





# 1 Цели и задачи освоении дисциплины

Целями освоения дисциплины (модуля) «Защита информации» является изучение основных понятий, связанных с угрозами безопасности, основ криптографии, формирование представлений о математических основах электронной цифровой подписи и аутентификации и границ их юридического применения. Знать существующие технологии по защите информации в различных информационных системах.

Для достижения поставленной цели в курсе «Защита информации» решаются задачи:

* изучение основной терминологии, связанной с защитой информации;
* изучение угроз безопасности информации, как на локальном компьютере, так и в сети;
* знакомство с руководящими документами США, Евросоюза и РФ по критериям надёжности компьютерных систем различного уровня.
* изучение основ криптографии и криптоанализа, инструментальных средств и известных алгоритмов шифрования информации;
* знакомство с аппаратными устройствами идентификации человека, с политикой безопасности предприятия, степенями секретности информации и методами её защиты.
* реализацию методов противодействия угрозам безопасности в сетях и получение навыков по настройке сетевых фильтров, сканеров безопасности и специализированного программного обеспечения для его эффективной работы.

# 2 Место дисциплины в структуре образовательной программы подготовки бакалавра

Дисциплина Б1.В.08 «Защита информации» входит в вариативную часть блока 1 образовательной программы.

Изучение дисциплины базируется на следующих курсах: дискретная математика, информатика, теория и практика обработки информации, математика, теория алгоритмов, программирование.

Дисциплина является предшествующей для изучения дисциплин нейрокомпьютерные системы и научно-исследовательской работы студентов.

# 3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Защиты информации» обучающийся должен обладать следующими компетенциями:

| Структурный  элемент  компетенции | Планируемые результаты обучения |
| --- | --- |
| **ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.** | |
| Знать | основные понятия, связанные с защитой информации |
| Уметь | применять готовые алгоритмы, используя современные программно-аппаратные средства защиты информации |
| Владеть | навыками работы по защите программного обеспечения общего назначения, методами защиты информации |
| **ПК-3 способность обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности.** | |
| Знать | основные методы защиты и средства информационной безопасности |
| Уметь | уметь применять алгоритмы и средства защиты персональных и корпоративных данных |
| Владеть | навыками работы со специальными программными средствами |
| **ПК-2 способностью разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования.** | |
| Знать | основные алгоритмы криптографической защиты информации |
| Уметь | разрабатывать алгоритмы защиты персональных и корпоративных данных |
| Владеть | навыками работы со специальными программными и аппаратными средствами,  навыками решения задач профессиональной деятельности с учетом основных требований информационной безопасности. |

# **4 Структура и содержание дисциплины (модуля)**

Общая трудоемкость дисциплины составляет 4 зачетных единиц 144 акад. часов, в том числе:

* контактная работа – 73,9 акад. часов:

аудиторная – 72 акад. часов;

внеаудиторная – 1,9 акад. часов

* самостоятельная работа – 70,1 акад. часов.

| Раздел/ тема  дисциплины | Семестр | Аудиторная  контактная работа  (в акад. часах) | | | Самостоятельная работа (в акад. часах) | Вид самостоятельной  работы | Форма текущего контроля успеваемости и  промежуточной аттестации | Код и структурный  элемент  компетенции |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| лекции | лаборат.  занятия | практич. занятия |
| Раздел 1. Основные понятия и стандарты информационной безопасности. Проблема потери электронной информации. | **7** |  | | | | | | |
| 1.1 Основные понятия угрозы безопасности. Пути утечки информации. Опасности в Интернет. |  | 2 |  |  | 4 | 1. Поиск дополнительной информации по заданной теме.  2. Самостоятельное изучение учебной литературы.  3. Работа с электронными библиотеками.  4. Подготовка к выполнению л.р.№1 | Устный опрос | ОПК-5–зув,  ПК-2-зув,  ПК-3 -зув |
| 1.2 Системная классификация угроз безопасности. Стандарты информационной безопасности. «Критерии оценки надёжных компьютерных систем» Министерства обороны США и Гармонизированные критерии Евросоюза. Требования и классы безопасности компьютерных систем. Критерии соответствия. |  | 2 |  |  | 4 | 1. Работа с электронными библиотеками.  2. Самостоятельное изучение учебной литературы. | Устный опрос | ОПК-5–зув,  ПК-2-зув,  ПК-3 -зув |
| 1.3 Компьютерные вирусы, их классификации по различным признакам и особенности алгоритмов работы вирусов. Классификация антивирусных программ. |  | 4 |  |  | 5,1 | 1. Работа с электронными библиотеками.  2. Самостоятельное изучение учебной литературы.  3. Подготовка к выполнению л.р.№2. | Устный опрос | ОПК-5–зув,  ПК-2-зув,  ПК-3 -зув |
| 1.4 Злоумышленники. Компьютерные преступления. УК РФ. |  | 2 | - |  | 4 | 1. Работа с электронными библиотеками.  2. Самостоятельное изучение учебной литературы. | Устный опрос | ОПК-5–зув,  ПК-2-зув,  ПК-3 -зув |
| **Итого по разделу** |  | **10** |  |  | **17,1** |  |  |  |
| Раздел 2. Криптографические методы защиты информации. | **7** |  | | | | | | |
| 2.1 Криптографические методы защиты информации. История криптографии. Основные понятия. Терминология. Алгоритмы и ключи, классификация криптографических алгоритмов. |  | 2 | 12 |  | 5 | 1. Подготовка и выполнение л.р.№1 и №2.  2. Самостоятельное изучение учебной литературы | Коллоквиум по л.р.№1, 2 | ОПК-5–зув,  ПК-2-зув,  ПК-3 -зув |
| 2.2 Понятие симметричного алгоритма. Виды. Потоковые шифры (скремблеры), блочные шифры. |  | 4 | 6 |  | 6 | 1. Подготовка к выполнению л.р.№3.  2. Поиск дополнительной информации по заданной теме.  3. Самостоятельное изучение учебной литературы. | Коллоквиум по л.р.№3. | ОПК-5–зув,  ПК-2-зув,  ПК-3 -зув |
| 2.3 Асимметричные алгоритмы. Области применения. Криптостойкость алгоритмов. Сравнение симметричных и асимметричных алгоритмов. |  | 4 | 6 |  | 6 | 1. Подготовка к выполнению л.р.№4.  2. Самостоятельное изучение учебной литературы. | Коллоквиум по л.р.№4 | ОПК-5–зув,  ПК-2-зув,  ПК-3 -зув |
| 2.4. Однонаправленные хэш-функции. Математические основы электронной цифровой подписи, создание и использование. Юридические основы использования ЭЦП. Методы криптоанализа. Электронная цифровая подпись. Стеганография. |  | 6 | 6 |  | 10 | 1. Подготовка к выполнению л.р. №5. | Коллоквиум по л.р.№5 | ОПК-5–зув,  ПК-2-зув,  ПК-3 -зув |
| **Итого по разделу** |  | **16** | **30** |  | **27** |  |  |  |
| Раздел 3. Технологии защиты доступа к информационным системам. Угрозы защиты информации в сетях и противодействие им. | 7 |  | | | | | | |
| 3.1 2 Средства анализа защищённости компьютерных сетей. Сетевые фильтры. Определение, возможности брандмауэра, компоненты брандмауэра. Правила фильтрации пакетов. Шлюзы приложений, канальные шлюзы, шлюзы с сохранением состояния.  Недостатки брандмауэров. Системы выявления вторжений в реальном времени. |  | 5 |  |  | 9 | 2. Самостоятельное изучение учебной литературы. | Устный опрос | ОПК-5–зув,  ПК-2-зув,  ПК-3 -зув |
| 3.2 Технологии защиты информации. «Имущественная» идентификация. Биометрические технологии. Программное и аппаратное обеспечение |  | 5 | 6 |  | 8 | 1. Подготовка к выполнению л.р.№6. | Коллоквиум по л.р.№6. | ОПК-5–зув,  ПК-2-зув,  ПК-3 -зув |
| **Итого по разделу** |  | **10** | **6** |  | **17** |  |  |  |
| **Итого за семестр** |  | **36** | **36** |  | **70,1** |  | Зачет |  |
| **Итого по дисциплине** |  | **36** | **36** |  | **70,1** |  |  |  |

# 5 Образовательные и информационные технологии

1. **Традиционные образовательные технологии,** ориентированные на организацию образовательного процесса и предполагающую прямую трансляцию знаний от преподавателя к студенту.

**Формы учебных занятий с использованием традиционных технологий:**

Информационная лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя).

Практическое занятие, посвященное освоению конкретных умений и навыков по предложенному алгоритму.

2. **Технологии проблемного обучения** – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности студентов.

**Формы учебных занятий с использованием технологий проблемного обучения:**

Практическое занятие в форме практикума – организация учебной работы, направленная на решение комплексной учебно-познавательной задачи, требующей от студента применения как научно-теоретических знаний, так и практических навыков.

3. **Интерактивные технологии** – организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе личностно значимого для них образовательного результата.

**Формы учебных занятий с использованием специализированных интерактивных технологий:**

Лекция «обратной связи» – лекция–провокация (изложение материала с заранее запланированными ошибками), лекция-беседа, лекция-дискуссия, лекция-пресс-конференция.

Семинар-дискуссия – коллективное обсуждение вопросов, проблемы, выявление мнений в группе по теме научного исследования студентов.

4. **Информационно-коммуникационные образовательные технологии** – организация образовательного процесса, основанная на применении программных сред и технических средств работы с информацией по теме научно-исследовательской работы студентов.

**Формы учебных занятий с использованием информационно-коммуникационных технологий**:

Лекция-визуализация – изложение содержания сопровождается презентацией и видеоматериалов по курсам «Защита информации» и «Средства и методы защиты компьютерной информации».

# 6 Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Защита информации» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа студентов предполагает решение задач при выполнении коллоквиума по теме лабораторной работы.

***Примерные вопросы на аудиторных коллоквиумах***

*Коллоквиум № 1.* Нахождение простых чисел с помощью решета Эратосфена. Детерминированные тесты на простоту.

|  |
| --- |
| 1. Какое число называют простым? Алгоритм детерминированного теста на простоту. |
| 2. Приведите примеры простых и взаимно простых чисел. Основная теорема алгебры. |
| 3. Чем различаются детерминированные и вероятностные тесты на простоту? Их применение. |
| 4. Алгоритм определения простоты числа методом пробного деления. |
| 5. Доказательство Эвклидов теоремы о бесконечности количества простых чисел. |

*Коллоквиум № 2.* Нахождение простых чисел с помощью вероятностных тестов Лемана и Рабина-Миллера.

|  |
| --- |
| 1. Алгоритм определения простоты числа методом Лемана. Чем он принципиально отличается от метода пробного деления? |
| 2. Алгоритм определения простоты числа методом Рабина-Миллера. |
| 3. Как алгоритмы Лемана и Рабина-Миллера используют малую теорему Ферма? |
| 4. Какие числа называют числами Кармайкла? |
| 5. Использование в компьютерной криптографии арифметики вычетов. |

*Коллоквиум № 3.* Шифры замены и их взлом статистическим методом

|  |
| --- |
| 1. Что такое алфавит и мощность алфавита, кодирование информации, код и длина кода? |
| 2. Чем занимается криптография и каковы ее основные функции? Новые направления современной криптографии: ЭЦП, стеганография. |
| 3. Какие шифры называют шифрами замены и перестановки? Приведите примеры шифров замены и перестановки. |
| 4. Алгоритм шифрования и дешифрования кодом Цезаря и Виженера.. |
| 5. В чем основная идея статистического алгоритма поиска ключа при расшифровке сообщения зашифрованного с использованием шифра замены? |

*Коллоквиум № 4.* Тестирование генератора псевдослучайной последовательности и его использование для алгоритма гаммирования данных

|  |
| --- |
| 1. Чем последовательность псевдослучайных чисел отличается от последовательности случайных чисел? |
| 2. Какие существуют алгоритмы получения псевдослучайной последовательности и можно ли использовать функцию генератора случайных чисел для получения криптографических ключей? |
| 3. Что такое гамма, ее период и что понимается под числом, порождающим последовательность? |
| 4. Что такое скремблер, как он работает, назначение генератора ПCП при работе скремблера. |
| 5.Применение ПСП в потоковых и блочных шифрах и почему в скремблере используется операция исключающего ИЛИ (XOR), а не операции И (AND), ИЛИ (OR)? |

*Коллоквиум № 5.* Симметричный и асимметричный алгоритмы шифрования. Электронная цифровая подпись

|  |
| --- |
| 1. Чем занимается криптография и каковы ее основные функции? Что такое криптографический ключ, его длина и какие виды ключей существуют? |
| 2. Каким образом генерируется криптографический ключ? Что такое асимметричные алгоритмы шифрования, их основные преимущества и недостатки. Какие вы знаете асимметричные алгоритмы шифрования? На основе каких необратимых преобразований базируется алгоритм RSA? На основе каких необратимых преобразований базируется алгоритм Эль-Гамаля? |
| 3. Что такое симметричные алгоритмы шифрования, их основные преимущества и недостатки. Какие вы знаете симметричные алгоритмы шифрования? |
| 4. Как работают блочные шифры? Длина блока. Что такое сеть Фейстеля и ее ветви? |
| 5. Каков юридический статус электронной цифровой подписи в РФ? Где используется ЭЦП и как практически реализуется механизм ее использования на территории РФ? Алгоритм создания электронной цифровой подписи на основе асимметричного алгоритма шифрования. Какими основными свойствами обладает электронная цифровая подпись и что ее отличает от обычной подписи? |

*Коллоквиум № 6*. Использование одноразовых паролей. Применение необратимой функции логарифмирования в конечном поле.

|  |
| --- |
| 1. Назовите основные требования к паролям для входа в информационную систему. |
| 2. Алгоритм одноразового блокнота. Его преимущества и недостатки. Технология использования одноразовых паролей для доступа к ИС. |
| 3. Какую функцию называют необратимой? Ее основные свойства. |
| 4. Объяснить алгоритм генерации одноразовых паролей по схеме Лампорта. |
| 5. Аутентификация пользователя и использованием одноразовых паролей по схеме Лампорта. |

# 7 Оценочные средства для проведения промежуточной аттестации

| Структурный элемент  компетенции | Планируемые результаты обучения | Оценочные средства |
| --- | --- | --- |
| **ОПК-5 Обладает способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.** | | |
| **Знать** | основные понятия, связанные с защитой информации | **Перечень теоретических вопросов**   1. Причины возникновения угроз безопасности информации. 2. Проблемы информационной безопасности. Причина кризиса информационной безопасности. 3. Проблема потери электронной информации. 4. Носители информации. Сигналы, знаки, символы. Информационные процессы и их взаимосвязь. Роль защиты данных в информационных процессах. 5. Основные пути утечки информации. Проблема потери электронных данных. 6. Классификация вирусов и других вредоносных программ по степени опасности, по заражаемым объектам, по методу заражения, по методу скрытия своего наличия в системе, по среде создания. 7. Особенности алгоритмов работы вирусов и основные методы определения их в системе. 8. Антивирусные программы, их классификация, источники компьютерных вирусов. 9. Задачи безопасности и существующие угрозы. Злоумышленники и их классификация. 10. Компьютерные преступления. Преступления в сфере компьютерной информации в УК РФ. 11. Критерии оценки надежных компьютерных систем. «Оранжевая книга». Классы безопасности компьютерных систем. 12. Гармонизированные критерии безопасности информационных технологий европейских стран. |
| **Уметь** | применять готовые алгоритмы, используя современные программно-аппаратные средства защиты информации | ***Примерные практические задания***  1.Выбрать правильный вариант ответа:  Конфиденциальность информации гарантирует:  +: доступность информации кругу лиц, для кого она предназначена  -: защищенность информации от потери  -: защищенность информации от фальсификации  -: доступность информации только автору  2.Основополагающим документом по информационной безопасности в РФ является?  +: Конституция РФ  -: Закон об информационной безопасности  -: Уголовный кодекс  3.Выбрать правильные варианты ответов:  Основными аспектами защиты является обеспечение ...?  -: контроля за работой пользователей  +: целостности информации  +: доступности информации  +: конфиденциальности информации  -: комплексности информации  4.Выбрать правильный вариант ответа:  Система безопасности - это ...?  +: организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно-важный интересов личности, предприятия, государства от внутренних и внешних угрозах  -: защищенность информации от случайных или преднамеренных воздействий искусственного или естественного характера, способных нанести неприемлемый ущерб субъектам информационных отношений  -: специфическое явление, представляющее собой сложную систему неразрывно взаимосвязанных и взаимозависимых процессов, каждый из которых в свою очередь имеет множество различных взаимообуславливающих друг друга сторон, свойств, тенденций  5.Какие цели могут преследовать злоумышленники (конкуренты, преступники, административно-управленческие органы)?  +: Ознакомление (получение) информации  +: Искажение (модификация) информации  +: Разрушение (уничтожение) информации  -: Обеспечение конфиденциальности, целостности, доступности информации |
| **Владеть** | навыками работы по защите программного обеспечения общего назначения, методами защиты информации | ***Задания на решение задач из области защиты информации***  Составить программу по разграничению доступа трех пользователей, входящих в систему по своему паролю.   1. может просматривать и редактировать данные для 1 предприятия; 2. может только просматривать данные для 2 предприятия (доступ к данным 1 предприятия запрещен); 3. администратор, имеет доступ ко всем данным и может менять пароль всем трем пользователям. |
| **ПК-3 Обладает способность обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности.** | | |
| **Знать** | основные методы защиты и средства информационной безопасности | **Перечень теоретических вопросов**   1. Криптографические методы защиты информации. История криптографии. Задачи криптографии и криптоанализа. Основные понятия (шифр, ключ, шифрование, дешифрование, криптостойкость). 2. Принципы кодирования информации. Алфавит и длина кода. Цифровая и дискретная информация. 3. Потоковые шифры. Аппаратные и программные скремблеры. 4. Алгоритм шифрования кодом Цезаря. Алгоритм взлома кода Цезаря и других алгоритмов замены. 5. Алгоритм шифрования кодом Виженера. Алгоритм взлома кода Виженера при известной длине ключа. 6. Алгоритмы генерации псевдослучайных чисел. Алгоритмы аддитивного конгруэнтного генератора псевдослучайной последовательности. Генераторы случайных чисел и их использование. 7. Потоковые шифры. Скремблеры. Алгоритм шифрования в режиме гаммирования, схема гаммирования с обратной связью. 8. Принципы построения симметричных блочных шифров (рассеивание и перемешивание). Сеть Фейстеля и ее ветви. 9. Схема абсолютно стойкого шифра, ее основные проблемы. 10. Основные характеристики и применение систем с секретным ключом DES, FEAL, IDEA, ГОСТ 28147-89, RC5. 11. Системы криптографической защиты данных с открытым ключом, их достоинства и недостатки. 12. Алгоритм RSA. 13. Алгоритм Эль-Гамаля. 14. Сравнение симметричных и несимметричных алгоритмов шифрования. Достоинства и недостатки асимметричных алгоритмов. Цифровой конверт. 15. Сертификаты открытых ключей. Назначение удостоверяющих центров (бюро сертификации). |
| **Уметь** | уметь применять алгоритмы и средства защиты персональных и корпоративных данных | ***Примерные практические задания***   1. Характерная черта алгоритма Эль-Гамаля состоит в :   **+ протоколе передачи подписанного сообщения, позволяющего подтверждать подлинность отправителя**  –в точной своевременной передаче сообщения  –алгоритм не имеет особенностей и идентичен RSA   1. Аутентификацией называют:   -процесс регистрации в системе  -способ защиты системы  + **процесс распознавания и проверки подлинности заявлений о себе пользователей и процессов**   1. Условие, при котором в распоряжении аналитика находиться возможность получить результат зашифровки для произвольно выбранного им зашифрованного сообщения размера n используется в анализе:   **+на основе произвольно выбранного шифротекста**  **–на основе произвольно выбранного открытого текста**  –на основе только шифротекста   1. В каком случае построение цифровой подписи не требует наличия в системе третьего лица – арбитра, занимающегося аутентификацией?   **+при шифровании с помощью асимметричного алгоритма**  -при шифровании с помощью симметричного алгоритма  -арбитр необходим всегда.   1. Шифрование-это:   –процесс создания алгоритмов шифрования  –процесс сжатия информации  **+процесс криптографического преобразования информации к виду, когда ее смысл полностью теряется.** |
| **Владеть** | навыками работы со специальными программными средствами | ***Задания на решения задач из области защиты информации.***   1. Посредством датчика псевдослучайной последовательности (ПСП) зашифруйте произвольную строку (посимвольное шифрование), причем параметры генератора ПСП являются секретным шифром. Покажите, что, используя их можно правильно расшифровать эту строку. |
| **ПК-2 Обладает способностью разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования.** | | |
| **Знать** | основные аппаратно-программные комплексы защиты информации | **Перечень теоретических вопросов**   1. Функция хеширования и ее свойства. Однонаправленные хэш-функции. 2. Электронная цифровая подпись с использованием симметричных алгоритмов. 3. Электронная цифровая подпись с использованием асимметричных алгоритмов. Классическая схема. 4. Сжатие данных без потерь. Алгоритмы Хаффмана и Лемпеля-Зива. 5. Стеганография как способ сокрытия секретных данных. Понятия: контейнер, стеганографический канал, стегоключ. 6. Ограничение стеганографических методов. Принципы построения тайных каналов. Защита музыки, видеофильмов посредством скрытых «водяных знаков». 7. Аутентификация пользователей с применением паролей. Почему взломщикам удается проникать в систему защищенную паролями? 8. Совершенствование безопасности паролей, схема аутентификации «отклик-отзыв». 9. Необратимые функции. Одноразовые пароли Лампорта. 10. Аутентификация пользователей с использованием физического объекта (пластиковые, магнитные, смарт-карты). 11. Аутентификация пользователей с использованием биометрических данных. 12. Угрозы защиты информации в сетях и противодействие им. Сетевые фильтры. 13. Организационные контрмеры и ловушки для взломщиков. |
| **Уметь** | разрабатывать алгоритмы защиты персональных и корпоративных данных | ***Примерные практические задания***   1. Найти все простые числа до заданного N. 2. Показать работу криптосистемы RSA шифрования-дешифрования для небольших чисел. 3. Показать работу криптосистемы Эль-Гамаля (ElGamal) для небольших чисел. 4. Написать алгоритм циклического избыточного кода CRC-32 (Cyclic Redundancy Check 32). 5. Написать алгоритм Диффи-Хеллмана для получения общего секретного ключа. |
| **Владеть** | навыками работы со специальными программными и аппаратными средствами,  навыками решения задач профессиональной деятельности с учетом основных требований информационной безопасности. | ***Задания на решения задач из области защиты информации***  Используя программы PGP 6‑10 под Windows решить следующую задачу. Подгруппа А пишет письмо и посылает его подгруппе Б, подписывая предварительно электронной подписью (ЭЦП) с использованием своего секретного ключа. Рассмотреть случаи, когда текст письма шифруется или не шифруется (остается открытым для прочтения). Каждая подгруппа должна проверить "подлинность" и авторство полученного письма, используя ЭЦП при его неизменном содержании и при корректировке "злоумышленником". |

**б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:**

Промежуточная аттестация по дисциплине «Защита информации» включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме зачета.

Зачет по дисциплине проводится в устной форме по экзаменационным билетам, каждый из которых включает 2 теоретических вопроса.

**Показатели и критерии оценивания зачета:**

– на оценку **«зачтено»** – обучающийся демонстрирует как минимум средний уровень сформированности компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

– на оценку **«не зачтено»** – обучающийся демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

# 8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

**а) Основная литература:**

1. Мартынов А.И. **Методы и задачи криптографической защиты информации**.– Учебн. пособ. Ульяновск: УлГТУ, 2007.– 92 с. <http://window.edu.ru/resource/904/58904/files/10.pdf>

**б) Дополнительная литература:**

1. **Ячиков, И. М.** Основы защиты компьютерной информации: учебное пособие / И. М. Ячиков, Ю. В. Кочержинская, М. М. Гладышева. - Магнитогорск : МГТУ, 2010. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: <https://magtu.informsystema.ru/uploader/fileUpload?name=1003.pdf&show=dcatalogues/1/1119188/1003.pdf&view=true> (дата обращения: 23.10.2020). - Макрообъект. - Текст: электронный. - Сведения доступны также на CD-ROM.
2. **Ячиков, И. М.** Практикум по дисциплине "Защита информации": практикум / И. М. Ячиков, Ю. В. Кочержинская, А. В. Леднов; МГТУ. - Магнитогорск: МГТУ, 2016. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: <https://magtu.informsystema.ru/uploader/fileUpload?name=2296.pdf&show=dcatalogues/1/1129906/2296.pdf&view=true> (дата обращения: 23.10.2020). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.

**в) Методические указания:**

1.Программирование алгоритмов криптографических методов защиты информации [Текст]. – Магнитогорск : МГТУ, 2005. – 26 с.

2. Защита информации: методические указания к лабораторным работам №1‑№6 по дисциплине «Защита информации» для студентов направления 230100.62 «Информатика и вычислительная техника». Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И.Носова, 2015. 20 с.

**г)** **Программное обеспечение** и **Интернет-ресурсы:**

*Программное обеспечение*: лицензионное программное обеспечение: операционная система; офисные программы; математические пакет, статистические пакеты, установленные на каждом персональном компьютере вычислительного центра ФГБОУ ВПО «МГТУ».

Перечень лицензионного программного обеспечения по ссылке:

<http://sps.vuz.magtu.ru/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2FShared%20Documents%2F%D0%9F%D0%BE%D0%B4%D0%B3%D0%BE%D1%82%D0%BE%D0%B2%D0%BA%D0%B0%20%D0%BA%20%D0%B0%D0%BA%D0%BA%D1%80%D0%B5%D0%B4%D0%B8%D1%82%D0%B0%D1%86%D0%B8%D0%B8%202020%2F%D0%A1%D0%B0%D0%BC%D0%BE%D0%BE%D0%B1%D1%81%D0%BB%D0%B5%D0%B4%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5%202019%D0%B3%2F%D0%9B%D0%B8%D1%86%D0%B5%D0%BD%D0%B7%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B5%20%D0%9F%D0%9E&InitialTabId=Ribbon.Document&VisibilityContext=WSSTabPersistence>

# Официальные сайты промышленных предприятий и организаций: <http://www.mmk.ru>, <http://www.creditural.ru>, <http://www.magtu.ru>, <http://www.gks.ru> и т.п.; разра­ботчиков программных продуктов: <http://www.statsoft.ru>, <http://www.microsoft.com>, <http://www.ptc.com> и т.п; сайты лабораторий компьютерной графики <http://graphics.cs.msu.ru> , <http://cgm.graphicon.ru>.

# **9 Материально-техническое обеспечение дисциплины (модуля)**

Материально-техническое обеспечение дисциплины включает:

| Тип и название аудитории | Оснащение аудитории |
| --- | --- |
| Лекционная аудитория | Мультимедийные средства хранения, передачи и представления информации |
| Компьютерный класс | Персональные компьютеры с пакетом Office, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета |
| Аудитории для самостоятельной работы: компьютерные классы; читальные залы библиотеки | Все классы УИТ и АСУ с персональными компьютерами, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета |
| Аудиторий для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации | Ауд. 282 и классы УИТ и АСУ |
| Помещения для самостоятельной работы обучающихся, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и наличием доступа в электронную информационно-образовательную среду организации | Классы УИТ и АСУ |
| Помещения для хранения и профилактического обслуживания учебного оборудования | Центр информационных технологий – ауд. 379 |