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)

|  |  |
| --- | --- |
|  | УТВЕРЖДАЮПервый проректор – проректор по учебной работеМГТУ им. Н.Э. Баумана\_\_\_\_\_\_\_\_\_\_\_\_ Б.В. Падалкин«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_ г. |

Факультет «Информатика и системы управления»

Кафедра ИУ5 «Системы обработки информации и управления»

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ**

**И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ**

**«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

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. ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ С УКАЗАНИЕМ ЭТАПОВ ИХ ФОРМИРОВАНИЯ В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 4](#_Toc531151688)

[2. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ НА РАЗЛИЧНЫХ ЭТАПАХ ИХ ФОРМИРОВАНИЯ, ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ 5](#_Toc531151689)

[3. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 14](#_Toc531151690)

[4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ. 15](#_Toc531151691)

[4.1. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности. 15](#_Toc531151692)

[4.2. Процедуры оценивания знаний, умений, навыков, формы и организация текущего контроля успеваемости и промежуточной аттестации обучающихся. 27](#_Toc531151693)

**1.** **ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ С УКАЗАНИЕМ ЭТАПОВ ИХ ФОРМИРОВАНИЯ В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

Перечень компетенций (планируемых результатов освоения образовательной программы), выявленных в матрице компетенций, представлен в таблице 1 рабочей программы дисциплины совместно с планируемыми результатами обучения по дисциплине, а также в таблице 1 фонда оценочных средств (раздел 2) с указанием этапов (семестров) их освоения.

Результаты обучения вносят свой вклад в формирование различных компетенций, предусмотренных образовательной программой. В свою очередь, компетенции на разных уровнях категорий «знать», «уметь», «владеть» формируются модулями (разделами) дисциплины, а также различными дисциплинами образовательной программы.

# ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ НА РАЗЛИЧНЫХ ЭТАПАХ ИХ ФОРМИРОВАНИЯ, ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Фонд оценочных средств (ФОС) предусматривает:

* анализ комплекса **показателей** - дескрипторов освоения компетенций в виде результатов обучения, которые студент может продемонстрировать (см. табл.1). Для контроля достижения каждого из них должны быть предусмотрены оценочные средства в виде вопросов, заданий и т.д.;
* обозначение **критериев** - правил принятия решения по оценке достигнутых результатов обучения и сформированности компетенций.

В качестве шкалы оценивания принимается 100-бальная система с выделением с градацией оценок в соответствии с Положением о текущем контроле успеваемости и промежуточной аттестации студентов МГТУ им. Н.Э. Баумана:

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

Показатели достижения планируемых результатов обучения и критерии их оценивания на разных уровнях формирования компетенций приведены в таблице 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)** | **Этап (се-местр)** | **Наименование оценочного средства** | **Критерии оценивания результатов обучения** |
| --- | --- | --- | --- | --- |
| ОПКС-1Способен 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 компонентовУМЕТЬ- применять естественнонаучные и общеинженерные знания, методы математического моделирования, анализа, и синтеза, теоретического и экспериментального исследования в профессиональной деятельностиВЛАДЕТЬ- навыками применения естественнонаучных и общеинженерных знаний, методов математического моделирования, анализа, и синтеза, теоретического и экспериментального исследования в профессиональной деятельности | 1 | Работа на семинарахРубежные контролиДомашнее заданиеПосещение лекций | Правильность и полнота ответов на вопросы рубежных контролей. Глубина понимания темы домашнего задания. Степень участия в обсуждении темы семинара. Объем посещенных лекций. |
| УКС-1Способен 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 ИнтернетУМЕТЬ- применять методики поиска, сбора, обработки информации, ее смысловой оптимизации и наглядного представления- проводить систематизацию, классификацию, интерпретацию соответствующей информации- выстраивать логику рассуждений и высказыванийВЛАДЕТЬ- методами поиска, сбора и обработки, критического анализа и синтеза информации, ее смысловой оптимизации и наглядного представления- навыками самостоятельного критического мышления | 1 | Работа на семинарахРубежные контролиДомашнее заданиеПосещение лекций | Правильность и полнота ответов на вопросы рубежных контролей. Глубина понимания темы домашнего задания. Степень участия в обсуждении темы семинара. Объем посещенных лекций. |
| ПКСо-1Способен 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 результатыВЛАДЕТЬ- практическими навыками поиска научно-технической информации по теме исследования | 1 | Работа на семинарахРубежные контролиДомашнее заданиеПосещение лекций | Правильность и полнота ответов на вопросы рубежных контролей. Глубина понимания темы домашнего задания. Степень участия в обсуждении темы семинара. Объем посещенных лекций. |
| ОПКС-2Способен 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 компонентовУМЕТЬ- использовать современные информационные технологии и программные средства отечественного и иностранного производства при решении задач профессиональной деятельностиВЛАДЕТЬ- методиками применения современных информационных технологий и программных средств отечественного и иностранного производства при решении задач профессиональной деятельности | 1 | Работа на семинарахРубежные контролиДомашнее заданиеПосещение лекций | Правильность и полнота ответов на вопросы рубежных контролей. Глубина понимания темы домашнего задания. Степень участия в обсуждении темы семинара. Объем посещенных лекций. |
| УКС-2Способен 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 деятельностьУМЕТЬ- 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 задачВЛАДЕТЬ- методиками разработки цели (целеполагания) и задач проекта- методами оценки потребности в ресурсах, продолжительности и стоимости проекта- навыками работы с нормативно-правовой документацией | 1 | Работа на семинарахРубежные контролиДомашнее заданиеПосещение лекций | Правильность и полнота ответов на вопросы рубежных контролей. Глубина понимания темы домашнего задания. Степень участия в обсуждении темы семинара. Объем посещенных лекций. |
| ОПКС-3Способен 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 безопасностиУМЕТЬ- решать стандартные задачи профессиональной деятельности на основе математической, информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасностиВЛАДЕТЬ- 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 | 1 | Работа на семинарахРубежные контролиДомашнее заданиеПосещение лекций | Правильность и полнота ответов на вопросы рубежных контролей. Глубина понимания темы домашнего задания. Степень участия в обсуждении темы семинара. Объем посещенных лекций. |
| УКС-3Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде, толерантно воспринимая социальные и культурные и иные различия | ЗНАТЬ- основные понятия, технологии межличностной и групповой коммуникацииУМЕТЬ- устанавливать и поддерживать социальные контакты, обеспечивающие успешную работу в коллективе- применять основные методы и нормы социального взаимодействия для реализации своей роли и взаимодействия внутри командыВЛАДЕТЬ- методами и приемами социального взаимодействия и работы в команде | 1 | Работа на семинарахРубежные контролиДомашнее заданиеПосещение лекций | Правильность и полнота ответов на вопросы рубежных контролей. Глубина понимания темы домашнего задания. Степень участия в обсуждении темы семинара. Объем посещенных лекций. |
| УКС-4Способен 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 коммуникацииУМЕТЬ- применять на практике деловую коммуникацию в устной и письменной формах, методы и навыки делового общения на русском и иностранном языкахВЛАДЕТЬ- навыками деловых коммуникаций в устной и письменной форме на русском и иностранном языках | 1 | Работа на семинарахРубежные контролиДомашнее заданиеПосещение лекций | Правильность и полнота ответов на вопросы рубежных контролей. Глубина понимания темы домашнего задания. Степень участия в обсуждении темы семинара. Объем посещенных лекций. |
| ОПКС-5Способен 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 системУМЕТЬ- собирать аппаратуру, и инсталлировать отечественное и иностранное программное обеспечение для информационных и автоматизированных систем | 1 | Работа на семинарахРубежные контролиДомашнее заданиеПосещение лекций | Правильность и полнота ответов на вопросы рубежных контролей. Глубина понимания темы домашнего задания. Степень участия в обсуждении темы семинара. Объем посещенных лекций. |
| УКС-6Способен 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 жизниУМЕТЬ- эффективно планировать и контролировать собственное времяВЛАДЕТЬ- методами управления собственным временем- технологиями приобретения, использования и обновления социокультурных и профессиональных знаний, умений и навыков | 1 | Работа на семинарахРубежные контролиДомашнее заданиеПосещение лекций | Правильность и полнота ответов на вопросы рубежных контролей. Глубина понимания темы домашнего задания. Степень участия в обсуждении темы семинара. Объем посещенных лекций. |
| ПКС-6Способен 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 системахУМЕТЬ- применять методы принятия решений в автоматизированных системах организационного управленияВЛАДЕТЬ- навыками моделирования процессов жизненного цикла информационных систем | 1 | Работа на семинарахРубежные контролиДомашнее заданиеПосещение лекций | Правильность и полнота ответов на вопросы рубежных контролей. Глубина понимания темы домашнего задания. Степень участия в обсуждении темы семинара. Объем посещенных лекций. |

##

Критерии оценки результатов обучения при различных видах контрольных мероприятий приведены в таблицах:

|  |
| --- |
| **Критерии оценивания результатов рубежного контроля (РК):** |
| **Критерии начисления баллов** | **Оценка** |
| Ответы содержательные, уверенные и четкие; показано свободное владение материалом различной степени сложности | *От\_85\_ до\_100\_% от максимального количества баллов за РК* |
| Твердо усвоен основной материал; ответы удовлетворяют требованиям, установленным для максимальной оценки, но при этом допускаются негрубые ошибки; делаются несущественные пропуски при изложении фактического материала. | *От\_71\_ до\_84\_ % от максимального количества баллов за РК* |
| Обучаемый знает и понимает основной материал программы, основные темы, но в усвоении материала имеются пробелы; излагает его упрощенно, с ошибками и затруднениями; изложение теоретического материала приводится с ошибками.  | *От\_60\_ до\_70\_ % от максимального количества баллов за РК* |
| Отказ от ответа или отсутствие минимальных знаний по дисциплине; присутствуют грубые ошибки в ответе. | *От\_0\_ до\_59\_ % от максимального количества баллов за РК* |

|  |
| --- |
| **Критерии оценивания доклада (домашнее задание):***От 17 до 20 баллов:* глубокое и хорошо аргументированное обоснование темы; четкая формулировка и понимание изучаемой проблемы; широкое и правильное использование относящейся к теме литературы и примененных аналитических методов; содержание исследования и ход защиты указывают на наличие навыков работы студента в данной области; оформление работы хорошее с наличием расширенной библиографии; выступление с докладом показало высокий уровень профессиональной подготовленности студента; *От 14 до 16 баллов:* аргументированное обоснование темы; четкая формулировка и понимание изучаемой проблемы; использование ограниченного, но достаточного для проведения исследования количества источников; работа основана на среднем по глубине анализе изучаемой проблемы и при этом сделано незначительное число обобщений; содержание исследования и выступление с докладом указывают на наличие практических навыков работы студента в данной области; доклад хорошо оформлен с наличием необходимой библиографии; выступление с докладом показало достаточную научную и профессиональную подготовку студента; *От 12 до 13 баллов:* достаточное обоснование выбранной темы, но отсутствует глубокое понимание рассматриваемой проблемы; в библиографии преобладают ссылки на стандартные литературные источники; труды, необходимые для всестороннего изучения проблемы, использованы в ограниченном объеме; заметна нехватка компетентности студента в данной области знаний; оформление доклада содержит небрежности; выступление с докладом показало удовлетворительную профессиональную подготовку студента; *От 0 до 11 баллов:* тема доклада представлена в общем виде; ограниченное число использованных литературных источников; шаблонное изложение материала; суждения по исследуемой проблеме не всегда компетентны; неточности и неверные выводы по рассматриваемой литературе; оформление доклада с элементами заметных отступлений от общих требований; во время выступления с докладом студентом проявлена ограниченная профессиональная эрудиция. |

|  |
| --- |
| **Критерии оценивания посещения лекций** (1 и 2 модули):*От 9 до 10 баллов:* Посещение всех лекций. Высокий уровень структурирования информации, полнота выделенных опорных понятий и тезисов.*От 7 до 8 баллов:* Посещение не менее 90 процентов лекций. Необходимый уровень структурирования информации, выделение понятий.*6 баллов:* Посещение не менее 70 процентов лекций. Наличие конспектов.*От 0 до 5 баллов:* Посещение менее 70 процентов занятий. Отсутствие конспектов. |
| **Критерии оценивания работы на семинарах**На каждом семинаре проводится опрос студентов по теме семинара. Ответы на вопросы по темам семинаров № 1-4 оцениваются следующим образом:*1 балл*: правильный ответ;*0 баллов*: неправильный ответ, отсутствие ответа.Ответы на вопросы по темам семинаров № 5-12 оцениваются следующим образом:*2 балла*: правильный содержательный ответ;*1 балл*: частично правильный ответ, допущены существенные неточности;*0 баллов*: неправильный ответ, отсутствие ответа.Суммарно в каждом модуле за работу на семинарах студент может набрать неболее 10 баллов. |
| **Критерии оценивания на зачете (для ликвидации академической задолженности, или перезачета дисциплины для студентов, переводящихся из других вузов, или для повышения балльной оценки за отдельные модули дисциплины):** Билет включает три вопроса. Каждый вопрос оценивается следующим образом:*5 баллов*: студент правильно и полно ответил на вопрос билета;*4 балла:* студент правильно ответил на вопрос билета, но ответ содержит некоторые неточности в формулировках и терминологии;*3 балла*: в ответе на вопрос билета студент продемонстрировал общее понимание материала, но допустил значительные неточности, ответил на вопрос частично;*от 0 до 2 баллов*: студент неправильно ответил на вопрос билета или не ответил на него вообще. |

Использование показателей и критериев оценивания компетенций на различных этапах их формирования совместно со шкалой балльно-рейтинговой системы позволяет формировать результаты обучения по модулям.

**Оценка результатов обучения**

|  |  |  |  |
| --- | --- | --- | --- |
| **Неделя** | **Номер и название модуля** | **Формы контроля** | **Баллы****(мин/****макс)** |
| **1 семестр** |
| 7 | 1. Система технической защиты информации
 | Рубежный контроль №1 | 12 / 20 |
| Работа на семинарах  | 6 / 10 |
| Посещение лекций | 6 / 10 |
| **ИТОГО** | **24 / 40** |
| 12  | 1. Методы и средства технической защиты информации
 | Рубежный контроль №2 | 12 / 20 |
| Работа на семинарах | 6 / 10 |
| Домашнее задание | 12 / 20 |
| Посещение лекций | 6 / 10 |
| **ИТОГО** | **36 / 60** |
|  |  | **ИТОГО за семестр** | **60 / 100** |

1. **ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

ФОС по дисциплине содержит следующие оценочные средства, позволяющие оценить знания, умения и уровень приобретенных компетенций при текущем и промежуточном контроле, разбитые по модулям дисциплины:

* примеры типовых вопросов по темам для оценки работы на семинарах;
* примеры вариантов рубежных контролей;
* список типовых тем для докладов (домашнее задание);
* вопросы для зачета (для ликвидации академической задолженности, или перезачета дисциплины для студентов, переводящихся из других вузов, или для повышения балльной оценки за отдельные модули дисциплины).

Средства для оценки различных уровней формирования компетенций по категориям знать, уметь, владеть обеспечивают реализацию следующих основных принципов контроля, таких, как объективность и независимость, практико-ориентированность, междисциплинарность.

С учетом этого, контрольные вопросы, задания, задачи, входящие a ФОС, для различных категорий и уровней освоения компетенций имеют вид.

**ЗНАТЬ**

**Примеры:**

1. Структура, задачи и основные функции государственной системы защиты информации.
2. Порядок лицензирования деятельности в области технической защиты конфиденциальной информации.
3. Основные рекомендации по защите информации, составляющей коммерческую тайну.

**УМЕТЬ**

**Примеры:**

1. Подключать и настраивать с учетом требований ТЗИ модули ЭВМ и периферийного оборудования.
2. Проверять с учетом требований ТЗИ техническое состояние вычислительного оборудования.
3. Составлять с учетом требований ТЗИ инструкции по эксплуатации оборудования.

**ВЛАДЕТЬ**

**Примеры:**

1. Навыками проверки с учетом требований ТЗИ состояния вычислительного оборудования и осуществления необходимых профилактических процедур для ИВТ.
2. Навыками написания с учетом требований ТЗИ инструкций по эксплуатации оборудования в области ИВТ.
3. Навыками подключения и настройки с учетом требований ТЗИ модулей ЭВМ и периферийного оборудования.
4. **МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ.**

**4.1. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности.**

|  |  |  |
| --- | --- | --- |
| **Наименование оценочного средства** | **Краткая характеристика оценочного средства** | **Представление оценочного средства в фонде** |
| Рубежный контроль | Средство проверки освоения уровней «знать», «уметь» компетенций СУОС 3++ | Примеры вариантов рубежных контролей. |
| Работа на семинарах | Средство проверки освоения уровней «знать», «уметь» компетенций СУОС 3++ | Примеры типовых вопросов для оценки работы на семинарах |
| Домашнее задание (доклад) | Средство проверки освоения уровней «знать» компетенций СУОС 3++ | Список типовых тем для докладов |
| Зачет (для ликвидации академической задолженности, или перезачета дисциплины для студентов, переводящихся из других вузов, или для повышения балльной оценки за отдельные модули дисциплины) | Средство проверки освоения уровней «знать», «уметь» компетенций СУОС 3++ | Перечень вопросов к зачету |

**Примеры вариантов рубежных контролей**

Кафедра «Системы обработки информации и управления»

по дисциплине «Защита информации»

**Рубежный контроль №1**

**Вариант №1**

1. Актуальность технической защиты конфиденциальной информации (ТЗИ).
2. Порядок лицензирования деятельности в области технической защиты конфиденциальной информации.
3. Общая характеристика компьютерной разведки.

**Вариант №2**

1. Структура, задачи и основные функции государственной системы защиты информации.
2. Лицензирование деятельности в области защиты информации, сертификация средств защиты информации и аттестация объектов информатизации.
3. Виды компьютерной разведки и их характеристика.

**Вариант №3**

1. Цели, задачи, структура, функции и роль информационной безопасности в системе национальной безопасности Российской Федерации.
2. Аттестация объектов информатизации.
3. Взаимодействие компьютерной разведки с другими видами технической разведки и способы комплексной технической разведки.

**Рубежный контроль №2**

**Вариант №1**

1. Общая характеристика оценки защищенности конфиденциальной информации от ее утечки по техническим каналам.
2. Защита кабинетов руководителей и помещений, предназначенных для проведения переговоров, от съема информации.
3. Идентификация и проверка подлинности.

**Вариант №2**

1. Оценка защищенности помещений от утечки речевой информации по акустическим и виброакустическим каналам.
2. Организация работ по комплексной защите информации от утечки по техническим каналам.
3. Обеспечение безопасности информации при подключении вычислительных средств к международным информационным системам.

**Вариант №3**

1. Оценка защищенности основных технических средств и систем от утечки информации по электромагнитным каналам.
2. Организация и проведение работ по защите информации от ее утечки по техническим каналам на объектах информатизации.
3. Сертифицированные программно-аппаратные средства.

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

(подпись)

**Перечень типовых вопросов по темам для оценки работы на семинарах**

Кафедра «Системы обработки информации и управления»

по дисциплине «Защита информации»

***Модуль 1.   Система технической защиты информации***

***Тема 1. Основы технической защиты конфиденциальной информации***

1. Актуальность технической защиты конфиденциальной информации (ТЗИ).
2. Роль защиты информации в области информатики и вычислительной техники.
3. Особенности создания защищенных автоматизированных систем обработки информации и управления.

***Тема 2. Государственная система защиты информации***

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

***Тема 3. Правовое регулирование ТЗИ***

1. Законодательная и нормативная база правового регулирования вопросов защиты информации.
2. 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.
3. Лицензирование деятельности в области защиты информации, сертификация средств защиты информации и аттестация объектов информатизации.
4. Порядок лицензирования деятельности в области технической защиты конфиденциальной информации.
5. Порядок сертификации технических средств защиты информации по требованиям безопасности информации.
6. Аттестация объектов информатизации.

***Тема 4. Специальные требования и рекомендации по технической защите конфиденциальной информации***

1. Общая характеристика основных специальных требований и рекомендаций по технической защите конфиденциальной информации.
2. Основные требования и рекомендации по защите речевой информации, циркулирующей в защищаемых помещениях.
3. Основные требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники.
4. Основные требования и рекомендации по защите служебной тайны и персональных данных.
5. Основные рекомендации по защите информации, составляющей коммерческую тайну.
6. Порядок обеспечения защиты информации при эксплуатации автоматизированных систем.
7. Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ.
8. Защита информации в локальных вычислительных сетях.
9. Защита информации при межсетевом взаимодействии.
10. Защита информации при работе с системами управления базами данных.
11. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.

***Тема 5. Технические каналы утечки информации и их характеристики***

1. Общая характеристика технических каналов утечки информации и их классификация.
2. Механизмы возникновения технических каналов утечки информации.
3. Технические каналы утечки речевой информации.
4. Характеристика акустического, виброакустического, электроакустического, электромагнитного каналов утечки информации.
5. Механизмы возникновения акустического, виброакустического, электроакустического, электромагнитного каналов утечки информации.
6. Технические средства и методы получения информации по акустическим, виброакустическим, электроакустическим, электромагнитным каналам утечки информации.
7. Утечка информации за счет побочных электромагнитных излучений и наводок (ПЭМИН).
8. Механизмы возникновения утечки информации по каналам ПЭМИН.
9. Технические средства и методы получения информации с использованием каналов ПЭМИН.

***Тема 6. Компьютерная разведка***

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

***Тема 7. Оценка защищенности конфиденциальной информации от ее утечки по техническим каналам***

1. Общая характеристика оценки защищенности конфиденциальной информации от ее утечки по техническим каналам.
2. Оценка защищенности помещений от утечки речевой информации по акустическим и виброакустическим каналам.
3. Оценка защищенности основных технических средств и систем от утечки информации по электромагнитным каналам.
4. Оценка защищенности помещений от утечки речевой информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах.
5. Оценка защищенности информации, обрабатываемой в основных технических средствах и системах от утечки за счет наводок.

***Модуль 2.   Методы и средства технической защиты информации***

***Тема 8. Проведение аттестационных испытаний на объектах информатизации***

1. Общая характеристика проведения аттестационных испытаний на объектах информатизации.
2. Необходимость проведения аттестационных испытаний.
3. Документация, необходимая для проведения аттестационных испытаний.
4. Аппаратура для проведения аттестационных испытаний.
5. Взаимодействие со специалистами по защите информации.
6. Возможность развития объектов информатизации и внесения изменений в документацию аттестационных испытаний на объектах информатизации.

***Тема 9. Методы защиты информации***

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

***Тема 10. Технические средства защиты информации***

1. Общая характеристика технических средств защиты информации.
2. Генераторы шума для защиты основных технических средств и систем (ОТСС) и подавления радиомикрофонов и диктофонов.
3. Основные принципы построения генераторов шума.
4. Модели генераторов шума, их технические характеристики и особенности применения.
5. Защита сети электропитания и заземления.
6. Основные принципы защиты информации от утечки по сети электропитания и заземления.
7. Технические средства, используемые для защиты, их технические характеристики.
8. Системы виброакустического зашумления.
9. Основные принципы построения и действия генераторов и датчиков.
10. Модели и их технические характеристики.
11. Особенности практического применения.
12. Способы защиты информации в телефонных линиях связи.
13. Пассивные и активные средства защиты телефонных линий связи от перехвата информации и их технические характеристики.

***Тема 11. Криптографические средства защиты информации***

1. Общая характеристика криптографических средств защиты информации.
2. Принципы криптографической защиты информации.
3. Аппаратно-программные средства защиты компьютерной информации.
4. Классические симметричные криптосистемы. Основные понятия и определения.
5. Шифры перестановки.
6. Шифрующие таблицы.
7. Методы генерации псевдослучайных последовательностей чисел.
8. Современные симметричные криптосистемы.
9. Американский стандарт шифрования данных DES.
10. Отечественный стандарт шифрования данных.
11. Блочные и поточные шифры.
12. Асимметричные криптосистемы.
13. Концепция криптосистемы с открытым ключом.
14. Криптосистема шифрования данных RSA.
15. Идентификация и проверка подлинности.
16. Идентификация и аутентификация пользователя.
17. Типовые схемы идентификации и аутентификации пользователя.
18. Особенности применения пароля для аутентификации пользователя.
19. Биометрическая идентификация и аутентификация.
20. Взаимная проверка подлинности пользователей.

***Тема 12. Программно-аппаратные средства защиты информации***

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

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

(подпись)

**Список типовых тем для докладов (домашнее задание)**

Кафедра «Системы обработки информации и управления»

по дисциплине «Защита информации»

1. Актуальность технической защиты конфиденциальной информации (ТЗИ).
2. Роль защиты информации в области информатики и вычислительной техники.
3. Особенности создания защищенных автоматизированных систем обработки информации и управления.
4. Структура, задачи и основные функции государственной системы защиты информации.
5. Цели, задачи, структура, функции и роль информационной безопасности в системе национальной безопасности Российской Федерации.
6. Основные термины и определения в области технической защиты информации.
7. Законодательная и нормативная база правового регулирования вопросов защиты информации.
8. 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.
9. Лицензирование деятельности в области защиты информации, сертификация средств защиты информации и аттестация объектов информатизации.
10. Порядок лицензирования деятельности в области технической защиты конфиденциальной информации.
11. Порядок сертификации технических средств защиты информации по требованиям безопасности информации.
12. Аттестация объектов информатизации.
13. Общая характеристика основных специальных требований и рекомендаций по технической защите конфиденциальной информации.
14. Основные требования и рекомендации по защите речевой информации, циркулирующей в защищаемых помещениях.
15. Основные требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники.
16. Основные требования и рекомендации по защите служебной тайны и персональных данных.
17. Основные рекомендации по защите информации, составляющей коммерческую тайну.
18. Порядок обеспечения защиты информации при эксплуатации автоматизированных систем.
19. Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ.
20. Защита информации в локальных вычислительных сетях.
21. Защита информации при межсетевом взаимодействии.
22. Защита информации при работе с системами управления базами данных.
23. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.
24. Общая характеристика технических каналов утечки информации и их классификация.
25. Механизмы возникновения технических каналов утечки информации.
26. Технические каналы утечки речевой информации.
27. Характеристика акустического, виброакустического, электроакустического, электромагнитного каналов утечки информации.
28. Механизмы возникновения акустического, виброакустического, электроакустического, электромагнитного каналов утечки информации.
29. Технические средства и методы получения информации по акустическим, виброакустическим, электроакустическим, электромагнитным каналам утечки информации.
30. Утечка информации за счет побочных электромагнитных излучений и наводок (ПЭМИН).
31. Механизмы возникновения утечки информации по каналам ПЭМИН.
32. Технические средства и методы получения информации с использованием каналов ПЭМИН.
33. Общая характеристика компьютерной разведки.
34. Виды компьютерной разведки и их характеристика.
35. Взаимодействие компьютерной разведки с другими видами технической разведки и способы комплексной технической разведки.
36. Угрозы технической разведки.
37. Общая характеристика оценки защищенности конфиденциальной информации от ее утечки по техническим каналам.
38. Оценка защищенности помещений от утечки речевой информации по акустическим и виброакустическим каналам.
39. Оценка защищенности основных технических средств и систем от утечки информации по электромагнитным каналам.
40. Оценка защищенности помещений от утечки речевой информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах.
41. Оценка защищенности информации, обрабатываемой в основных технических средствах и системах от утечки за счет наводок.
42. Общая характеристика проведения аттестационных испытаний на объектах информатизации.
43. Необходимость проведения аттестационных испытаний.
44. Документация, необходимая для проведения аттестационных испытаний.
45. Аппаратура для проведения аттестационных испытаний.
46. Взаимодействие со специалистами по защите информации.
47. Возможность развития объектов информатизации и внесения изменений в документацию аттестационных испытаний на объектах информатизации.
48. Общая характеристика методов защиты информации.
49. Организация работ по обеспечению комплексной защиты сведений, составляющих конфиденциальную информацию.
50. Организация охраны, пропускного режима и объектового режима.
51. Организация работ по комплексной защите информации от утечки по техническим каналам.
52. Защита территории, здания, помещений от несанкционированного проникновения (охранная сигнализация, системы обзорного телевидения, металлодетекторы, дозиметры, досмотровые зеркала).
53. Модели, технические характеристики используемых устройств.
54. Защита кабинетов руководителей и помещений, предназначенных для проведения переговоров, от съема информации.
55. Организация и проведение работ по защите информации от ее утечки по техническим каналам на объектах информатизации.
56. Пассивные и активные методы, используемые при создании систем защиты информации.
57. Экранирование как метод предотвращения утечки информации за счет ПЭМИН.
58. Фильтрация как метод предотвращения утечки информации по проводным коммуникациям.
59. Маскирование шумоподобными сигналами.
60. Маскирование методом преобразования речевой информации.
61. Общая характеристика технических средств защиты информации.
62. Генераторы шума для защиты основных технических средств и систем (ОТСС) и подавления радиомикрофонов и диктофонов.
63. Основные принципы построения генераторов шума.
64. Модели генераторов шума, их технические характеристики и особенности применения.
65. Защита сети электропитания и заземления.
66. Основные принципы защиты информации от утечки по сети электропитания и заземления.
67. Технические средства, используемые для защиты, их технические характеристики.
68. Системы виброакустического зашумления.
69. Основные принципы построения и действия генераторов и датчиков.
70. Модели и их технические характеристики.
71. Особенности практического применения.
72. Способы защиты информации в телефонных линиях связи.
73. Пассивные и активные средства защиты телефонных линий связи от перехвата информации и их технические характеристики.
74. Общая характеристика криптографических средств защиты информации.
75. Принципы криптографической защиты информации.
76. Аппаратно-программные средства защиты компьютерной информации.
77. Классические симметричные криптосистемы. Основные понятия и определения.
78. Шифры перестановки.
79. Шифрующие таблицы.
80. Методы генерации псевдослучайных последовательностей чисел.
81. Современные симметричные криптосистемы.
82. Американский стандарт шифрования данных DES.
83. Отечественный стандарт шифрования данных.
84. Блочные и поточные шифры.
85. Асимметричные криптосистемы.
86. Концепция криптосистемы с открытым ключом.
87. Криптосистема шифрования данных RSA.
88. Идентификация и проверка подлинности.
89. Идентификация и аутентификация пользователя.
90. Типовые схемы идентификации и аутентификации пользователя.
91. Особенности применения пароля для аутентификации пользователя.
92. Биометрическая идентификация и аутентификация.
93. Взаимная проверка подлинности пользователей
94. Общая характеристика программно-аппаратных средств защиты информации.
95. Сертифицированные программно-аппаратные средства.
96. Способы освоения систем защиты информации с применением программно-аппаратных средств защиты информации от несанкционированного доступа.
97. Обеспечение безопасности информации при подключении вычислительных средств к международным информационным системам.
98. Требования руководящих документов по обеспечению информационной безопасности при использовании информационно-телекоммуникационных сетей международного информационного обмена.
99. Особенности обеспечения безопасности информации при подключении автоматизированных систем к международным информационным системам, в том числе Интернет.

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

(подпись)

**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)**

Кафедра «Системы обработки информации и управления»

по дисциплине «Защита информации»

1. Актуальность технической защиты конфиденциальной информации (ТЗИ).
2. Роль защиты информации в области информатики и вычислительной техники.
3. Особенности создания защищенных автоматизированных систем обработки информации и управления.
4. Структура, задачи и основные функции государственной системы защиты информации.
5. Цели, задачи, структура, функции и роль информационной безопасности в системе национальной безопасности Российской Федерации.
6. Основные термины и определения в области технической защиты информации.
7. Законодательная и нормативная база правового регулирования вопросов защиты информации.
8. 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.
9. Лицензирование деятельности в области защиты информации, сертификация средств защиты информации и аттестация объектов информатизации.
10. Порядок лицензирования деятельности в области технической защиты конфиденциальной информации.
11. Порядок сертификации технических средств защиты информации по требованиям безопасности информации.
12. Аттестация объектов информатизации.
13. Общая характеристика основных специальных требований и рекомендаций по технической защите конфиденциальной информации.
14. Основные требования и рекомендации по защите речевой информации, циркулирующей в защищаемых помещениях.
15. Основные требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники.
16. Основные требования и рекомендации по защите служебной тайны и персональных данных.
17. Основные рекомендации по защите информации, составляющей коммерческую тайну.
18. Порядок обеспечения защиты информации при эксплуатации автоматизированных систем.
19. Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ.
20. Защита информации в локальных вычислительных сетях.
21. Защита информации при межсетевом взаимодействии.
22. Защита информации при работе с системами управления базами данных.
23. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.
24. Общая характеристика технических каналов утечки информации и их классификация.
25. Механизмы возникновения технических каналов утечки информации.
26. Технические каналы утечки речевой информации.
27. Характеристика акустического, виброакустического, электроакустического, электромагнитного каналов утечки информации.
28. Механизмы возникновения акустического, виброакустического, электроакустического, электромагнитного каналов утечки информации.
29. Технические средства и методы получения информации по акустическим, виброакустическим, электроакустическим, электромагнитным каналам утечки информации.
30. Утечка информации за счет побочных электромагнитных излучений и наводок (ПЭМИН).
31. Механизмы возникновения утечки информации по каналам ПЭМИН.
32. Технические средства и методы получения информации с использованием каналов ПЭМИН.
33. Общая характеристика компьютерной разведки.
34. Виды компьютерной разведки и их характеристика.
35. Взаимодействие компьютерной разведки с другими видами технической разведки и способы комплексной технической разведки.
36. Угрозы технической разведки.
37. Общая характеристика оценки защищенности конфиденциальной информации от ее утечки по техническим каналам.
38. Оценка защищенности помещений от утечки речевой информации по акустическим и виброакустическим каналам.
39. Оценка защищенности основных технических средств и систем от утечки информации по электромагнитным каналам.
40. Оценка защищенности помещений от утечки речевой информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах.
41. Оценка защищенности информации, обрабатываемой в основных технических средствах и системах от утечки за счет наводок.
42. Общая характеристика проведения аттестационных испытаний на объектах информатизации.
43. Необходимость проведения аттестационных испытаний.
44. Документация, необходимая для проведения аттестационных испытаний.
45. Аппаратура для проведения аттестационных испытаний.
46. Взаимодействие со специалистами по защите информации.
47. Возможность развития объектов информатизации и внесения изменений в документацию аттестационных испытаний на объектах информатизации.
48. Общая характеристика методов защиты информации.
49. Организация работ по обеспечению комплексной защиты сведений, составляющих конфиденциальную информацию.
50. Организация охраны, пропускного режима и объектового режима.
51. Организация работ по комплексной защите информации от утечки по техническим каналам.
52. Защита территории, здания, помещений от несанкционированного проникновения (охранная сигнализация, системы обзорного телевидения, металлодетекторы, дозиметры, досмотровые зеркала).
53. Модели, технические характеристики используемых устройств.
54. Защита кабинетов руководителей и помещений, предназначенных для проведения переговоров, от съема информации.
55. Организация и проведение работ по защите информации от ее утечки по техническим каналам на объектах информатизации.
56. Пассивные и активные методы, используемые при создании систем защиты информации.
57. Экранирование как метод предотвращения утечки информации за счет ПЭМИН.
58. Фильтрация как метод предотвращения утечки информации по проводным коммуникациям.
59. Маскирование шумоподобными сигналами.
60. Маскирование методом преобразования речевой информации.
61. Общая характеристика технических средств защиты информации.
62. Генераторы шума для защиты основных технических средств и систем (ОТСС) и подавления радиомикрофонов и диктофонов.
63. Основные принципы построения генераторов шума.
64. Модели генераторов шума, их технические характеристики и особенности применения.
65. Защита сети электропитания и заземления.
66. Основные принципы защиты информации от утечки по сети электропитания и заземления.
67. Технические средства, используемые для защиты, их технические характеристики.
68. Системы виброакустического зашумления.
69. Основные принципы построения и действия генераторов и датчиков.
70. Модели и их технические характеристики.
71. Особенности практического применения.
72. Способы защиты информации в телефонных линиях связи.
73. Пассивные и активные средства защиты телефонных линий связи от перехвата информации и их технические характеристики.
74. Общая характеристика криптографических средств защиты информации.
75. Принципы криптографической защиты информации.
76. Аппаратно-программные средства защиты компьютерной информации.
77. Классические симметричные криптосистемы. Основные понятия и определения.
78. Шифры перестановки.
79. Шифрующие таблицы.
80. Методы генерации псевдослучайных последовательностей чисел.
81. Современные симметричные криптосистемы.
82. Американский стандарт шифрования данных DES.
83. Отечественный стандарт шифрования данных.
84. Блочные и поточные шифры.
85. Асимметричные криптосистемы.
86. Концепция криптосистемы с открытым ключом.
87. Криптосистема шифрования данных RSA.
88. Идентификация и проверка подлинности.
89. Идентификация и аутентификация пользователя.
90. Типовые схемы идентификации и аутентификации пользователя.
91. Особенности применения пароля для аутентификации пользователя.
92. Биометрическая идентификация и аутентификация.
93. Взаимная проверка подлинности пользователей
94. Общая характеристика программно-аппаратных средств защиты информации.
95. Сертифицированные программно-аппаратные средства.
96. Способы освоения систем защиты информации с применением программно-аппаратных средств защиты информации от несанкционированного доступа.
97. Обеспечение безопасности информации при подключении вычислительных средств к международным информационным системам.
98. Требования руководящих документов по обеспечению информационной безопасности при использовании информационно-телекоммуникационных сетей международного информационного обмена.
99. Особенности обеспечения безопасности информации при подключении автоматизированных систем к международным информационным системам, в том числе Интернет.

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

(подпись)

**4.2. Процедуры оценивания знаний, умений, навыков, формы и организация текущего контроля успеваемости и промежуточной аттестации обучающихся.**

Текущий контроль успеваемости и промежуточная аттестация студентов в университете ведется в соответствии с «Положением о текущем контроле успеваемости и промежуточной аттестации студентов МГТУ им. Н.Э. Баумана».

**Текущий контроль успеваемости**

Дисциплина в семестре делится на два модуля учебной дисциплины. Каждый модуль учебной дисциплины включает в себя изучение законченного раздела, части дисциплины.

Основными видами контроля знаний, умений и навыков в течение каждого модуля учебной дисциплины являются домашнее задание, рубежные контроли, посещение лекций, работа на семинарах.

Текущий контроль по модулю учебной дисциплины осуществляется по графику учебного процесса. Сроки контрольных мероприятий (КМ) и сроки подведения итогов по модулям учебной дисциплины отображаются в рабочих учебных планах на семестр (отрезках). Студент должен выполнить все контрольные мероприятия, предусмотренные в модуле учебной дисциплины к указанному сроку, после чего преподаватель проставляет балльные оценки, набранные студентом по результатам текущего контроля модуля учебной дисциплины в ЭУ.

Контрольное мероприятие считается выполненным, если за него студент получил оценку в баллах, не ниже минимальной оценки, установленной программой дисциплины по данному мероприятию.

Студенты, не сдавшие контрольное мероприятие в установленный срок, продолжают работать над ним в соответствие с порядком, принятым кафедрой.

**Промежуточная аттестация**

Формой промежуточной аттестации является зачет.

**Зачет**

В рамках рейтинговой системы контроля успеваемости студентов, зачет по дисциплине формируется набором в течение семестра предусмотренной в программе дисциплины суммы баллов, при выполнении им всех контрольных мероприятий. При этом экзаменационная сессия может использоваться для сдачи задолженностей по контрольным мероприятиям или для повышения семестровой составляющей оценки по учебной дисциплине.

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

**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 |

При наборе студентом по результатам текущего контроля по дисциплине 60 и более баллов, при обязательной сдаче им всех предусмотренных в программе контрольных мероприятий, ему выставляется «зачет».

Рейтинг студента по дисциплине за семестр определяется как сумма баллов, полученных им за все модули учебной дисциплины, и баллов за промежуточную аттестацию. Максимальное количество баллов за дисциплину в семестре устанавливается равным 100.

ЛИСТ ВНЕСЕННЫХ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ

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