самостоятельно устанавливаемого образовательного стандарта (СУОС 3++) по направлению подготовки 09.03.01 «Информатика и вычислительная техника».

При освоении дисциплины планируется формирование компетенций, предусмотренных ОПОП на основе СУОС 3++ по направлению подготовки 09.03.01 «Информатика и вычислительная техника» (уровень бакалавриата).

| **Код компетенции по СУОС 3++** | **Формулировка компетенции** |
| --- | --- |
|  | **Общепрофессиональные компетенции собственные** |
| ОПКС-1 | Способен применять естественнонаучные и общеинженерные знания, методы математического моделирования, анализа, и синтеза, теоретического и экспериментального исследования в профессиональной деятельности |
| ОПКС-2 | Способен использовать современные информационные технологии и программные средства отечественного и иностранного производства при решении задач профессиональной деятельности |
| ОПКС-3 | Способен решать стандартные задачи профессиональной деятельности на основе математической, информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности |
| ОПКС-5 | Способен собирать аппаратуру, и инсталлировать отечественное и иностранное программное обеспечение для информационных и автоматизированных систем |
|  | **Универсальные компетенции собственные** |
| УКС-1 | Способен осуществлять поиск, критический анализ и синтез информации, ее смысловую оптимизацию и наглядное представление, применять системный подход для решения поставленных задач; использовать основы философских знаний и анализировать закономерности исторического развития общества для формирования мировоззрения и гражданской позиции. |
| УКС-2 | Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, опираясь на экономические знания и исходя из действующих правовых норм, имеющихся ресурсов и технологий |
| УКС-3 | Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде, толерантно воспринимая социальные и культурные и иные различия |
| УКС-4 | Способен осуществлять деловую коммуникацию и межличностное взаимодействие в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах) |
| УКС-6 | Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов самоорганизации и образования в течение всей жизни, а также самостоятельно приобретать знания. |
|  | **Профессиональные компетенции собственные (обязательные)** |
| ПКСо-1 | Способен участвовать в исследовательских и опытно-конструкторских разработках в области создания и совершенствования ИТ-систем |
|  | **Профессиональные компетенции собственные** |
| ПКС-6 | Способен выполнять и управлять работами по созданию (модификации) и сопровождению информационных систем, автоматизирующих задачи организационного управления |

Для категорий «знать, уметь, владеть» планируется достижение следующих результатов обучения (РО), вносящих на соответствующих уровнях вклад в формирование компетенций, предусмотренных основной профессиональной образовательной программой (табл. 1).

**Таблица 1**. Результаты обучения

| **Компетенция:**  **код по СУОС 3++, формулировка** | **Результаты обучения.**  **Дескрипторы – основные признаки освоения компетенций (показатели достижения результата обучения, которые студент может**  **продемонстрировать)** | **Формы и методы обучения, способствующие формированию и развитию компетенции** |
| --- | --- | --- |
| **1** | **2** | **3** |
| ОПКС-1 Способен применять естественнонаучные и общеинженерные знания, методы математического моделирования, анализа, и синтеза, теоретического и экспериментального исследования в профессиональной деятельности | ЗНАТЬ - методы математических, естественнонаучных и общеинженерных дисциплин, используемые для решения задач анализа и проектирования программных или программно-аппаратных систем различного назначения или их компонентов УМЕТЬ - применять естественнонаучные и общеинженерные знания, методы математического моделирования, анализа, и синтеза, теоретического и экспериментального исследования в профессиональной деятельности ВЛАДЕТЬ - навыками применения естественнонаучных и общеинженерных знаний, методов математического моделирования, анализа, и синтеза, теоретического и экспериментального исследования в профессиональной деятельности | * **Лекции** * **Семинары** * **Самостоятельная работа**   **Активные и интерактивные**  **формы (методы) обучения:**  - обсуждение практических примеров на лекциях и семинарах;  - совместный анализ результатов рубежных контролей в форме дискуссии. |
| УКС-1 Способен осуществлять поиск, критический анализ и синтез информации, ее смысловую оптимизацию и наглядное представление, применять системный подход для решения поставленных задач; использовать основы философских знаний и анализировать закономерности исторического развития общества для формирования мировоззрения и гражданской позиции. | ЗНАТЬ - методики поиска, сбора, обработки информации, ее смысловой оптимизации и наглядного представления в сфере профессиональной деятельности, включая сайты Интернет УМЕТЬ - применять методики поиска, сбора, обработки информации, ее смысловой оптимизации и наглядного представления - проводить систематизацию, классификацию, интерпретацию соответствующей информации - выстраивать логику рассуждений и высказываний ВЛАДЕТЬ - методами поиска, сбора и обработки, критического анализа и синтеза информации, ее смысловой оптимизации и наглядного представления - навыками самостоятельного критического мышления | * **Лекции** * **Семинары** * **Самостоятельная работа**   **Активные и интерактивные**  **формы (методы) обучения:**  - обсуждение практических примеров на лекциях и семинарах;  - совместный анализ результатов рубежных контролей в форме дискуссии. |
| ПКСо-1 Способен участвовать в исследовательских и опытно-конструкторских разработках в области создания и совершенствования ИТ-систем | ЗНАТЬ - методы поиска научно-технической информации по теме исследования; методы проведения экспериментов и наблюдений, обобщения и обработки их результатов. УМЕТЬ - выполнять поиск и анализ научно-технической информации по теме исследования, проводить эксперименты, обобщать и обрабатывать полученные результаты ВЛАДЕТЬ - практическими навыками поиска научно-технической информации по теме исследования | * **Лекции** * **Семинары** * **Самостоятельная работа**   **Активные и интерактивные**  **формы (методы) обучения:**  - обсуждение практических примеров на лекциях и семинарах;  - совместный анализ результатов рубежных контролей в форме дискуссии. |
| ОПКС-2 Способен использовать современные информационные технологии и программные средства отечественного и иностранного производства при решении задач профессиональной деятельности | ЗНАТЬ - современные информационные технологии и программные средства отечественного и иностранного производства, используемые при проектировании и реализации программных или программно-аппаратных систем различного назначения или их компонентов УМЕТЬ - использовать современные информационные технологии и программные средства отечественного и иностранного производства при решении задач профессиональной деятельности ВЛАДЕТЬ - методиками применения современных информационных технологий и программных средств отечественного и иностранного производства при решении задач профессиональной деятельности | * **Лекции** * **Семинары** * **Самостоятельная работа**   **Активные и интерактивные**  **формы (методы) обучения:**  - обсуждение практических примеров на лекциях и семинарах;  - совместный анализ результатов рубежных контролей в форме дискуссии. |
| УКС-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, опираясь на экономические знания и исходя из действующих правовых норм, имеющихся ресурсов и технологий | ЗНАТЬ - виды ресурсов и технологий для решения профессиональных задач - основные методы, технической, технико-экономической и правовой оценки разных способов решения задач - действующее законодательство и правовые нормы, регулирующие профессиональную деятельность УМЕТЬ - проводить анализ поставленной цели как модели планируемого результата и формулировать задачи, которые необходимо решить для ее достижения - анализировать альтернативные варианты для достижения намеченных результатов - использовать нормативно-правовую документацию в сфере профессиональной деятельности - использовать экономические знания для решения профессиональных задач ВЛАДЕТЬ - методиками разработки цели (целеполагания) и задач проекта - методами оценки потребности в ресурсах, продолжительности и стоимости проекта - навыками работы с нормативно-правовой документацией | * **Лекции** * **Семинары** * **Самостоятельная работа**   **Активные и интерактивные**  **формы (методы) обучения:**  - обсуждение практических примеров на лекциях и семинарах;  - совместный анализ результатов рубежных контролей в форме дискуссии. |
| ОПКС-3 Способен решать стандартные задачи профессиональной деятельности на основе математической, информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | ЗНАТЬ - приемы и методы решения стандартных задач профессиональной деятельности - основные правила обеспечения информационной безопасности УМЕТЬ - решать стандартные задачи профессиональной деятельности на основе математической, информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ВЛАДЕТЬ - методиками решения стандартных задач профессиональной деятельности на основе математической, информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | * **Лекции** * **Семинары** * **Самостоятельная работа**   **Активные и интерактивные**  **формы (методы) обучения:**  - обсуждение практических примеров на лекциях и семинарах;  - совместный анализ результатов рубежных контролей в форме дискуссии. |
| УКС-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде, толерантно воспринимая социальные и культурные и иные различия | ЗНАТЬ - основные понятия, технологии межличностной и групповой коммуникации УМЕТЬ - устанавливать и поддерживать социальные контакты, обеспечивающие успешную работу в коллективе - применять основные методы и нормы социального взаимодействия для реализации своей роли и взаимодействия внутри команды ВЛАДЕТЬ - методами и приемами социального взаимодействия и работы в команде | * **Лекции** * **Семинары** * **Самостоятельная работа**   **Активные и интерактивные**  **формы (методы) обучения:**  - обсуждение практических примеров на лекциях и семинарах;  - совместный анализ результатов рубежных контролей в форме дискуссии. |
| УКС-4 Способен осуществлять деловую коммуникацию и межличностное взаимодействие в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах) | ЗНАТЬ - правила и закономерности деловой устной и письменной коммуникации УМЕТЬ - применять на практике деловую коммуникацию в устной и письменной формах, методы и навыки делового общения на русском и иностранном языках ВЛАДЕТЬ - навыками деловых коммуникаций в устной и письменной форме на русском и иностранном языках | * **Лекции** * **Семинары** * **Самостоятельная работа**   **Активные и интерактивные**  **формы (методы) обучения:**  - обсуждение практических примеров на лекциях и семинарах;  - совместный анализ результатов рубежных контролей в форме дискуссии. |
| ОПКС-5 Способен собирать аппаратуру, и инсталлировать отечественное и иностранное программное обеспечение для информационных и автоматизированных систем | ЗНАТЬ - порядок и правила инсталляции отечественного и иностранного программного обеспечения для информационных и автоматизированных систем УМЕТЬ - собирать аппаратуру, и инсталлировать отечественное и иностранное программное обеспечение для информационных и автоматизированных систем | * **Лекции** * **Семинары** * **Самостоятельная работа**   **Активные и интерактивные**  **формы (методы) обучения:**  - обсуждение практических примеров на лекциях и семинарах;  - совместный анализ результатов рубежных контролей в форме дискуссии. |
| УКС-6 Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов самоорганизации и образования в течение всей жизни, а также самостоятельно приобретать знания. | ЗНАТЬ - основные методики самоконтроля, саморазвития и самообразования на протяжении всей жизни УМЕТЬ - эффективно планировать и контролировать собственное время ВЛАДЕТЬ - методами управления собственным временем - технологиями приобретения, использования и обновления социокультурных и профессиональных знаний, умений и навыков | * **Лекции** * **Семинары** * **Самостоятельная работа**   **Активные и интерактивные**  **формы (методы) обучения:**  - обсуждение практических примеров на лекциях и семинарах;  - совместный анализ результатов рубежных контролей в форме дискуссии. |
| ПКС-6 Способен выполнять и управлять работами по созданию (модификации) и сопровождению информационных систем, автоматизирующих задачи организационного управления | ЗНАТЬ - этапы и принципы создания программных средств и автоматизированных информационных систем - методы поддержки принятия решений в автоматизированных системах УМЕТЬ - применять методы принятия решений в автоматизированных системах организационного управления ВЛАДЕТЬ - навыками моделирования процессов жизненного цикла информационных систем | * **Лекции** * **Семинары** * **Самостоятельная работа**   **Активные и интерактивные**  **формы (методы) обучения:**  - обсуждение практических примеров на лекциях и семинарах;  - совместный анализ результатов рубежных контролей в форме дискуссии. |
| ОПКС-1 Способен применять естественнонаучные и общеинженерные знания, методы математического моделирования, анализа, и синтеза, теоретического и экспериментального исследования в профессиональной деятельности | ЗНАТЬ - методы математических, естественнонаучных и общеинженерных дисциплин, используемые для решения задач анализа и проектирования программных или программно-аппаратных систем различного назначения или их компонентов УМЕТЬ - применять естественнонаучные и общеинженерные знания, методы математического моделирования, анализа, и синтеза, теоретического и экспериментального исследования в профессиональной деятельности ВЛАДЕТЬ - навыками применения естественнонаучных и общеинженерных знаний, методов математического моделирования, анализа, и синтеза, теоретического и экспериментального исследования в профессиональной деятельности | * **Лекции** * **Семинары** * **Самостоятельная работа**   **Активные и интерактивные**  **формы (методы) обучения:**  - обсуждение практических примеров на лекциях и семинарах;  - совместный анализ результатов рубежных контролей в форме дискуссии. |

1. **МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

Дисциплина входит в базовую часть блока Б1 «Дисциплины (модули)» образовательной программы бакалавриата по направлению подготовки 09.03.01 «Информатика и вычислительная техника».

Изучение дисциплины предполагает предварительное освоение следующих дисциплин учебного плана:

1. Основы программирования.
2. Информатика.
3. Электротехника.
4. Электроника.
5. Базы данных.
6. Операционные системы.
7. Сети и телекоммуникации.
8. Философия.
9. Безопасность жизнедеятельности.
10. Экономика.

Освоение данной дисциплины необходимо как предшествующее для следующих дисциплин образовательной программы:

1. Преддипломная практика.
2. Подготовка и защита ВКР.

Освоение учебной дисциплины связано с формированием компетенций с учетом матрицы компетенций ОПОП по направлению подготовки 09.03.01 «Информатика и вычислительная техника».

1. **ОБЪЕМ ДИСЦИПЛИНЫ**

Общий объем дисциплины составляет 2 зачётные единицы (з.е.), 72 ч. В том числе: 1 семестр - 2 з.е. (72 ч.).

Таблица 2. Объём дисциплины по видам учебных занятий (в часах)

|  |  |  |
| --- | --- | --- |
| **Виды учебной работы** | **Объем по семестрам, ч** | |
| **Всего** | **1 семестр** |
| **Объем дисциплины** | **72** | **72** |
| **Аудиторная работа** | **48** | **48** |
| Лекции (Л) | 24 | 24 |
| Семинары (С) | 24 | 24 |
| **Самостоятельная работа (СР)** | **24** | **24** |
| Проработка материала лекций | 4 | 4 |
| Подготовка к семинарам | 2 | 2 |
| Подготовка к рубежным контролям | 6 | 6 |
| Выполнение домашнего задания | 12 | 12 |
| **Вид промежуточной аттестации** |  | **зачёт** |

# **СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО МОДУЛЯМ С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ИЛИ АСТРОНОМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ**

**Таблица 3.** Содержание дисциплины

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Тема (название) модуля** | **Виды занятий, часы** | | | **Активные и интерактивные формы проведения занятий** | | **Компетенции, закрепленные за темой (код по СУОС 3++)** | **Текущий контроль результатов обучения** | | |
| **Л** | **С** | **СР** | **Форма проведения занятий** | **Ча-сы** | **Срок**  **(неделя)** | **Формы** | **Баллы**  **(мин/**  **макс)** |
| **1 семестр** | | | | | | | | | | |
| 1 | Система технической защиты информации | 14 | 14 | 6 | - обсуждение практических примеров на лекциях и семинарах;  - совместный анализ результатов рубежных контролей в форме дискуссии. | 5 | ОПКС-1,  УКС-1,  ПКСо-1,  ОПКС-2,  УКС-2,  ОПКС-3,  УКС-3,  УКС-4,  ОПКС-5,  УКС-6,  ПКС-6 | 7 | Рубежный контроль №1 | 12 / 20 |
| Работа на семинарах | 6 / 10 |
| Посещение лекций | 6 / 10 |
| **ИТОГО** | **24 / 40** |
| 2 | Методы и средства технической защиты информации | 10 | 10 | 18 | 4 | 12 | Рубежный контроль №2 | 12 / 20 |
| Работа на семинарах | 6 / 10 |
| Домашнее задание | 12 / 20 |
| Посещение лекций | 6 / 10 |
| **ИТОГО** | **36 / 60** |
|  | **ИТОГО за семестр** | **24** | **24** | **24** | **-** | **9** | **-** | **-** | **-** | **60 / 100** |

**Содержание дисциплины, структурированное по модулям.**

**Модуль 1. Система технической защиты информации. Объем: 34 часа**

**Лекции по модулю 1……………………………………………………………….…. *14 часов***

***1. Основы технической защиты конфиденциальной информации …………….…. 2 часа***

Актуальность ТЗИ. Роль защиты информации в области информатики и вычислительной техники. Предмет, система и методология курса обучения. Особенности создания защищенных автоматизированных систем обработки информации и управления.

***2. Государственная система защиты информации ………………………………… 2 часа***

Структура, задачи и основные функции государственной системы защиты информации. Цели, задачи, структура, функции и роль информационной безопасности в системе национальной безопасности Российской Федерации. Основные термины и определения в области технической защиты информации.

***3. Правовое регулирование ТЗИ ………………………………………………………... 2 часа***

Законодательная и нормативная база правового регулирования вопросов защиты информации. Федеральные законы Российской Федерации, Указы Президента Российской Федерации и постановления Правительства Российской Федерации, а также нормативно-методические документы ФСТЭК России, регулирующие вопросы технической защиты конфиденциальной информации. Лицензирование деятельности в области защиты информации, сертификация средств защиты информации и аттестация объектов информатизации. Порядок лицензирования деятельности в области технической защиты конфиденциальной информации. Порядок сертификации технических средств защиты информации по требованиям безопасности информации. Аттестация объектов информатизации.

***4. Специальные требования и рекомендации по технической защите конфиденциальной информации ………………………………………………………. 2 часа***

Основные требования и рекомендации по защите речевой информации, циркулирующей в защищаемых помещениях. Основные требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники. Основные требования и рекомендации по защите служебной тайны и персональных данных. Основные рекомендации по защите информации, составляющей коммерческую тайну. Порядок обеспечения защиты информации при эксплуатации автоматизированных систем. Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ. Защита информации в локальных вычислительных сетях. Защита информации при межсетевом взаимодействии. Защита информации при работе с системами управления базами данных. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.

***5. Технические каналы утечки информации и их характеристики ……………… 2 часа***

Общая характеристика технических каналов утечки информации и их классификация. Механизмы возникновения технических каналов утечки информации. Технические каналы утечки речевой информации. Характеристика акустического, виброакустического, электроакустического, электромагнитного каналов утечки информации. Механизмы их возникновения. Технические средства и методы получения информации по этим каналам. Утечка информации за счет побочных электромагнитных излучений и наводок (далее - ПЭМИН). Механизмы возникновения утечки информации по каналам ПЭМИН. Технические средства и методы получения информации с использованием этих каналов.

***6. Компьютерная разведка ……………………………………………………………... 2 часа***

Общая характеристика компьютерной разведки. Виды компьютерной разведки и их характеристика. Взаимодействие компьютерной разведки с другими видами технической разведки и способы комплексной технической разведки. Угрозы технической разведки.

***7. Оценка защищенности конфиденциальной информации от ее утечки по техническим каналам ……………………………………………………………….….. 2 часа***

Оценка защищенности помещений от утечки речевой информации по акустическим и виброакустическим каналам. Оценка защищенности основных технических средств и систем от утечки информации по электромагнитным каналам. Оценка защищенности помещений от утечки речевой информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах. Оценка защищенности информации, обрабатываемой в основных технических средствах и системах от утечки за счет наводок.

**Семинары по модулю 1…………………………………………………………….… *14 часов***

***1. Основы технической защиты конфиденциальной информации ……………….. 2 часа***

Актуальность ТЗИ. Роль защиты информации в области информатики и вычислительной техники. Предмет, система и методология курса обучения. Особенности создания защищенных автоматизированных систем обработки информации и управления.

***2. Государственная система защиты информации ………………………………… 2 часа***

Структура, задачи и основные функции государственной системы защиты информации. Цели, задачи, структура, функции и роль информационной безопасности в системе национальной безопасности Российской Федерации. Основные термины и определения в области технической защиты информации.

***3. Правовое регулирование ТЗИ ………………………………………………..……… 2 часа***

Законодательная и нормативная база правового регулирования вопросов защиты информации. Федеральные законы Российской Федерации, Указы Президента Российской Федерации и постановления Правительства Российской Федерации, а также нормативно-методические документы ФСТЭК России, регулирующие вопросы технической защиты конфиденциальной информации. Лицензирование деятельности в области защиты информации, сертификация средств защиты информации и аттестация объектов информатизации. Порядок лицензирования деятельности в области технической защиты конфиденциальной информации. Порядок сертификации технических средств защиты информации. Аттестация объектов информатизации.

***4. Специальные требования и рекомендации по технической защите конфиденциальной информации ………………………………………………………. 2 часа***

Основные требования и рекомендации по защите речевой информации, циркулирующей в защищаемых помещениях. Основные требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники. Основные требования и рекомендации по защите служебной тайны и персональных данных. Основные рекомендации по защите информации, составляющей коммерческую тайну. Порядок обеспечения защиты информации при эксплуатации автоматизированных систем. Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ. Защита информации в локальных вычислительных сетях. Защита информации при межсетевом взаимодействии. Защита информации при работе с системами управления базами данных. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования (интернет).

***5. Технические каналы утечки информации и их характеристики ……………… 2 часа***

Общая характеристика технических каналов утечки информации и их классификация. Механизмы возникновения технических каналов утечки информации. Технические каналы утечки речевой информации. Характеристика акустического, виброакустического, электроакустического, электромагнитного каналов утечки информации. Механизмы их возникновения. Технические средства и методы получения информации по этим каналам. Утечка информации за счет побочных электромагнитных излучений и наводок (далее - ПЭМИН). Механизмы возникновения утечки информации по каналам ПЭМИН. Технические средства и методы получения информации с использованием этих каналов.

***6. Компьютерная разведка …………………………………………………………….. 2 часа***

Общая характеристика компьютерной разведки. Виды компьютерной разведки и их характеристика. Взаимодействие компьютерной разведки с другими видами технической разведки и способы комплексной технической разведки. Угрозы технической разведки.

***7. Оценка защищенности конфиденциальной информации от ее утечки по техническим каналам …………………………………………………………...……… 2 часа***

Оценка защищенности помещений от утечки речевой информации по акустическим и виброакустическим каналам. Оценка защищенности основных технических средств и систем от утечки информации по электромагнитным каналам. Оценка защищенности помещений от утечки речевой информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах. Оценка защищенности информации, обрабатываемой в основных технических средствах и системах от утечки за счет наводок.

**Самостоятельная работа по модулю 1……………………………………..…….….. *6 часов***

Проработка разделов лекционного курса……………………………………………...... *2 часа*

Подготовка к семинарам …………………………………………………………….…... *1 час*

Подготовка к рубежному контролю №1…………………………………………….…... *3 часа*

***Модуль 2. Методы и средства технической защиты информации. Объем: 38 часов***

**Лекции по модулю 2……………………………………………………………….…. *10 часов***

***8. Проведение аттестационных испытаний на объектах информатизации ….. 2 часа***

Необходимость проведения аттестационных испытаний. Документация, необходимая для проведения аттестационных испытаний. Аппаратура для проведения аттестационных испытаний. Взаимодействие со специалистами по защите информации. Возможность развития объектов информатизации и внесения изменений в документацию аттестационных испытаний на объектах информатизации.

***9. Методы защиты информации ……………………………………………………… 2 часа***

Организация работ по обеспечению комплексной защиты сведений, составляющих конфиденциальную информацию. Организация охраны, пропускного режима и объектового режима. Организация работ по комплексной защите информации от утечки по техническим каналам. Защита территории, здания, помещений от несанкционированного проникновения (охранная сигнализация, системы обзорного телевидения, металлодетекторы, дозиметры, досмотровые зеркала). Модели, технические характеристики используемых устройств. Защита кабинетов руководителей и помещений, предназначенных для проведения переговоров, от съема информации. Организация и проведение работ по защите информации от ее утечки по техническим каналам на объектах информатизации. Пассивные и активные методы, используемые при создании систем защиты информации. Экранирование как метод предотвращения утечки информации за счет ПЭМИН. Фильтрация как метод предотвращения утечки информации по проводным коммуникациям. Маскирование шумоподобными сигналами. Маскирование методом преобразования речевой информации.

***10. Технические средства защиты информации ……………………………………. 2 часа***

Генераторы шума для защиты основных технических средств и систем (ОТСС) и подавления радиомикрофонов и диктофонов. Основные принципы построения генераторов шума. Модели генераторов шума, их технические характеристики и особенности применения. Защита сети электропитания и заземления. Основные принципы защиты информации от утечки по сети электропитания и заземления. Технические средства, используемые для защиты, их технические характеристики. Системы виброакустического зашумления. Основные принципы построения и действия генераторов и датчиков. Модели и их технические характеристики. Особенности практического применения. Способы защиты информации в телефонных линиях связи. Пассивные и активные средства защиты телефонных линий связи от перехвата информации и их технические характеристики.

***11. Криптографические средства защиты информации …………………………... 2 часа***

Принципы криптографической защиты информации. Аппаратно-программные средства защиты компьютерной информации. Классические симметричные криптосистемы. Основные понятия и определения. Шифры перестановки. Шифрующие таблицы. Методы генерации псевдослучайных последовательностей чисел. Современные симметричные криптосистемы. Американский стандарт шифрования данных DES. Отечественный стандарт шифрования данных. Блочные и поточные шифры. Асимметричные криптосистемы. Концепция криптосистемы с открытым ключом. Криптосистема шифрования данных RSA. Идентификация и проверка подлинности. Идентификация и аутентификация пользователя. Типовые схемы идентификации и аутентификации пользователя. Особенности применения пароля для аутентификации пользователя. Биометрическая идентификация и аутентификация. Взаимная проверка подлинности пользователей

***12. Программно-аппаратные средства защиты информации ……………………. 2 часа***

Сертифицированные программно-аппаратные средства. Способы освоения систем защиты информации с применением программно-аппаратных средств защиты информации от несанкционированного доступа. Обеспечение безопасности информации при подключении вычислительных средств к международным информационным системам. Требования руководящих документов по обеспечению информационной безопасности при использовании информационно-телекоммуникационных сетей международного информационного обмена. Особенности обеспечения безопасности информации при подключении автоматизированных систем к международным информационным системам, в том числе Интернет.

**Семинары по модулю 2……………………………………………………….……… *10 часов***

***8. Проведение аттестационных испытаний на объектах информатизации …... 2 часа***

Необходимость проведения аттестационных испытаний. Документация, необходимая для проведения аттестационных испытаний. Аппаратура для проведения аттестационных испытаний. Взаимодействие со специалистами по защите информации. Возможность развития объектов информатизации и внесения изменений в документацию аттестационных испытаний на объектах информатизации.

***9. Методы защиты информации ……………………………………………………… 2 часа***

Организация работ по обеспечению комплексной защиты сведений, составляющих конфиденциальную информацию. Организация охраны, пропускного режима и объектового режима. Организация работ по комплексной защите информации от утечки по техническим каналам. Защита территории, здания, помещений от несанкционированного проникновения (охранная сигнализация, системы обзорного телевидения, металлодетекторы, дозиметры, досмотровые зеркала). Модели, технические характеристики используемых устройств. Защита кабинетов руководителей и помещений, предназначенных для проведения переговоров, от съема информации. Организация и проведение работ по защите информации от ее утечки по техническим каналам на объектах информатизации. Пассивные и активные методы, используемые при создании систем защиты информации. Экранирование как метод предотвращения утечки информации за счет ПЭМИН. Фильтрация как метод предотвращения утечки информации по проводным коммуникациям. Маскирование шумоподобными сигналами. Маскирование методом преобразования речевой информации.

***10. Технические средства защиты информации ……………………………………. 2 часа***

Генераторы шума для защиты основных технических средств и систем (ОТСС) и подавления радиомикрофонов и диктофонов. Основные принципы построения генераторов шума. Модели генераторов шума, их технические характеристики и особенности применения. Защита сети электропитания и заземления. Основные принципы защиты информации от утечки по сети электропитания и заземления. Технические средства, используемые для защиты, их технические характеристики. Системы виброакустического зашумления. Основные принципы построения и действия генераторов и датчиков. Модели и их технические характеристики. Особенности практического применения. Способы защиты информации в телефонных линиях связи. Пассивные и активные средства защиты телефонных линий связи от перехвата информации и их технические характеристики.

***11. Криптографические средства защиты информации ………………………….. 2 часа***

Принципы криптографической защиты информации. Аппаратно-программные средства защиты компьютерной информации. Классические симметричные криптосистемы. Основные понятия и определения. Шифры перестановки. Шифрующие таблицы. Методы генерации псевдослучайных последовательностей чисел. Современные симметричные криптосистемы. Американский стандарт шифрования данных DES. Отечественный стандарт шифрования данных. Блочные и поточные шифры. Асимметричные криптосистемы. Концепция криптосистемы с открытым ключом. Криптосистема шифрования данных RSA. Идентификация и проверка подлинности. Идентификация и аутентификация пользователя. Типовые схемы идентификации и аутентификации пользователя. Особенности применения пароля для аутентификации пользователя. Биометрическая идентификация и аутентификация. Взаимная проверка подлинности пользователей

***12. Программно-аппаратные средства защиты информации ……………………. 2 часа***

Сертифицированные программно-аппаратные средства. Способы освоения систем защиты информации с применением программно-аппаратных средств защиты информации от несанкционированного доступа. Обеспечение безопасности информации при подключении вычислительных средств к международным информационным системам. Требования руководящих документов по обеспечению информационной безопасности при использовании информационно-телекоммуникационных сетей международного информационного обмена. Особенности обеспечения безопасности информации при подключении автоматизированных систем к международным информационным системам, в том числе Интернет.

**Самостоятельная работа по модулю 1……………………………………..…...….. *18 часов***

Проработка разделов лекционного курса……………………………………………….. *2 часа*

Подготовка к семинарам …………………………………………………………….…... *1 час*

Подготовка к рубежному контролю №2…………………………………………….…... *3 часа*

Выполнение домашнего задания…………………………………………………....… *12 часов*

# **ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ**

Для обеспечения самостоятельной работы студентов по дисциплине сформирован методический комплекс, включающий следующие учебно-методических материалы.

1. Программа курса.
2. Учебники и учебные пособия [1].
3. Конспект лекций в электронном виде.
4. Указания кафедральной разработки по выполнению домашнего задания в электронном виде.
5. Набор презентаций для использования в аудиторных занятиях в электронном виде.
6. Список адресов сайтов сети Интернет, содержащих актуальную информацию по теме дисциплины.

Материалы учебно-методического комплекса рассылаются студентам по электронной почте. Библиографические ссылки на учебные издания, входящие в методический комплекс, приведены в перечне основной и дополнительной учебной литературы, необходимой для освоения дисциплины (раздел 7).

К дополнительным материалам также относится перечень ресурсов сети интернет, рекомендуемых для самостоятельной работы при освоении дисциплины (раздел 8).

Студенты получают доступ к указанным материалам на первом занятии по дисциплине.

6.  **ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ**

Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине базируется на перечне компетенций с указанием этапов их формирования в процессе освоения образовательной программы (раздел 1). ФОС должен обеспечивать объективный контроль достижения всех результатов обучения, запланированных для дисциплины.

ФОС включает в себя:

* описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
* методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.
* типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и уровня овладения формирующимися компетенциями в процессе освоения дисциплины (примеры типовых вопросов по темам для оценки работы на семинарах; примеры вариантов рубежных контролей; список типовых тем для докладов, презентаций (домашнее задание); перечень вопросов к зачету (для ликвидации академической задолженности, или перезачета дисциплины для студентов, переводящихся из других вузов, или для повышения балльной оценки за отдельные модули дисциплины)).

Контроль освоения дисциплины производится в соответствии с Положением о текущем контроле успеваемости и промежуточной аттестации студентов МГТУ им. Н.Э. Баумана.

ФОС является приложением к данной программе дисциплины.

# **ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ**

**Основная литература**

1. Меньшаков Ю.К. Основы защиты от технических разведок / Учебное пособие. Электронные издательства МГТУ им. Н.Э. Баумана. 2010. ISBN: 978-5-7038-3382-7. Режим доступа: <http://ebooks.bmstu.ru/catalog/117/book1207.html>
2. Меньшаков Ю.К. Виды и средства иностранных технических разведок / Учебное пособие. Электронные издательства МГТУ им. Н.Э. Баумана. 2009. ISBN: 978-5-7038-3244-8. Режим доступа: http://ebooks.bmstu.ru/catalog/117/book1206.html
3. Меньшаков Ю.К. Теоретические основы технических разведок / Учебное пособие. Электронные издательства МГТУ им. Н.Э. Баумана. 2007. ISBN: 978-5-7038-3019-2. Режим доступа: <http://ebooks.bmstu.ru/catalog/117/book1176.html>.

**Дополнительная литература**

1. Варламов О.О. Эволюционные базы данных и знаний для адаптивного синтеза интеллектуальных систем. Миварное информационное пространство. - М.: Радио И Связь, 2002.
2. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: Изд-Во Мифи, 1997.
3. Грушо А. А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: издательство агентства «Яхтсмен», 1996.
4. Хорев А.А. Способы и средства защиты информации. Учебное пособие. - М: МО РФ, 2000.
5. Малюк А.А., Горбатов В.С., Королев В.И., Фомичев В.М., Дураковский A.П., Кондратьева Т.А. [Введение в информационную безопасность](https://elibrary.ru/item.asp?id=29176343). Москва, 2013.
6. Малюк А.А. [Теория защиты информации. Монография](https://elibrary.ru/item.asp?id=20245632). Москва, 2012.
7. Малюк А.А. [Защита информации в информационном обществе](https://elibrary.ru/item.asp?id=24422717). Москва, 2015.
8. Грушо А.А., Применко Э.А., Тимонина Е.Е. [Теоретические основы компьютерной безопасности](https://elibrary.ru/item.asp?id=19592918) // Учебное пособие. Москва, 2009.
9. Садовская Т.Г., Хорев А.А. [Средства и методы обеспечения безопасности бизнеса. Технические каналы утечки информации](https://elibrary.ru/item.asp?id=19593025) // учебное пособие для студентов высших учебных заведений. Московский гос. Технический ун-т им. Н. Э. Баумана. Москва, 2009.
10. Хорев А.А. [Техническая защита информации](https://elibrary.ru/item.asp?id=19592197) // учебное пособие для студентов высших учебных заведений, обучающихся по специальностям в области информационной безопасности : в 3 т. / Московский гос. Ин-т электронной техники (технический ун-т). Москва, 2008.
11. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. [Семь безопасных информационных технологий](https://elibrary.ru/item.asp?id=27731662) / под ред. А. С. Маркова. Москва, 2017.
12. Зима В.М., Котухов М.М., Ломако А.Г., Марков А.С., Молдовян А.А. [Разработка систем информационно-компьютерной безопасности](https://elibrary.ru/item.asp?id=22996929). Санкт-петербург, 2003.
13. Федеральный закон: об информации, информационных технологиях и о защите информации // электронный документ. Режим доступа: <http://fstec.ru/litsenzionnaya-deyatelnost/tekhnicheskaya-zashchita-informatsii/74-zakony/221-federalnyj-zakon-rossijskoj-federatsii-ot-27-iyulya-2006-g-n-149-fz>. 2017.
14. Закон о государственной тайне // электронный документ. Режим доступа: http://fstec.ru/litsenzionnaya-deyatelnost/tekhnicheskaya-zashchita-informatsii/74-zakony/220-zakon-rossijskoj-federatsii-ot-21-iyulya-1993-g-n-5485-1. 2017.
15. Федеральный закон: о банках и банковской деятельности // электронный документ. Режим доступа: http://fstec.ru/protivodejstvie-korruptsii/normativnye-pravovye-i-inye-akty/49-zakony/634-federalnyj-zakon-ot-2-dekabrya-1990-g-n-395-1. 2017.
16. Административный регламент федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации // электронный документ. Режим доступа: http://fstec.ru/normotvorcheskaya/administrativnye-reglamenty/1359-prikaz-fstek-rossii-ot-17-iyulya-2017-g-n-133. 2017.
17. Административный регламент федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации // электронный документ. Режим доступа: http://fstec.ru/litsenzionnaya-deyatelnost/tekhnicheskaya-zashchita-informatsii/249-administrativnye-reglamenty/1361-prikaz-fstek-rossii-ot-17-iyulya-2017-g-n-134-1. 2017.
18. Административный регламент федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации // электронный документ. Режим доступа: <http://fstec.ru/normotvorcheskaya/administrativnye-reglamenty/476-prikaz-fstek-rossii-ot-12-iyulya-2012-g-n-83>. 2017.
19. Сайт федеральной службы по техническому и экспортному контролю: <http://fstec.ru/>. 2017.
20. Варламов О.О., Чибирова М.О., Хадиев А.М., Антонов П.Д., Сергушин Г.С., Шошев И.А., Назаров К.В. Практикум по созданию миварных экспертных систем. Учебное пособие / под ред. О.О. Варламова. М.: «Белый ветер», 2016. — 184 с. ISBN 978-5-905714-97-9
21. Варламов О.О. Эволюционные базы данных и знаний для адаптивного синтеза интеллектуальных систем. Миварное информационное пространство. Изд. 2-е, стереотип. — М.: НИИ МИВАР, 2016. — 288 с. (Электронная версия).
22. Варламов О.О., Чибирова М.О., Хадиев А.М., Антонов П.Д., Сергушин Г.С., Протопопова Д.А., Жданович Е.А., Збавитель П.Ю., Сараев Д.В., Шошев И.А., Петерсон А.О. Практикум по миварному моделированию и созданию экспертных систем (на  примере программного комплекса "Конструктор экспертных систем МИВАР 1.1" (КЭСМИ 1.1). Учебное пособие / Под ред. Варламова О.О. - М.: Издательство НИИ МИВАР, 2015. - 246 с. ISBN 978-5-905714-51-1.
23. Барабанов А.В., Марков А.С., Цирлов В.Л. [Испытания межсетевых экранов по требованиям безопасности информации](https://elibrary.ru/item.asp?id=28793564) // Учебное издание / Москва, 2017.
24. Гладков Л.А., Курейчик В.В., Курейчик В.М. Дискретная математика. — М.: ФИЗМАТЛИТ, 2014. — 496 с.
25. Люгер Дж.Ф. Искусственный интеллект: стратегии и методы решения сложных проблем. 4-е изд. — М.: Вильямс, 2005. — 864 с.
26. Варламов О.О. Прикладная математика: гносеологические основы миварных технологий создания систем искусственного интеллекта. Учебное пособие. — М.: МАДИ, 2013. 84 с.
27. Варламов О.О. Основы миварного подхода к созданию логического искусственного интеллекта. Учебное пособие. — М.: МАДИ, 2013. 80 с.

# **ПЕРЕЧЕНЬ РЕСУРСОВ СЕТИ ИНТЕРНЕТ, РЕКОМЕНДУЕМЫХ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПРИ ОСВОЕНИИ ДИСЦИПЛИНЫ**

1. Сайт библиотеки МГТУ им. Н.Э. Баумана: <http://library.bmstu.ru>.
2. Сайты кафедры ИУ5 «Системы обработки информации и управления»:
   1. <http://e-learning.bmstu.ru/portal_iu5/>
   2. <http://iu5.bmstu.ru>
3. Сайт веб-консорциума: <https://www.w3.org/>
4. <http://elibrary.ru/defaultx.asp>
5. Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России): <http://fstec.ru/>
6. http://elibrary.ru/author\_items.asp?authorid=143177
7. <http://www.aiportal.ru>
8. <http://www.mivar.ru>
9. <http://mivar.ru/vse-o-mivarakh/biblioteka>
10. <http://science.mivar.ru>
11. <http://cyberleninka.ru>
12. <http://www.aiportal.ru/downloads/books/system-analysis-and-synthesis-models-by-varlamov.html>
13. <http://sk.ru/news/>
14. <http://ai-center.botik.ru/Airec/>
15. **МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ СТУДЕНТОВ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ**

Приступая к работе, каждый студент должен принимать во внимание следующие положения.

Дисциплина построена по модульному принципу, каждый модуль представляет собой логически завершенный раздел курса. Дисциплина делится на два модуля.

На первом занятии каждый студент получает в электронном виде полный комплекс учебно-методических материалов по дисциплине.

**Лекционные занятия** посвящены рассмотрению ключевых, базовых положений курса и разъяснению учебных заданий, выносимых на самостоятельную проработку.

**Семинарские занятия** проводятся для закрепления усвоенной информации, приобретения навыков ее применения для решения практических задач в предметной области дисциплины.

**Самостоятельная работа** студентов включает проработку материала лекций, подготовку к семинарам, подготовку к рубежным контролям, выполнение домашнего задания.

**Текущий контроль** проводится в течение каждого модуля, его итоговые результаты складываются из оценок по следующими видам контрольных мероприятий:

* домашнее задание;
* посещение лекций;
* работа на семинарах;
* рубежные контроли.

Освоение дисциплины, ее успешное завершение на стадии промежуточной аттестации возможно только при регулярной работе во время семестра и планомерном прохождении текущего контроля.

Для завершения работы в семестре студент должен выполнить все контрольные мероприятия.

**Промежуточная аттестация** по результатам семестра по дисциплине проходит в форме зачета. Для ликвидации академической задолженности, или перезачета дисциплины для студентов, переводящихся из других вузов, или для повышения балльной оценки за отдельные модули дисциплины проводится зачет в форме собеседования для проверки ключевых результатов обучения по дисциплине, обеспечивающее возможность объективной независимой оценки приобретенных знаний, умений и навыков.

**Методика оценки по рейтингу**

Студент, выполнивший все предусмотренные учебным планом задания и сдавший все контрольные мероприятия, получает итоговую оценку по дисциплине за семестр в соответствии со шкалой:

|  |  |
| --- | --- |
| **Рейтинг** | **Оценка на зачете** |
| 60 – 100 | зачет |
| 0 – 59 | незачет |

Оценивание дисциплины ведется в соответствии с Положением о текущем контроле успеваемости и промежуточной аттестации студентов МГТУ им. Н.Э. Баумана.

1. **ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ**

В процессе преподавания дисциплины используются следующие методы и средства и ежегодно обновляемое программное обеспечение информационных технологий:

* e-mail преподавателей для оперативной связи: [varlamovoo@bmstu.ru](mailto:ovar@narod.ru);
* электронные учебно-методические материалы для обеспечения самостоятельной работы студентов, доступные в Интернет**;**
* презентации в среде PowerPoint и видео сюжеты по теме дисциплины;
* список сайтов в среде Интернет для поиска научно-технической информации по разделам дисциплины;
* программный комплекс «Конструктор экспертных систем миварный Wi!Mi РАЗУМАТОР» (КЭСМИ 2.1);
* офисный пакет приложений – Microsoft Office;
* правовая система КонсультантПлюс (<http://www.consultant.ru/>);
* информационно-правовой портал ГАРАНТ (<http://www.garant.ru/>);
* информационно-поисковые системы российских и американских патентов (<http://www1.fips.ru/wps/wcm/connect/content_ru/ru/inform_resources/inform_retrieval_system/>; United States Patent and Trademark Office [www.uspto.gov](http://www.uspto.gov)).

# **ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ**

Перечень материально-технического обеспечения дисциплины

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Вид занятий** | **Вид и наименование оборудования** |
| 1. | Лекционные и семинарские занятия | Аудитория с доской и проектором |
| 2. | Самостоятельная работа | Библиотека, имеющая рабочие места для студентов; Аудитории, оснащенные компьютерами с доступом к сети Интернет. Социокультурное пространство университета, позволяющее студенту качественно выполнять самостоятельную работу. |

ЛИСТ ВНЕСЕННЫХ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ

|  |  |
| --- | --- |
| Номер изменения, дата внесения изменения, номер страницы для внесения изменений | |
| БЫЛО: | СТАЛО: |
| Основание: | |
| Подпись лица, ответственного за внесение изменений | |