**Тамбовское государственное автономное профессиональное**

**образовательное учреждение «Тамбовский бизнес-колледж»**

**Предметно-цикловая комиссия информационных технологий**

Утверждаю:

Директор ТОГАПОУ

«Тамбовский бизнес-колледж»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Н.В. Астахова

Пр. 104/1 от 28.08.2017

**Фонд оценочных средств**

текущего контроля и промежуточной аттестации по учебной дисциплине

**ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ**

среднее профессиональное образование

(программа подготовки специалистов среднего звена)

10.02.05 «Обеспечение информационной безопасности автоматизированных

систем»

Тамбов 2017

***Лист согласования программы***

**Фонд оценочных средств**

**ПМ.02 «Защита информации в автоматизированных системах программным и программно-аппаратными средствами»)**

ПМ.02 «Защита информации в автоматизированных системах программным и и программно-аппаратными средствами» относится к циклу профессиональных модулей основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, квалификация – техник по защите информации.

Программа ПМ.02 «Защита информации в автоматизированных системах программным и программно-аппаратными средствами» может быть использована для изучения дисциплин специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, изучаемых в учреждениях среднего профессионального образования при подготовке квалифицированных специалистов среднего звена.

**Организация разработчик:**

Тамбовское областное государственное автономное профессиональное образовательное учреждение «Тамбовский бизнес-колледж»

**Разработчики:**

Трефилов П.А. преподаватель ТОГАПОУ «Тамбовский бизнес-колледж».

Программа рассмотрена и рекомендована на заседании ПЦК информационных технологий.

Протокол №1 от «28» августа 2017 г.

СОГЛАСОВАНО:

АНО «Академический правовой центр»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ О.В. Штах

«28» августа 2017 г.

**СОДЕРЖАНИЕ**

|  |  |
| --- | --- |
| **1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** |  |
| **2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** |  |
| **3.  УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** |  |
| **4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** |  |

**1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ**

**ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ**

**1.1. Цель и планируемые результаты освоения профессионального модуля**

1.1.1.В результате изучения профессионального модуля студент должен освоить вид деятельности *Защита информации в автоматизированных системах программными и программно-аппаратными средствами* и соответствующие ему профессиональные компетенции:

|  |  |
| --- | --- |
| Код | Наименование видов деятельности и профессиональных компетенций |
| **ВД 2** | **Защита информации в автоматизированных системах программными и программно-аппаратными средствами** |
| ПК 2.1. | Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. |
| ПК 2.2. | Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. |
| ПК 2.3. | Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. |
| ПК 2.4. | Осуществлять обработку, хранение и передачу информации ограниченного доступа. |
| ПК 2.5. | Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. |
| ПК 2.6. | Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. |

* + 1. **Общие компетенции**

|  |  |
| --- | --- |
| Код | Наименование видов деятельности и профессиональных компетенций |
| ОК 1. | Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. |
| ОК 2. | Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. |
| ОК 3. | Планировать и реализовывать собственное профессиональное и личностное развитие. |
| ОК 4. | Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. |
| ОК 5. | Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста. |
| ОК 6. | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей. |
| ОК 7. | Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. |
| ОК 8. | Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности. |
| ОК 9. | Использовать информационные технологии в профессиональной деятельности. |
| ОК 10. | Пользоваться профессиональной документацией на государственном и иностранном языках. |

1.1.3. В результате освоения профессионального модуля студент должен:

|  |  |
| --- | --- |
| **Иметь практический опыт** | * установки, настройки программных средств защиты информации в автоматизированной системе; * обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; * тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; * решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; * применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных; * учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; * работы с подсистемами регистрации событий; * выявления событий и инцидентов безопасности в автоматизированной системе. |
| **уметь** | * устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; * устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; * диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; * применять программные и программно-аппаратные средства для защиты информации в базах данных; * проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; * применять математический аппарат для выполнения криптографических преобразований; * использовать типовые программные криптографические средства, в том числе электронную подпись; * применять средства гарантированного уничтожения информации; * устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; * осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак |
| **знать** | * особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; * методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; * типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; * основные понятия криптографии и типовых криптографических методов и средств защиты информации; * особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; * типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа. |

**Назначение фонда оценочных средств**

Фонд оценочных средств (ФОС) составляется в соответствии с требованиями ФГОС ВО для проведения промежуточной аттестации обучающихся по дисциплине на соответствие их учебных достижений поэтапным требованиям соответствующей основной профессиональной образовательной программы (ОПОП). ФОС является составной частью рабочей программы дисциплины.

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине ключает в себя: перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП; описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания; типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения ОПОП; методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Фонд оценочных средств сформирован на основе ключевых принципов оценивания:

* валидности: объекты оценки должны соответствовать поставленным целям обучения;
* надежности: использование единообразных стандартов и критериев для оценивания достижений;
* объективности: разные студенты должны иметь равные возможности добиться успеха.

Основными параметрами и свойствами ФОС являются:

* предметная направленность (соответствие предмету изучения конкретной учебной дисциплины);
* содержание (состав и взаимосвязь структурных единиц, образующих содержание теоретической и практической составляющих учебной дисциплины);
* объем (количественный состав оценочных средств, входящих в ФОС);
* качество оценочных средств и ФОС в целом, обеспечивающее получение объективных и достоверных результатов при проведении контроля с различными целями.

## **ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НАОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ , НАВЫКОВ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ОСОВЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

**Тема: Предмет и задачи программно-аппаратной защиты информации.**

**Задание 1. Перечень вопросов по теме для устного обсуждения:**

1. Предмет и задачи программно-аппаратной защиты информации
2. Уязвимость компьютерных систем
3. Политика безопасности в компьютерных системах. Оценка защищенности.
4. Механизмы защиты

**Задание 2. Лабораторные работы**

1. Программные средства гарантированного уничтожения информации

**Тема: Контроль доступа к файлам**

**Задание 1. Перечень вопросов по теме для устного обсуждения:**

1. Защита информации в КС от несанкционированного доступа
2. Система разграничения доступа к информации в КС
3. Концепция построения систем разграничения доступа
4. Организация доступа к ресурсам КС
5. Обеспечение целостности и доступности информации в КС

**Задание 2. Лабораторные работы**

1. Система контроля разграничения доступа «РЕВИЗОР ХР»

**Тема: Программно-аппаратные средства шифрования**

**Задание 1. Перечень вопросов по теме для устного обсуждения:**

1. Основные элементы и средства защиты от несанкционированного доступа
2. Системы защиты информации от несанкционированного доступа
3. Комплекс КРИПТОН-ЗАМОК для ограничения доступа к компьютеру
4. Система защиты данных Crypton Sigma

**Задание 2. Лабораторные работы**

1. Применение криптографических средств защиты информации

**Тема: Методы и средства ограничения доступа**

**Задание 1. Перечень вопросов по теме для устного обсуждения:**

1. Защита информации в ПЭВМ
2. Защита информации, обрабатываемой ПЭВМ и ЛВС, от утечки по сети электропитания
3. Виды мероприятий по защите информации
4. Современные системы защиты ПЭВМ от несанкционированного доступа к информации

**Задание 2. Лабораторные работы**

1. СЗИ DallosLock и ПАК «Соболь»

**Тема: Защита программ**

**Задание 1. Перечень вопросов по теме для устного обсуждения:**

1. Методы, затрудняющие считывание скопированной информации
2. Методы, препятствующие использованию скопированной информации
3. Основные функции средств защиты от копирования
4. Основные методы защиты от копирования
5. Методы противодействия динамическим способам снятия защиты программ от копирования

**Задание 2. Лабораторные работы**

1. Средства контроля целостности программ «ФИКС»

**Тема: Защита от разрушающих программных воздействий (РПВ)**

**Задание 1. Перечень вопросов по теме для устного обсуждения:**

1. Классификация средств исследования программ
2. Методы защиты программ от исследования
3. Общая характеристика и классификация компьютерных вирусов
4. Общая характеристика средств нейтрализации компьютерных вирусов
5. Классификация методов защиты от компьютерных вирусов

**Задание 2. Лабораторные работы**

1. Антивирусные средства защиты информации

**Тема: Средства предотвращения утечки информации по техническим каналам**

**Задание 1. Перечень вопросов по теме для устного обсуждения:**

1. Классификация технических каналов утечки информации
2. Защита информации от утечки по ПЭМИН

**Задание 2. Лабораторные работы**

**Материалы тестирования по дисциплине**

1. **Под угрозой безопасности информации в компьютерной системе (КС) понимают:** 
   1. возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.
   2. событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.
   3. действие, предпринимаемое нарушителем, которое заключается в

поиске и использовании той или иной уязвимости.

1. **Уязвимость информации — это:**
2. возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.
3. событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.
4. это действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

**3. Атакой на КС называют:**

1. возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.
2. событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.
3. действие, предпринимаемое нарушителем, которое заключается в

поиске и использовании той или иной уязвимости.

**4. Искусственные угрозы исходя из их мотивов разделяются на:**

a ) непреднамеренные и преднамеренные

1. косвенные и непосредственные
2. несанкционированные и санкционированные

1. **К непреднамеренным угрозам относятся:** 
   1. ошибки в разработке программных средств КС
   2. несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями.
   3. угроза нарушения конфиденциальности, т.е. утечки информации ограниченного доступа, хранящейся в КС или передаваемой от одной КС к другой;

1. **К умышленным угрозам относятся:** 
   1. несанкционированные действия обслуживающего персонала КС (например, ослабление политики безопасности администратором, отвечающим за безопасность КС);
   2. воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости) и др.
   3. ошибки пользователей КС;

1. **Косвенными каналами утечки называют:** 
   1. каналы, не связанные с физическим доступом к элементам КС
   2. каналы, связанные с физическим доступом к элементам КС
   3. каналы, связанные с изменение элементов КС и ее структуры.

1. **К косвенным каналам утечки информации относятся:**
2. использование подслушивающих (радиозакладных) устройств;
3. маскировка под других пользователей путем похищения их идентифицирующей информации (паролей, карт и т.п.);
4. злоумышленное изменение программ для выполнения ими несанкционированного копирования информации при ее обработке;

1. **Непосредственными каналами утечки называют:**
   * 1. каналы, связанные с физическим доступом к элементам КС.
     2. каналы, не связанные с физическим доступом к элементам КС
     3. каналы, связанные с изменение элементов КС и ее структуры.

1. **К непосредственным каналам утески информации относятся:** 
   * 1. обход средств разграничения доступа к информационным ресурсам

вследствие недостатков в их программном обеспечении и др.

* + 1. перехват побочных электромагнитных излучений и наводок (ПЭМИН).
    2. дистанционное видеонаблюдение;

1. **Избирательная политика безопасности подразумевает, что:** 
   * 1. права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).
     2. все субъекты и объекты системы должны быть однозначно

идентифицированы;

* + 1. каждому объекту системы присвоена метка критичности,

определяющая ценность содержащейся в нем информации;

1. **Полномочная политика безопасности подразумевает, что:**

каждому субъекту системы присвоен уровень прозрачности (security

clearance), определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

* + 1. все субъекты и объекты системы должны быть идентифицированы;
    2. права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

1. **Достоверная вычислительная база - это:** 
   * 1. абстрактное понятие, обозначающее полностью защищенный механизм вычислительной системы (включая аппаратные и программные средства), отвечающий за поддержку реализации политики безопасности.
     2. активный компонент системы, который может явиться причиной

потока информации от объекта к объекту или изменения состояния системы.

* + 1. пассивный компонент системы, хранящий, принимающий или

передающий информацию.

1. **Достоверная вычислительная база выполняет задачи:** 
   1. поддерживает реализацию политики безопасности и является

гарантом целостности механизмов защиты

* 1. функционирует на фоне избирательной политики, придавая ее требованиям иерархически упорядоченный характер (в соответствии с уровнями безопасности)
  2. представляет собой некоторый соответствующую проверку,

организационных мер набор требований, прошедших реализуемых при помощи

1. **Уязвимость информации — это:** 
   * 1. возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.
     2. набор документированных норм, правил и практических приемов,

регулирующих управление, защиту и распределение информации ограниченного доступа.

* + 1. неизменность информации в условиях ее случайного и (или)

преднамеренного искажения или разрушения.

1. **Идентификация объекта - это:** 
   * 1. одна из функций подсистемы защиты.
     2. взаимное установление подлинности объектов, связывающихся между

собой по линиям связи.

* + 1. сфера действий пользователя и доступные ему ресурсы КС

1. **Процедуру установки сфер действия пользователя и доступные ему ресурсы КС называют:**

авторизацией

* + 1. аутентификацией
    2. Идентификация

1. **Авторизация - это:**

а) предоставлением полномочий

* + 1. подтверждение подлинности
    2. цифровая подпись

1. **Аутентификация – это:** 
   * 1. подтверждение подлинности
     2. предоставлением полномочий
     3. цифровая подпись

1. **Биометрическая идентификация и аутентификация пользователя это:** 
   * 1. идентификация потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения.
     2. схема идентификации позволяющая увеличить число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса идентификации.
     3. схема идентификации с нулевой передачей знаний.

1. **Для чего используется процедура «рукопожатия»:** 
   * 1. для взаимной проверки подлинности
     2. для распределения ключей между подлинными партнерами
     3. для безопасного использования интеллектуальных карт

1. **Параллельная схема идентификации позволяет увеличить:**
   * 1. число аккредитаций, выполняемых за один цикл, и тем самым

уменьшить длительность процесса идентификации.

* + 1. регистрацию времени для каждого сообщения
    2. объект-эталон для идентификации и аутентификации пользователей

1. **Внешняя и внутренняя формы представления аутентифицирующего объекта должны быть:** 
   * 1. семантически тождественны
     2. модифицированы
     3. структурированы

1. **Для чего были разработаны протоколы идентификации с нулевой передачей знаний:**

для безопасного использования интеллектуальных карт

* 1. для взаимной проверки подлинности
  2. для распределения ключей между подлинными партнерами

1. **Механизм запроса-ответа используется для:** 
   1. проверки подлинности
   2. шифрования
   3. регистрации времени для каждого сообщения

1. **Кто разработал алгоритм идентификации с нулевой передачей знания:** 
   1. Гиллоу и Ж. Куискуотером
   2. У. Фейге
   3. А. Фиат и А. Шамир

1. **Схему идентификации с нулевой передачей знаний предложили:** 
   1. У. Фейге, А. Фиат и А. Шамир
   2. Гиллоу и Ж. Куискуотером
   3. А. Фиат и А. Шамир

1. **Для чего создается система разграничения доступа к информации:** 
   1. для защиты информации от НСД
   2. для осуществления НСДИ
   3. определения максимального уровня конфиденциальности документа

1. **Какие методы организации разграничения доступа используются в КС:** a) матричный
   1. структурированный
   2. метод Гиллоу-Куискуотера

1. **Мандатный метод основывается на:** 
   1. многоуровневой модели защиты
   2. использование матриц доступа
   3. криптографическом преобразовании

1. **Какой из функциональных блоков должна содержать система разграничения доступа к информации:**
2. блок криптографического преобразования информации при ее хранении и передаче;
3. блок контроля среды размещения
4. блок контроля среды выполнения.

**32. Диспетчер доступа реализуется в виде:**

1. аппаратно-программных механизмов
2. аппаратных механизмов
3. программных механизмов

1. **Под ядром безопасности понимают:** 
   1. локализованную, минимизированную, четко ограниченную и надежно изолированную совокупность программно-аппаратных механизмов, доказательно правильно реализующих функции диспетчера доступа.
   2. сведения о лицах, предметах, фактах, событиях, явлениях и процессах

независимо от формы их представления.

* 1. событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

1. **Главным условием создания ядра безопасности является:** 
   1. обеспечение многоуровневого режима выполнения команд
   2. мандатное управление
   3. Матричная структура

1. **Под организацией доступа к ресурсам понимается** 
   1. весь комплекс мер, который выполняется в процессе эксплуатации КС

для предотвращения несанкционированного воздействия на технические и программные средства, а также на информацию.

* 1. хранения атрибутов системы защиты, поддержки криптографического

закрытия информации, обработки сбоев и отказов и некоторые другие.

* 1. предотвращение несанкционированного перехода пользовательских

процессов в привилегированное состояние

1. **При эксплуатации механизмов аутентификации основными задачами являются:** 
   1. генерация или изготовление идентификаторов, их учет и хранение, передача идентификаторов пользователю и контроль над правильностью выполнения процедур аутентификации в КС.
   2. разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц;
   3. реализация механизма виртуальной памяти с разделением адресных

пространств;

1. **В чем заключается правило разграничения доступа**
2. лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа равен или выше уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.
3. лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа ниже уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.
4. лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа ниже уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа,не содержатся все категории, определенные для данного документа.

1. **Правильность функционирования ядра безопасности доказывается путем:** 
   1. полной формальной верификации его программ и пошаговым доказательством их соответствия выбранной математической модели защиты.
   2. использования дополнительных программных или аппаратнопрограммных средств.
   3. использования строго определенного множества программ.

1. **Матричное управление доступом предполагает использование:** 
   1. матриц доступа
   2. аппаратно-программных механизмов
   3. субъекта допуска

1. **Основной проблемой создания высокоэффективной защиты от НСД является** 
   1. предотвращение несанкционированного перехода пользовательских

процессов в привилегированное состояние.

* 1. использования дополнительных программных или аппаратнопрограммных средств.
  2. разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц

1. **Аппаратно-программмные средства криптографической защиты информации выполняют функции:**

* 1. аутентификацию пользователя, разграничение доступа к информации, обеспечение целостности информации и ее защиты от уничтожения, шифрование и электронную цифровую подпись.
  2. организовывают реализацию политики безопасности информации на

этапе эксплуатации КС.

* 1. проверяют на отсутствие закладок приборов, устройств.

1. **Использование аппаратных средств снимает проблему:**
2. обеспечения целостности системы.
3. разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц
4. использования строго определенного множества программ.

1. **Криптографические функции плат КРИПТОН образующие ядро системы безопасности реализуются** 
   1. аппаратно
   2. программно
   3. аппаратно и программно

1. **Безопасность в частично контролируемым компьютерных системамах может быть обеспечена** 
   1. изоляцией от злоумышленника ненадежной компьютерной среды, отдельного ее компонента или отдельного процесса с помощью полностью контролируемых средств.
   2. схемой идентификации позволяющая увеличить число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса идентификации.
   3. внешней аутентификацией объекта, не принадлежащего системе;

1. **Платы серии КРИПТОН, обеспечивают защиту:**
2. ключей шифрования и электронной цифровой подписи (ЭЦП), так и неизменность их алгоритмов.
3. аппаратно-программных механизмов
4. реализации механизма виртуальной памяти с разделением

адресных пространств;

1. **К основным компонентам сети относятся:** 
   1. центры коммутации пакетов, маршрутизаторы, шлюзы и сетевые

экраны;

* 1. субъекты доступа
  2. платы серии КРИПТОН

1. **В качестве ключевых носителей устройств криптографической защиты данных серии КРИПТОН используются:** 
   1. дискеты, смарт-карты и Touch-Memory.
   2. смарт-карты, Touch-Memory
   3. дискеты, смарт-карты

1. **Средства серии КРИПТОН независимо от операционной среды обеспечивают:** 
   1. защиту ключей шифрования и электронной цифровой подписи (ЭЦП)

и неизменность алгоритма шифрования и ЭЦП.

* 1. криптомаршрутизацию
  2. функции шифрования и электронной цифровой подписи.

1. **В системе Secret Disk используется:**
2. смешанная программно-аппаратная схема защиты с возможностью выбора
3. реализация механизма виртуальной памяти с разделением

адресных пространств;

1. механизм RUN-файлов позволяет в процессе работы запускать любые

программы с предварительной проверкой их целостности.

1. **В чем заключается особенность системы Secret Disk:** 
   1. для доступа к защищенной информации необходим не только

вводимый пользователем пароль, но и электронный идентификатор.

* 1. для доступа к защищенной информации необходим только вводимый

пользователем пароль.

* 1. для доступа к защищенной информации необходим только электронный идентификатор.

1. **Мастер-ключ в Устройствах криптографической защиты данных серии КРИПТОН загружается:** 
   1. до загрузки операционной системы
   2. после загрузки операционной системы
   3. вообще не загружается

1. **Криптографических функций в устройствах криптографической защиты данных серии КРИПТОН выполняются:** 
   1. внутри платы
   2. в операционной системе
   3. в блоке загрузки операционной системы

1. **Под защитой информации понимается** 
   1. совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по проверке целостности информации и исключении несанкционированного доступа к ресурсам ПЭВМ и хранящимся в ней программам и данным.
   2. совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по реализации механизма виртуальной памяти с разделением адресных пространств;
   3. совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по разграничению прав пользователей и обслуживающего персонала.

1. **Возможные каналы утечки информации по классификации разделяют:** 
   1. человек, аппаратура, программа
   2. человек, линия связи
   3. коммутационное оборудование, человек

1. **К группе каналов утечки информации в которой основным средством является человек, относятся следующие утечки:** 
   1. расшифровка программой зашифрованной информации;
   2. несанкционированный доступ программы к информации;
   3. копирование программой информации с носителей.

1. **К группе каналов утечки информации в которой основным средством является аппаратура, относятся следующие утечки:**
   1. подключение к ПЭВМ специально разработанных аппаратных

средств, обеспечивающих доступ к информации;

* 1. хищение носителей информации (магнитных дисков, дискет, лент)
  2. копирование программой информации с носителей

1. **К группе каналов утечки информации в которой основным средством является программа, относятся следующие утечки:** 
   1. несанкционированный доступ программы к информации
   2. хищение носителей информации (магнитных дисков, дискет, лент)
   3. использование специальных технических средств для перехвата

электромагнитных излучений технических средств ПЭВМ.

1. **К средствам активной защиты относятся:** 
   1. искаженные программы (программы вирусы, искажение функций)
   2. заказное проектирование
   3. специальная аппаратура

1. **К средствам пассивной защиты относятся:** 
   1. частотный анализ
   2. авторская эстетика
   3. аппаратура защиты (ПЗУ, преобразователи)

1. **К средствам собственной защиты относятся:** 
   1. машинный код
   2. сигнатура
   3. корреляционный анализ

1. **Мероприятия по инженерно-технической защите информации от утечки по электромагнитному каналу подразделяются на:**
2. организационные и технические
3. технические и коммутационные
4. организационные и объективные

1. **Технические мероприятия направлены :** 
   1. на недопущение выхода информативного сигнала за пределы контролируемой территории с помощью сертифицированных технических средств защиты.
   2. на использование специальных технических средств для перехвата

электромагнитных излучений технических средств ПЭВМ.

* 1. на защиту ключей шифрования и электронной цифровой подписи (ЭЦП) и неизменность алгоритма шифрования и ЭЦП.

1. **Организационными мероприятиями предусматривается** 
   1. исключение нахождения в местах наличия информативного сигнала

злоумышленника и контроль за его действиями и передвижением

* 1. исключение значительной части загрузочных модулей из сферы их

досягаемости.

* 1. исключение несанкционированного доступа к ресурсам ПЭВМ и

хранящимся в ней программам и данным

1. **Активные способы защиты информации при ее утечке через сеть электропитания направленные на:** 
   1. создание маскирующего шума
   2. перехвата информации
   3. минимизацию паразитных связей внутри ПЭВМ

1. **Пассивные способы защиты информации при ее утечке через сеть электропитания направленные на**
2. минимизацию паразитных связей внутри ПЭВМ
3. создание маскирующего шума
4. перехвата информации

1. **Для минимизации паразитных связей внутри ПЭВМ используются** 
   1. радиоэкранирующие и радиопоглощающие материалы
   2. двигатели-генераторы
   3. разомкнутые линии

1. **Под системой защиты от несанкционированного использования и копирования понимается** 
   1. комплекс программных или программно-аппаратных средств, предназначенных для усложнения или запрещения нелегального распространения, использования и (или) изменения программных продуктов и иных информационных ресурсов.
   2. комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации.
   3. комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности.

1. **Под надежностью системы защиты от несанкционированного копирования понимается:**
2. способность противостоять попыткам изучения алгоритма ее работы и обхода реализованных в нем методов защиты.
3. способность систем с открытыми ключами генерировать цифровые подписи, обеспечивающие различные функции защиты, компенсирует избыточность требуемых вычислений.
4. способность к самостоятельному внедрению в тела других программ и

последующему самовоспроизведению и самораспространению в информационновычислительных сетях и отдельных ЭВМ

1. **Методы, затрудняющие считывание скопированной информации основываются на** 
   1. придании особенностей процессу записи информации, которые не позволяют считывать полученную копию на других накопителях, не входящих в защищаемую КС
   2. разграничении прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц
   3. использования дополнительных программных или аппаратнопрограммных средств.

1. **Мероприятия по инженерно-технической защите информации от утечки по электромагнитному каналу подразделяются на:**
   1. организационные и технические
   2. технические и коммутационные
   3. организационные и объективные

1. **Любая криптографическая система основана на использовании:** 
   1. криптографических ключей
   2. разомкнутых линии
   3. односторонних функций

1. **В симметричной криптосистеме отправитель и получатель сообщения используют** 
   1. один и тот же секретный ключ
   2. разные секретных ключи
   3. вообще не используют секретных ключей

1. **Асимметричная криптосистема предполагает использование** 
   1. двух ключей открытого и личного (секретного)
   2. системы разграничения доступа
   3. переносных носителей для хранения секретной информации

1. **Под ключевой информацией понимают:** 
   1. совокупность всех действующих в АСОИ ключей
   2. совокупность документов и массивов документов и информационных

технологий, реализующих информационные процессы.

* 1. совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации.

1. **Какая из функций не входит в процесс управления ключами?** 
   1. переадресация ключей
   2. генерация ключей
   3. распределение ключей

1. **Модификация ключа - это** 
   1. генерирование нового ключа из предыдущего значения ключа с

помощью односторонней (однонаправленной) функции.

* 1. генерирование нового ключа из последующего значения ключа с

помощью односторонней (однонаправленной) функции.

* 1. генерирование нового ключа из предыдущего значения ключа с

помощью двусторонней (двунаправленной) функции.

1. **Под функцией хранения ключей понимают** 
   1. организацию их безопасного хранения, учета и удаления.
   2. организацию их генерации, учета и удаления.
   3. организацию их безопасного хранения, учета и сопостовления.

1. **Механизм отметки времени позволяет каждому субъекту сети определить:** 
   1. насколько старо пришедшее сообщение, и отвергнуть его, если

появится сомнение в его подлинности.

* 1. были ли внесены изменения в файл.
  2. какие информационные потоки в системе являются "легальными", то

есть не ведут к утечке информации

1. **Модель рукопожатия применяется для:** 
   1. проверки подлинности партнеров
   2. для симметричных криптосистем с секретными ключами
   3. для асимметричных криптосистем с открытыми ключами

1. **Каким из перечисленных способов не реализуется Распределение ключей между пользователями компьютерной сети:** 
   1. документирование алгоритмов обеспечения защиты информации
   2. использованием одного или нескольких центров распределения

ключей

* 1. прямым обменом сеансовыми ключами между пользователями сети

1. **Задача распределения ключей сводится к** 
   1. построению протокола распределения ключей
   2. взаимному подтверждению подлинности участников сеанса
   3. использование минимального числа сообщений при обмене ключами

1. **Протокол Kerberos основывается на** 
   1. симметричной криптографии
   2. ассиметричной криптографии
   3. нескольких центров распределения ключей

1. **Первым алгоритмом с открытыми ключами был алгоритм:** 
   1. Диффи-Хеллмана
   2. А. Фиата
   3. А. Шамира

1. **SKIP Протокол управления:** 
   1. криптоключами
   2. защищенного канала
   3. симметричной криптосистемой

1. **В каких режимах может выполняться изучение логики работы программы:**

а) статическом

* 1. динамическом
  2. и в статическом и в динамическом

1. **Сущность статического режима заключается** 
   1. в изучении исходного текста программы
   2. в выполнение трассировки программы
   3. в использование самогенерирующих кодов

1. **Динамический режим изучения алгоритма программы предполагает** 
   1. выполнение трассировки программы
   2. изучении исходного текста программы
   3. использование самогенерирующих кодов

1. **Какой метод может противодействовать дизассемблированию** 
   1. шифрование
   2. хэширование
   3. изучение

1. **Сущность метода, основанного на использовании самогенерируемых кодов, заключается в том что** 
   1. исполняемые коды программы получаются самой программой в процессе ее выполнения.
   2. исполняемые коды программы получаются самой программой после

процесса ее выполнения.

с) исполняемые коды программы получаются самой программой до процесса ее выполнения.

1. **Трассировка программ обычно осуществляется с помощью:** 
   1. программных продуктов, называемых отладчиками
   2. шифрования
   3. самогенерируемых кодов

1. **Под компьютерным вирусом понимается:** 
   1. автономно функционирующая программа, обладающая способностью к самостоятельному внедрению в тела других программ и последующему самовоспроизведению и самораспространению в информационновычислительных сетях и отдельных ЭВМ.
   2. программа имеющая доступ к файлам системы, и имеющая возможность работать с процессами системы.
   3. программа не имеющая доступ к файлам системы, и не имеющая

возможность работать с процессами системы.

1. **Резидентные вирусы это:** 
   1. вирусы, которые после активизации постоянно находятся в

оперативной памяти компьютера и контролируют доступ к его ресурсам;

* 1. вирусы, которые выполняются только в момент запуска зараженной

программы.

* 1. вирусы, заражающие программы, хранящиеся в системных областях

дисков.

1. **Транзитные вирусы это:**

а) вирусы, которые выполняются только в момент запуска зараженной программы.

* 1. вирусы, которые после активизации постоянно находятся в

оперативной памяти компьютера и контролируют доступ к его ресурсам;

* 1. вирусы, заражающие программы, хранящиеся в системных областях

дисков.

1. **Вирусы-мутанты (MtE-вирусы) это** 
   1. вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие

различие разных копий вируса.

* 1. вирусы, пытающиеся быть невидимыми на основе контроля доступа к

зараженным элементам данных;

* 1. вирусы, заражающие программы, хранящиеся в системных областях

дисков.

1. **Stealth-вирусы это** 
   1. вирусы, пытающиеся быть невидимыми на основе контроля доступа к

зараженным элементам данных:

* 1. вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие

различие разных копий вируса.

* 1. вирусы, которые после активизации постоянно находятся в

оперативной памяти компьютера и контролируют доступ к его ресурсам;

1. **Загрузочные (бутовые) вирусы это:** 
   1. вирусы, заражающие программы, хранящиеся в системных областях

дисков.

* 1. вирусы, которые после активизации постоянно находятся в

оперативной памяти компьютера и контролируют доступ к его ресурсам;

* 1. вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие

различие разных копий вируса.

1. **Трянские программы это:**
2. программы которые содержат скрытые последовательности команд (модули), выполняющие действия, наносящие вред пользователям.
3. программы , содержащие в себе алгоритмы шифрования,

обеспечивающие различие разных копий вируса.

1. программы которые после активизации постоянно находятся в

оперативной памяти компьютера и контролируют доступ к его ресурсам;

**98. Файловые вирусы это:**

1. вирусы, заражающие файлы с программами
2. вирусы, заражающие программы, хранящиеся в системных областях

дисков.

вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам.

**Темы рефератов**

1. Применение привязки к биту и электронной жеребьевки для совместной выработки ключей.
2. Применение схем разделения секрета для безопасной отправки сообщений и депонирования ключей.
3. Идентификация и аутентификация в ОС Windows и Unix.
4. Разновидности цифровых подписей в электронном документообороте.
5. Схемы электронных денег WebMoney и payCash.
6. Схемы электронных денег eCash и PayCash.
7. Криптографические средства в электронном документообороте федеральных и местных органов управления в РФ.
8. Системы управления криптографическими ключами в федеральных и местных органах управления в РФ.
9. Обзор криптографических протоколов, использующих цифровую подпись.
10. Практика электронного голосования на примере ЕС.
11. Применение протокола «Покер по телефону» к раздаче электронных бланков.
12. Идентификация на основе биометрических данных.

**ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ**

**ВОПРОСЫ К ЭКЗАМЕНУ**

1. Идентификация субъекта 2. Идентифицирующая информация 3. Понятие защищённой системы 4. Правила разграничения доступа 5. Модели ОС. Сравнительный анализ ОС 6. Избирательное разграничение доступа 7. Изолированная программная среда 8. Полномочное разграничение доступа без контроля информационных потоков 9. Полномочное разграничение доступа 10. Матрица доступа и вектор доступа 11. Обеспечение конфиденциальности (правила NRU и NWD) 12. Критерии информационной безопасности 13. Технология ЭЦП

14. Понятие “лобовой атаки”, методы формирования паролей

15. Методы борьбы с подбором идентифицирующей информации 16. Методы борьбы с подбором паролей, полученных на основе ошибок администратора 17. Методы борьбы с подбором паролей, полученных на основе ошибок реализации 18. Социальная психология и иные способы получения паролей 19. Принципы построения криптосистем 20. Уровни криптосистем 21. Компоненты Криптосистем 22. Функции Криптосистем

1. Методы получения “случайности”
2. Принципы построения генераторов ПСП и ИСП.
3. Архивация. Алгоритмы архивации
4. Генерация ключей. Распределение ключей. Главный ключ.

27. Восстановление системы при компрометации ключей

1. Классификация криптоалгоритмов
2. Симметричные криптоалгоритмы
3. Асимметричные криптоалгоритмы

31. Технология Хэш-функций

1. Криптосистема семейства программ ViPNet.
2. Состав и назначение компонентов ViPNet [Администратор]
3. Состав и назначение компонентов ViPNet [Координатор]
4. Состав и назначение компонентов ViPNet [Клиент]
5. Состав и назначение компонентов ViPNet [Криптомания]
6. Состав и назначение компонентов ViPNet [PersonalFirewoll]
7. Назначение и принципы построения VPN
8. Формирование структуры виртуальной сети ViPNet
9. Формирование ключевой информации ViPNet
10. Содержание ключевого набора и \*.dst – файла
11. Формирование ключей при изменениях в структуре своей сети

43. Межсетевое взаимодействие ViPNet

1. Противодействие изучению исходных текстов
2. Противодействие анализу двоичного кода
3. Защита от РПВ
4. Классификация РПВ
5. Методы и средства защиты информации от технических сбоев, поломок, стихийных бедствий
6. Понятие избыточности
7. Принципы функционирования систем в чрезвычайных условиях. Восстановление работоспособности систем

**Задачи к экзамену:**

**КРИТЕРИИ И ШКАЛА ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ЗАЧЕТЕ / ЭКЗАМЕНЕ**

|  |  |  |
| --- | --- | --- |
| Баллы | Оценка  /зачет | критерии оценивания |
| 85 – 100 | *«отлично»*  */ зачтено* | Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал различной литературы, правильно обосновывает принятое нестандартное решение, владеет разносторонними навыками и приемами выполнения практических задач по формированию общепрофессиональных компетенций. |
| 75 - 84 | *«хорошо» /*  *зачтено* | Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения, а также имеет достаточно полное представление о значимости знаний по дисциплине. |
| 51 – 74 | *«удовлетв о-* | Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, |
|  | *рительно»*  */ зачтено* | но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает сложности при выполнении практических работ и затрудняется связать теорию вопроса с практикой. |
| менее 51 | *«неудовле творитель но»/ незачтено* | Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, неуверенно отвечает, допускает серьезные ошибки, не имеет представлений по методике выполнения практической работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по данной дисциплине. |

**ТЕМАТИКА КУРСОВЫХ РАБОТ / ПРОЕКТОВ**

**(не предусмотрено)**

**IV. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ**

**ОЦЕНИИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ,**

**ХАРАКТЕРИЗУЮЩИЕ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ**

Процедура оценивания – порядок действий при подготовке и проведении аттестационных испытаний и формировании оценки.

Процедура промежуточной аттестации проходит в соответствии с Положением о промежуточной (рубежной) аттестации знаний студентов и учащихся ДГИНХ.

* Аттестационные испытания проводятся преподавателем (или комиссией преподавателей – в случае модульной дисциплины), ведущим лекционные занятия по данной дисциплине, или преподавателями, ведущими практические и лабораторные занятия (кроме устного экзамена). Присутствие посторонних лиц в ходе проведения аттестационных испытаний без разрешения ректора или проректора не допускается (за исключением работников университета, выполняющих контролирующие функции в соответствии со своими должностными обязанностями). В случае отсутствия ведущего преподавателя аттестационные испытания проводятся преподавателем, назначенным письменным распоряжением по кафедре (структурному подразделению).
* Инвалиды и лица с ограниченными возможностями здоровья, имеющие нарушения
* опорно-двигательного аппарата, допускаются на аттестационные испытания в сопровождении ассистентов-сопровождающих.
* Во время аттестационных испытаний обучающиеся могут пользоваться программой учебной дисциплины, а также с разрешения преподавателя справочной и нормативной литературой, непрограммируемыми калькуляторами.
* Время подготовки ответа при сдаче зачета/экзамена в устной форме должно составлять не менее 40 минут (по желанию обучающегося ответ может быть досрочным). Время ответа – не более 15 минут.
* При подготовке к устному экзамену экзаменуемый, как правило, ведет записи в листе устного ответа, который затем (по окончании экзамена) сдается экзаменатору.
* При проведении устного экзамена экзаменационный билет выбирает сам экзаменуемый в случайном порядке.
* Экзаменатору предоставляется право задавать обучающимся дополнительные вопросы в рамках программы дисциплины текущего семестра, а также, помимо теоретических вопросов, давать задачи, которые изучались на практических занятиях.
* Оценка результатов устного аттестационного испытания объявляется обучающимся в день его проведения. При проведении письменных аттестационных
* испытаний или компьютерного тестирования – в день их проведения или не позднее следующего рабочего дня после их проведения.
* Результаты выполнения аттестационных испытаний, проводимых в письменной форме, форме итоговой контрольной работы или компьютерного тестирования, должны быть объявлены обучающимся и выставлены в зачётные книжки не позднее следующего рабочего дня после их проведения.

Порядок подготовки и проведения промежуточной аттестации в форме экзамена

|  |  |  |  |
| --- | --- | --- | --- |
| действие | сроки | методика | ответственный |
| выдача  вопросов для  промежуточной аттестации | 1 неделя семестра | на лекционных  /практических и др.занятиях, на офиц.сайте вуза и др. | ведущий преподаватель |
| консультации | последняя неделя  семестра/пери од сессии | на групповой консультации | ведущий преподаватель |
| промежуточная аттестация | в период  сессии | устно | ведущий  преподаватель, комиссия |

**КРИТЕРИИ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ НА РАЗЛИЧНЫХ**

**ЭТАПАХ ИХ ФОРМИРОВАНИЯ ПО ВИДАМ ОЦЕНОЧНЫХ СРЕДСТВ**

**ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №  п/п | наименование  оценочного средства | характеристика оценочного средства | Представление оценочного средства в фонде | |
|  | **УСТНЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА** | | | |
| 1 | собеседование, устный опрос | Средство контроля,  организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. | | Вопросы по темам/разделам дисциплины |
|  | **ПИСЬМЕННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА** | | | |
| 1 | Реферат | Продукт самостоятельной работы аспиранта, представляющий собой краткое изложение в письменном виде полученных результатов теоретического | | Темы рефератов |
|  |  | анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее. | |  |
| 2 | Тест | Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. | | Фонд тестовых заданий |
| 3 | Контрольная работа | Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу | | комплект контрольных заданий по вариантам |
| 4 | Курсовая работа | Продукт самостоятельной работы обучающегося, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной учебноисследовательской темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а так же собственные взгляды на нее. | | Темы курсовых работ |
| 5 | Лабораторная работа | Средство для закрепления и практического освоения материала по определенному  разделу | | Комплект лабораторных заданий |
| 6 | Задача | Это средство раскрытия  связи между данными и искомым, заданные условием задачи, на основе чего надо выбрать, а затем выполнить действия, в том числе арифметические, и дать ответ на вопрос задачи. | | задания по задачам |

**А) КРИТЕРИИ И ШКАЛА ОЦЕНИВАНИЯ ОТВЕТОВ НА УСТНЫЕ**

**ВОПРОСЫ**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/ | критерии оценивания | количество баллов | оценка/з ачет |
| п |  |  |  |
| 1. | 1. полно и аргументированно отвечает по содержанию задания; 2. обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные; 3. излагает материал последовательно и правильно. | 10 | отлично |
| 2. | студент дает ответ, удовлетворяющий тем же требованиям, что и для оценки «5», но допускает 1-2 ошибки, которые сам же исправляет. | 8 | хорошо |
| 3. | ставится, если студент обнаруживает знание и понимание основных положений данного задания, но:   1. излагает материал неполно и допускает неточности в определении понятий или формулировке правил; 2. не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; 3. излагает материал непоследовательно и допускает ошибки. | 5 | удовлет ворител ьно |
| 4. | студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал; отмечаются такие недостатки в подготовке студента, которые являются серьезным препятствием к успешному овладению последующим материалом. | 0 | неудовл етворит ельно |

**Б) КРИТЕРИИ И ШКАЛА ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ**

**ТЕСТИРОВАНИЯ**

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | тестовые нормы:% правильных ответов | количество баллов | оценка/зачет |
| 1 | 90-100 % | 25-30 |  |
| 2 | 80-89% | 19-24 |  |
| 3 | 70-79% | 13-18 |  |
| 4 | 60-69% | 7-12 |  |
| 5 | 50-59% | 11-6 |  |
| 6 | менее 50% | 0 |  |

**В) КРИТЕРИИ И ШКАЛА ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ РЕШЕНИЯ**

**ЗАДАЧ**

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | критерии оценивания | количество баллов | оценка/зачет |
| 1 | Полное верное решение. В логическом рассуждении и решении нет ошибок, задача решена рациональным способом. Получен правильный ответ.Ясно описан способ решения. | 9-10 |  |
| 2 | Верное решение, но имеются небольшие недочеты, в целом не влияющие на решение, такие как небольшие логические пропуски, не связанные с основной идеей решения. Решение оформлено не вполне аккуратно, но это не мешает пониманию решения. | 7-8 |  |
| 3 | Решение в целом верное. В логическом рассуждении и решении нет существенных ошибок, но задача решена неоптимальным способом или допущено не более двух незначительных ошибок. В работе присутствуют арифметическая ошибка, механическая ошибка или описка при переписывании выкладок или ответа, не исказившие экономическое содержание ответа. | 5-6 |  |
| 4 | В логическом рассуждении и решении нет ошибок, но допущена существенная ошибка в математических расчетах. При объяснении сложного экономического явления указаны не все существенные факторы. | 3-4 |  |
| 5 | Имеются существенные ошибки в логическом рассуждении и в решении. Рассчитанное значение искомой величины искажает экономическое содержание ответа. Доказаны вспомогательные утверждения, помогающие в решении задачи. | 2-3 |  |
| 6 | Рассмотрены отдельные случаи при отсутствии решения. Отсутствует окончательный |  |  |
|  | численный ответ (если он предусмотрен в задаче). Правильный ответ угадан, а выстроенное под него решение - безосновательно. | 1 |  |
| 7 | Решение неверное или отсутствует. | 0 |  |

**Г) КРИТЕРИИ И ШКАЛА ОЦЕНИВАНИЯ РЕФЕРАТОВ**

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | критерии оценивания | количество баллов | оценка/зачет |
| 1 | выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы. | *9-10 баллов* |  |
| 2 | основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы. | *7-8 баллов* |  |
| 3 | имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы. | *4-6 баллов* |  |
| 4 | тема освоена лишь частично; допущены грубые ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод. | 1-3 баллов |  |
| 5 | тема реферата не раскрыта, обнаруживается существенное непонимание проблемы. | *0 баллов* |  |

**Д) КРИТЕРИИ И ШКАЛА ОЦЕНИВАНИЯ КОНТРОЛЬНЫХ РАБОТ**

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | критерии оценивания | количество баллов | оценка |
| 1 | исключительные знания, абсолютное понимание сути вопросов, безукоризненное знание основных понятий и положений, логически и лексически грамотно изложенные, содержательные, аргументированные и исчерпывающие ответы | 19-20 |  |
| 2 | глубокие знания материала, отличное понимание сути вопросов, твердое знание основных понятий и положений по вопросам, структурированные, последовательные,  полные, правильные ответы | 17-18 |  |
| 3 | глубокие знания материала, правильное понимание сути вопросов, знание основных понятий и положений по вопросам, содержательные, полные и конкретные ответ на вопросы. Наличие несущественных или технических ошибок | 15-16 |  |
| 4 | твердые, достаточно полные знания, хорошее понимание сути вопросов, правильные ответы на вопросы, минимальное количество  неточностей, небрежное оформление | 13-14 |  |
| 5 | твердые, но недостаточно полные знания, по сути верное понимание вопросов, в целом правильные ответы на вопросы, наличие неточностей, небрежное оформление | 11-12 |  |
| 6 | общие знания, недостаточное понимание сути вопросов, наличие большого числа  неточностей, небрежное оформление | 9-10 |  |
| 7 | относительные знания, наличие ошибок, небрежное оформление | 7-8 |  |
| 8 | поверхностные знания, наличие грубых ошибок, отсутствие логики изложения  материала | 5-6 |  |
| 9 | непонимание сути, большое количество грубых ошибок, отсутствие логики изложения  материала | 3-4 |  |
| 10 | не дан ответ на поставленные вопросы | 1-2 |  |
| 11 | отсутствие ответа, дан ответ на другие вопросы, списывание в ходе выполнения | 0 |  |
|  | работы, наличие на рабочем месте технических средств, в том числе телефона |  |  |

**Ж) КРИТЕРИИ И ШКАЛА ОЦЕНКИ ПРЕЗЕНТАЦИЙ**

|  |  |  |
| --- | --- | --- |
| №  п/п | критерии оценки | максимальное  количество баллов |
| 1 | титульный слайд с заголовком | 5 |
| 2 | дизайн слайдов | 10 |
| 3 | использование дополнительных эффектов (смена слайдов, звук, графика, анимация) | 5 |
| 4 | список источников информации | 5 |
| 5 | широта кругозора | 5 |
| 6 | логика изложения материала | 10 |
| 7 | текст хорошо написан и сформированные идеи ясно изложены и структурированы | 10 |
| 8 | слайды представлены в логической последовательности | 5 |
| 9 | грамотное создание и сохранение документов в папке рабочих материалов | 5 |
| 10 | слайды распечатаны в форме заметок | 5 |
|  | средняя оценка: |  |