

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Забайкальский государственный университет»
(ФГБОУ ВО «ЗабГУ»)

Энергетический факультет
Кафедра Прикладной информатики и математики

УТВЕРЖДАЮ:

Декан факультета

Энергетический факультет

Батухтин Андрей
Геннадьевич

«___» _____ 20___
г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.О.24 Информационная безопасность
на 180 часа(ов), 5 зачетных(ые) единиц(ы)
для направления подготовки (специальности) 09.03.03 - Прикладная информатика

составлена в соответствии с ФГОС ВО, утвержденным приказом
Министерства образования и науки Российской Федерации от
«___» _____ 20___ г. №___

Профиль – Прикладная информатика в экономике (для набора 2021)
Форма обучения: Очная

1. Организационно-методический раздел

1.1 Цели и задачи дисциплины (модуля)

Цель изучения дисциплины:

Целью дисциплины является ознакомление учащихся с международными стандартами информационной безопасности, с нормативно-руководящими документами и основными понятиями, относящимися к информационной безопасности и способам защиты информации, а также обучение студентов основным принципам построения системы защиты и применения основных технологий построения защищенных ИС на практике. Сформировать у студентов теоретические знания и практические навыки выбора и использования технических и программных средств защиты информации от НСД при построении системы защиты в условиях автоматизированных систем обработки информации.

Задачи изучения дисциплины:

Освоение технологий диагностики опасностей и угроз для информационных систем и методов работы с моделями безопасности, каналов утечки информации, компьютерные вирусы, закладки, атаки на информационные системы, имеющие доступ к глобальным телекоммуникациям (несанкционированный доступ с применением сетевых технологий); -освоение технологий защиты, аутентификации, разграничения прав доступа к конфиденциальной информации.

1.2. Место дисциплины (модуля) в структуре ОП

Дисциплина «Информационная безопасность» является обязательной для студентов очной формы обучения и изучается ими на втором году обучения. Она базируется на знаниях, полученных при изучении предмета «Информатика и программирование», а также математических дисциплин изучаемых на первом и втором годах обучения. Теоретические знания и практические навыки, полученные студентами при ее изучении, должны быть использованы при подготовке курсовых работ и дипломной работы, выполнении научной студенческой работы, а также при подготовке к Государственному экзамену. Рассматриваемая дисциплина для бакалавров прикладной информатики является базовой для подготовки к решению профессиональных задач в соответствии с видами профессиональной деятельности (производственно – технологической и аналитической). Знания и умения полученные в результате изучения дисциплины, в дальнейшем потребуются для успешного освоения следующих дисциплин: «Базы данных»; «Проектирование информационных систем»; «Разработка программных приложений»; «Современные технологии программирования»

1.3. Объем дисциплины (модуля) с указанием трудоемкости всех видов учебной работы

Общая трудоемкость дисциплины (модуля) составляет 5 зачетных(ые) единиц(ы), 180 часов.

| Виды занятий | Семестр 4 | Семестр 5 | Всего часов |
|--------------|-----------|-----------|-------------|
|--------------|-----------|-----------|-------------|

| | | | |
|--|-------|--------------------------|-----|
| Общая трудоемкость | | | 180 |
| Аудиторные занятия, в т.ч. | 48 | 34 | 82 |
| Лекционные (ЛК) | 16 | 17 | 33 |
| Практические (семинарские) (ПЗ, СЗ) | 0 | 0 | 0 |
| Лабораторные (ЛР) | 32 | 17 | 49 |
| Самостоятельная работа студентов (СРС) | 60 | 38 | 98 |
| Форма промежуточной аттестации в семестре | Зачет | Дифференцированный зачет | 0 |
| Курсовая работа (курсовой проект) (КР, КП) | | | |

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

| Планируемые результаты освоения образовательной программы | | Планируемые результаты обучения по дисциплине |
|---|--|---|
| Код и наименование компетенции | Индикаторы достижения компетенции, формируемые в рамках дисциплины | Дескрипторы: знания, умения, навыки и (или) опыт деятельности |
| УК-2 | УК-2.1. Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения. | Знать: - нормативноправовые акты в сфере информационной безопасности и методологические основы принятия управленческого решения по вопросам информационной безопасности |
| УК-2 | УК-2.2. Умеет анализировать альтернативные варианты решений для достижения | Уметь: анализировать альтернативные варианты решений для решения |

| | | |
|-------|---|---|
| | <p>намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ</p> | <p>задач информационной безопасности; - разрабатывать план работ по информационной безопасности, - определять целевые этапы и основные направления работ по защите информации.</p> |
| УК-2 | <p>УК-2.3. Владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах</p> | <p>Владеть: - методиками разработки цели и задач политики информационной безопасности; -методами оценки продолжительности и стоимости проекта работ по реализации мер информационной безопасности на предприятии</p> |
| ОПК-3 | <p>ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационны х технологий и с учетом основных требований информационной безопасности.</p> | <p>Знать: принципы, методы и средства решения стандартных задач в сфере защиты информации с учетом информационной и библиографической культуры с применением информационнокоммуникационны х технологий в рамках требований информационной безопасности.</p> |
| ОПК-3 | <p>ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационны х технологий и с учетом основных требований информационной безопасности.</p> | <p>Уметь: - решать стандартные задачи информационной безопасности на основе информационной и библиографической культуры с применением информационнокоммуникационны х технологий в рамках правового поля информационной безопасности.</p> |

| | | |
|-------|---|--|
| ОПК-3 | ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности. | Владеть: Владеть: Навыками подготовки обзоров, составления рефератов и докладов по вопросам защиты информации с учетом требований информационной безопасности. |
| ПК-10 | ПК-10.1. Знает методы и модели организации ИТ инфраструктуры; виды угроз и меры по обеспечению информационной безопасности ИС; основы конфигурационного управления; основы управления изменениями. | Знать: - методы и модели организации ИТинфраструктуры; виды угроз и меры по обеспечению информационной безопасности ИС; -основы разработки политики информационной безопасности |
| ПК-10 | Умеет применять методы и модели организации ИТ- инфраструктуры; виды угроз и меры по обеспечению информационной безопасности ИС; работать с системой контроля версий; | Уметь: применять методы и модели организации ИТинфраструктуры с учетом требований информационной безопасности; -выявлять виды угроз и устанавливать меры по обеспечению информационной безопасности ИС |
| ПК-10 | ПК-10.3. Владеет навыками организации ИТ- инфраструктуры и управления информационной безопасностью, в т.ч., обеспечения и контроля соответствия технических, программных и коммуникационных средств для функционирования ИС, разграничение прав доступа к ИС; | Владеть: навыками создания ИТ- инфраструктуры и управления информационной безопасностью с применением технических, криптографических, программных и коммуникационных средств для функционирования ИС |

3. Содержание дисциплины

3.1. Разделы дисциплины и виды занятий

3.1 Структура дисциплины для очной формы обучения

| Модуль | Номер раздела | Наименование раздела | Темы раздела | Всего часов | Аудиторные занятия | | | С Р С |
|--------|---------------|--|---|-------------|--------------------|--------------------|--------|-------------|
| | | | | | Л К | П З (С З) | Л Р | |
| 1 | 1.1 | Основы обеспечения комплексной защиты конфиденциальной информации | Основы обеспечения комплексной защиты конфиденциальной информации | 11 | 2 | 0 | 4 | 5 |
| | 1.2 | Актуальность проблем информационной безопасности | Актуальность проблем информационной безопасности | 11 | 2 | 0 | 2 | 7 |
| | 1.3 | Ландшафт угроз и уязвимостей | Основные угрозы информационной безопасности. Атаки на информационную систему. | 18 | 3 | 0 | 5 | 10 |
| | 1.4 | Законодательный уровень обеспечения ИБ | Законодательный уровень обеспечения ИБ | 18 | 3 | 0 | 5 | 10 |
| 2 | 2.1 | Принципы обеспечения информационной безопасности | Принципы обеспечения информационной безопасности | 9 | 2 | 0 | 2 | 5 |
| | 2.2 | Классические симметричные методы, современные симметричные криптосистемы | Основные понятия и определения. Основные методы шифрования. Комбинирование блочных алгоритмов. Алгоритм шифрования данных IDEA. Отечественный стандарт шифрования данных. | 27 | 4 | 0 | 8 | 15 |
| | 2.3 | Асимметричные криптосистемы | Асимметричные криптосистемы | 19 | 4 | 0 | 5 | 10 |
| | | | | | | | | |

| | | | | | | | | |
|-------|-----|---|---|-----|----|---|----|----|
| | 2.4 | Управление криптографическими ключами. ЭЦП | Управление криптографическими ключами. ЭЦП | 20 | 4 | 0 | 5 | 11 |
| 3 | 3.1 | Стандарты в области ИБ | Стандарты в области ИБ | 9 | 2 | 0 | 2 | 5 |
| | 3.2 | Защита персональных данных | Защита персональных данных | 9 | 2 | 0 | 2 | 5 |
| | 3.3 | Методы и средства защиты от удаленных атак через сеть Internet. | Основные схемы сетевой защиты. Методы и средства защиты от удаленных атак через сеть Internet | 18 | 3 | 0 | 5 | 10 |
| | 3.4 | Приватность и безопасность операционных систем. | Приватность и безопасность операционных систем. | 11 | 2 | 0 | 4 | 5 |
| Итого | | | | 180 | 33 | 0 | 49 | 98 |

3.2. Содержание разделов дисциплины

3.2.1. Лекционные занятия, содержание и объем в часах

| Модуль | Номер раздела | Тема | Содержание | Трудоемкость (в часах) |
|--------|---------------|---|---|------------------------|
| 1 | 1.1 | Основы обеспечения комплексной защиты конфиденциальной информации | Предмет информационной безопасности. Механизмы обеспечения Безопасности. Виды защиты информации. | 2 |
| | 1.2 | Актуальность проблем информационной безопасности | Динамика числа зарегистрированных утечек информации в мире. Распределение утечек по странам и по виновнику. Распределение утечек по типам данных и по каналам. Основные тенденции: нарушения и проблемы | 2 |
| | 1.3 | Ландшафт угроз и | Понятие и классификация угроз. Моделирование угроз и оценка | 3 |

| | | | | |
|---|-----|--|---|---|
| | | уязвимостей | рисков. Примеры реализации угрозы нарушения конфиденциальности. Примеры реализации угрозы нарушения целостности данных. Примеры реализации угрозы отказа в доступе. | |
| | 1.4 | Законодательный уровень обеспечения ИБ | Меры законодательного уровня ИБ. Акты федерального законодательства. Нормативно-методические документы. Органы (подразделения), обеспечивающие информационную безопасность | 3 |
| 2 | 2.1 | Принципы обеспечения и информационной безопасности | Подходы к обеспечению информационной безопасности. Принципы обеспечения информационной безопасности. Методы обеспечения ИБ. Средства защиты информационных систем | 2 |
| | 2.2 | Классические симметричные криптосистемы | Основные понятия и определения. Шифры перестановки. Шифрующие таблицы. Применение магических квадратов. Шифры простой замены. Система шифрования Цезаря. Аффинная система подстановок Цезаря. Система Цезаря с ключевым словом. Одноразовая система шифрования. Шифрование методом гаммирования. Методы генерации псевдослучайных последовательностей чисел | 2 |
| | 2.2 | Современные симметричные криптосистемы | Американский стандарт шифрования данных DES. Алгоритм шифрования данных IDEA. Отечественный стандарт шифрования данных. Режим простой замены. Режим гаммирования. Режим гаммирования с обратной связью. Режим выработки имитовставки. Блочные и поточные шифры. Криптосистема с депонированием ключа. Процедура генерации ключей. Обслуживание ключей. Процедура дешифрования | 2 |
| | 2.3 | Асимметричные криптосистемы | Концепция криптосистемы с открытым ключом. Однонаправленные функции. Криптосистема шифрования данных | 4 |

| | | | | |
|---|-----|---|--|---|
| | | | <p>RSA. Процедуры шифрования и расшифрования в криптосистеме RSA. Безопасность и быстродействие криптосистемы RSA. Схема шифрования Полига – Хеллмана. Схема шифрования Эль Гамала. Комбинированный метод шифрования</p> | |
| | 2.4 | Управление криптографическими ключами. ЭЦП | <p>Генерация ключей. Хранение ключей. Носители ключевой информации. Концепция иерархии ключей. Распределение ключей. Распределение ключей с участием центра распределения ключей. Прямой обмен ключами между пользователями</p> | 4 |
| 3 | 3.1 | Стандарты в области ИБ | <p>Оценочные стандарты в области информационной безопасности. Структура требований «Оранжевой книги». Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий». Виды требований информационной безопасности</p> | 2 |
| | 3.2 | Защита персональных данных | <p>Аудит соответствия требованиям Российского законодательства в области защиты персональных данных</p> | 2 |
| | 3.3 | Методы и средства защиты от удаленных атак через сеть Internet. | <p>Социальная инженерия. Нападение и защита в социальных сетях.</p> | 3 |
| | 3.4 | Приватность и безопасность операционных систем. | <p>Средства и функциональные возможности безопасности Баги и уязвимости в безопасности Статистика использования систем Windows 10 - Отслеживание приватности Windows 10 - Контроль Wi-Fi Windows 7, 8 и 8.1 - слежка за личной информацией</p> | 2 |

3.2.2. Практические занятия, содержание и объем в часах

| | | | | |
|--|--|--|--|--|
| | | | | |
|--|--|--|--|--|

| Модуль | Номер раздела | Тема | Содержание | Трудоемкость (в часах) |
|--------|---------------|------|------------|------------------------|
| | | | | |

3.2.3. Лабораторные занятия, содержание и объем в часах

| Модуль | Номер раздела | Тема | Содержание | Трудоемкость (в часах) |
|--------|---------------|---|---|------------------------|
| 1 | 1.1 | Основы обеспечения комплексной защиты конфиденциальной информации | Аппаратно-программные средства защиты компьютерной информации. Схема описания инцидентов. Инциденты информационной безопасности. | 4 |
| | 1.2 | Актуальность проблем информационной безопасности | Описание и классификация угроз инцидентов ИБ Описание и характеристика атак в инцидентах ИБ | 2 |
| | 1.3 | Ландшафт угроз и уязвимостей | Описание и классификация угроз инцидентов ИБ. Социальная инженерия. Даркнет, темные рынки и наборы эксплойтов. Цензура | 5 |
| | 1.4 | Законодательный уровень обеспечения ИБ | Аппаратно-программные средства защиты компьютерной информации. Экспертные системы и базы знаний по информационной безопасности. Виды тайн | 5 |
| 2 | 2.1 | Принципы обеспечения информационной безопасности | Принципы обеспечения информационной безопасности Криптографическая защита информации. Экспертные системы и базы знаний по информационной безопасности | 2 |
| | 2.2 | Классические симметричные криптосистемы | Американский стандарт шифрования данных DES. Режим "Электронная кодовая книга". Режим "Сцепление блоков шифра". Режим "Обратная связь по шифру". Режим "Обратная связь по выходу". Области применения алгоритма DES | 2 |
| | 2.2 | Современные симметричные криптосистемы | Алгоритм шифрования данных IDEA. Режим гаммирования. Режим гаммирования с обратной связью. | 2 |

| | | | | |
|---|-----|---|---|---|
| | | ы | | |
| | 2.3 | Асимметричные криптосистемы | Криптосистема шифрования данных RSA. Схема шифрования Эль Гамала | 5 |
| | 2.4 | Управление криптографическими ключами. ЭЦП | Генерация ключей. Хранение ключей. Обмен. Системы управления и соответствия требованиям. Основные алгоритмы формирования ЭЦП. Хеш-функция. | 5 |
| 3 | 3.1 | Стандарты в области ИБ | Основные стандарты по информационной безопасности, особенности. Актуальные изменения | 2 |
| | 3.2 | Защита персональных данных | Основные принципы использования и защиты персональных данных. Порядок и особенности аудита. | 2 |
| | 3.3 | Методы и средства защиты от удаленных атак через сеть Internet. | Поведенческие меры безопасности от атак социального типа Технические средства защиты от атак социального типа | 5 |
| | 3.4 | Приватность и безопасность операционных систем. | Windows 10 - Инструмент "Disable Windows 10 Tracking" Windows 10 - Cortana Windows 10 - Контроль Wi-Fi Windows 7, 8 и 8.1 - слежка за личной информацией Mac - слежка за личной информацией | 4 |

3.3. Содержание материалов, выносимых на самостоятельное изучение

| Модуль | Номер раздела | Содержание материалов, выносимого на самостоятельное изучение | Виды самостоятельной деятельности | Трудоемкость (в часах) |
|--------|---------------|--|---------------------------------------|------------------------|
| 1 | 1.1 | Основы обеспечения комплексной защиты конфиденциальной информации Взаимосвязь понятий: опасность, фактор опасности, источник опасности, угроза, атака, риск | Составление терминологической системы | 5 |

| | | | | |
|---|-----|--|--|----|
| | 1.2 | Актуальность проблем информационной безопасности Анализ динамики и структуры правонарушений в сфере информационной безопасности в РФ за последние 10 лет | подготовка сообщений и докладов | 7 |
| | 1.3 | Основные угрозы информационной безопасности Компоненты угроз информационной безопасности современного предприятия | Составление конспекта, разработка макета угроз | 10 |
| | 1.4 | Законодательный уровень обеспечения ИБ 3 Структура нормативно-правовых документов по информационной безопасности | Анализ нормативных документов | 10 |
| 2 | 2.1 | Принципы обеспечения информационной безопасности Современные подходы к обеспечению информационной безопасности | Составления блок схем, выполнение тестирования | 5 |
| | 2.2 | Классические симметричные криптосистемы | Написание различных симметричных криптографических алгоритмов. Составления обзор таблицы. | 15 |
| | 2.3 | Асимметричные криптосистемы | Написание различных асимметричных алгоритмов, составление обзор-таблицы наиболее эффективных из них. | 10 |
| | 2.4 | Управление криптографическими ключами. ЭЦП | Проектный метод, анализ нормативной документации, реализация алгоритмов создания ЭЦП | 11 |
| 3 | 3.1 | Стандарты в области ИБ | Подготовка к | 5 |

| | | | | |
|--|-----|---|--|----|
| | | Национальные стандарты в области информационной безопасности (по странам) | интеллектуальной игре, составление конспекта | |
| | 3.2 | Защита персональных данных (ПДн) Базовая модель угроз безопасности ПДн при их обработке в информационных системах ПДн. | Проработка учебного материала лекций, расчеты по индивидуальному заданию, работа с литературой и НПА подготовка к лабораторным работам | 5 |
| | 3.3 | Поведенческие меры безопасности от атак социального типа | расчеты по индивидуальному заданию подготовка к лабораторным работам подготовка сообщений и докладов | 10 |
| | 3.4 | Мас - слежка за личной информацией Linux- и Unix-подобные операционные системы Linux - Debian 8 Jessie - Проблема добавления Дополнений гостевой ОС в Virtual Box | Проработка учебного материала лекций, работа с литературой и НПА, подготовка к лабораторным работам | 5 |

4. Фонд оценочных средств для проведения текущей и промежуточной аттестации обучающихся по дисциплине

Фонд оценочных средств текущего контроля и промежуточной аттестации по итогам освоения дисциплины представлен в приложении.

[Фонд оценочных средств](#)

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Основная литература

5.1.1. Печатные издания

1. 1. Бондарев В.В. Введение в информационную безопасность автоматизированных систем: учебное пособие / Бондарев В.В.- 2-е изд.- М.: Изд-во МГТУ им. Н. Э. Баумана, 2018. - 250 с.: ил. – 2. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий/ под ред. А.С. Маркова. – М.: ДМК Пресс, 2017.

5.1.2. Издания из ЭБС

1. 1. Информационная безопасность и защита информации [Электронный ресурс] / Шаньгин В.Ф. - М. : ДМК Пресс, 2014. - <http://www.studentlibrary.ru/book/ISBN9785940747680.html> 2. Информационная безопасность : Учебник и практикум / Нестеров Сергей Александрович; Нестеров С.А. - М. : Издательство Юрайт, 2017. - 321. - (Университеты России). - ISBN 978-5-534-00258-4 : 123.67.<http://www.biblioonline.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7>

5.2. Дополнительная литература

5.2.1. Печатные издания

1. 1. Ю.В. Романец и др. Защита информации в компьютерных системах и сетях Изд. 2-е., М:Радио и связь, 2001-376с. 2. Б. Шнаер Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си.-М.:ТРИУМФ, 2003-816с. 3. Математические и компьютерные основы криптологии: Учеб. пособие/Ю.С.Харин и др.-Минск:Новое Знание, 2003-382с. 4. Исагулиев К.П. Справочник по криптологии. Минск:Новое знание, 2004 - 237с

5.2.2. Издания из ЭБС

1. 1. Сайт веб-консорциума: <https://www.w3.org/> 2. ISO/IEC 12207:2008: Информационные технологии. Процессы жизненного цикла программного обеспечения: - http://www.iso.org/iso/ru/catalogue_detail?csnumber=43447;

5.3. Базы данных, информационно-справочные и поисковые системы

| Название | Ссылка |
|--|---|
| Scopus Поисковая система научной информации. Поиск по более чем 450 млн. научных документов. Кроме свободных сайтов, индексируются научные базы (NaturePublishing, LexisNexis, ScienceDirect, Sage и др.). | http://www.info.sciverse.com/scopus/ |
| Информационно-поисковая система Российских патентных документов | http://www1.fips.ru/wps/wcm/connect/content_ru/ru/inform_resources/inform_retrieval_system/ |

6. Перечень программного обеспечения

Программное обеспечение общего назначения: ОС Microsoft Windows, Microsoft Office, АБВУУ FineReader, ESET NOD32 Smart Security Business Edition, Foxit Reader, АИБС "МегаПро".

Программное обеспечение специального назначения:

- 1) Oracle VirtualBox
- 2) Python
- 3) Visual Studio
- 4) Visual Studio Community

7. Материально-техническое обеспечение дисциплины

| | |
|--|--|
| Наименование помещений для проведения учебных занятий и для самостоятельной работы обучающихся | Оснащенность специальных помещений и помещений для самостоятельной работы |
| Учебные аудитории для проведения занятий лекционного типа | Состав оборудования и технических средств обучения указан в паспорте аудитории, закреплённой расписанием по факультету |
| Учебные аудитории для проведения лабораторных занятий | |
| Учебные аудитории для проведения групповых и индивидуальных консультаций | Состав оборудования и технических средств обучения указан в паспорте аудитории, закреплённой расписанием по кафедре |
| Учебные аудитории для текущей аттестации | |

8. Методические рекомендации по организации изучения дисциплины

Общие методические рекомендации по изучению дисциплины

Практика преподавания дисциплины демонстрирует тот факт, что, несмотря на доступность необходимой информации по дисциплине (наличие учебников, учебных и учебно-методических пособий и печатном виде, в ЭБС, возможность получения информации из ресурсов сети интернет и т.д.), серьезные затруднения у студентов вызывают анализ, синтез, систематизация материала, а также выделение в нем принципиальных и существенных аспектов, отвечающим современным научным концепциям и подходам.

В связи с этим основным источником теоретического материала по дисциплине выступают лекции, посещение которых является обязательной составляющей успешного освоения дисциплины. Для эффективного освоения материала дисциплины необходимым является выполнение следующих требований:

- обязательное посещение всех лекционных и практических занятий, способствующее системному овладению материалом курса;
- все вопросы соответствующих разделов и тем по дисциплине необходимо фиксировать (на любых носителях информации);
- обязательное выполнение домашних заданий является важнейшим требованием и условием формирования целостного и системного знания по дисциплине;
- обязательность личной активности каждого студента на всех занятиях по дисциплине;
- в случаях неясности каких-либо вопросов, обсуждаемых на занятиях, необходимо задать соответствующие вопросы преподавателю, а не оставлять их непонятыми;
- в случаях пропусков занятий по уважительным причинам студентам предоставляется право подготовки и представления заданий и ответов на вопросы изученного материала, с

расчетом на помощь преподавателя в его усвоении;

- в случаях пропусков без уважительной причины студент обязан самостоятельно изучить соответствующий материал;
- необходимым условием является самостоятельность и инициативность студентов при контроле набора баллов по дисциплине для успешного прохождения промежуточной аттестации.

Порядок организации самостоятельной работы студентов

Самостоятельная работа студентов предполагает:

- самостоятельный поиск, обработку (анализ, синтез, обобщение и систематизацию), адаптацию необходимой по дисциплине информации;
- выполнение заданий для самостоятельной работы;
- изучение и усвоение теоретического материала, представленного на лекционных занятиях и в соответствующих литературных источниках (рекомендуемая основная и дополнительная литература);
- самостоятельное изучение отдельных вопросов курса;
- подготовка к практическим и семинарским занятиям, в соответствии с рекомендациями преподавателя (выполнение конкретных заданий, соответствующие организационные действия и т.д.).

Как правило, организация самостоятельной работы предполагает:

- постановку цели;
- составление соответствующего плана;
- поиск, обработку информации;
- представление результатов работы.

Разработчик/группа разработчиков:
Алёна Дмитриевна Федотова

Типовая программа утверждена

Согласована с выпускающей кафедрой
Заведующий кафедрой

_____ «___» _____ 20___ г.