**Областное государственное бюджетное образовательное учреждение**

**среднего профессионального образования**

**«Смоленский промышленно-экономический колледж»**

**Комплект контрольно-измерительных материалов по учебной дисциплине**

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

основной профессиональной образовательной программы (ОПОП)

по специальности СПО

**230115 Программирование в компьютерных системах**

**(углубленная подготовка)**

Комплект контрольно-измерительных материалов по учебной дисциплине Информационная безопасность разработан на основе Федерального государственного образовательного стандарта по специальности СПО 230115 Программирование в компьютерных системах (углубленная подготовка)

Организация разработчик: ОГБОУ СПО «Смоленский промышленно-экономический колледж»

Разработчик: Ромашкова И.И., преподаватель специальных дисциплин кафедры Информационных технологий

Рассмотрено на заседании кафедры Информационных технологий

Протокол №\_\_\_\_ от «\_\_\_\_»\_\_\_\_\_\_\_20\_\_\_г.

Зав. кафедрой (декан)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Малахова В.Г.

Рассмотрено научно-методическим советом ОГБОУ СПО «Смоленский промышленно-экономический колледж»

Протокол №\_\_\_ от «\_\_\_»\_\_\_\_\_20\_\_г.

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

Содержание

1. Паспорт комплекта контрольно-измерительных средств...................................................................4

1.1. Область применения........................................................................................................................4

* 1. Система контроля и оценки освоения программы учебной дисциплины .................................4
     1. Форма итоговой аттестации по ОПОП при освоении учебной дисциплины......................5

1.2.2. Организация контроля и оценки освоения программы ОП..................................................5

2. Комплект материалов для оценки освоенных умений и усвоенных знаний по дисциплине «Информационная безопасность»...............................................................,,,,,,,,,,,,,,.......................................6

3. Образец пакета экзаменатора.................................................................................................................8

**I. Паспорт комплекта контрольно-оценочных средств**

**1.1. Область применения**

Комплект контрольно-измерительных материалов предназначен для проверки результатов освоения общепрофессиональной дисциплины Информационная безопасность по специальности 230115 Программирование в компьютерных системах (по программе углубленной подготовки).

**Комплект контрольно-оценочных средств позволяет оценивать:**

* + 1. Освоение умений и усвоение знаний:

|  |  |  |
| --- | --- | --- |
| **Знания и умения для проверки** | **Показатели оценки результата** | **№№ заданий**  **для проверки** |
| Классифицировать основные угрозы безопасности информации | - Точность определения угроз безопасности информации в соответствии с классификацией | Практическая задача |
| Применять организационные, правовые, программно-технические, криптографические методы и средства защиты информации | - Грамотность применения организационных, правовых, программно-технических, криптографических методов и средств защиты информации защиты информации |
| Применять антивирусные средства защиты информации | Техничность применения антивирусных средств защиты информации |
| Знать сущность и понятия информационной безопасности | - Точность изложения сущности ИБ  - Точность соотнесения понятий информационной безопасности с их определениями | Теоретический  вопрос 1 |
| Знать основные угрозы, методы и средства обеспечения информационной безопасности | - Точность определения угроз информационной безопасности  - Соответствие выбранных средств обеспечения информационной безопасности для предотвращения угроз | Теоретический  вопрос 1 |
| Знать принципы защиты информации от несанкционированного доступа | - Точность изложения принципов защиты информации от несанкционированного доступа. | Теоретический  вопрос 2 |
| Знать правила применения, эксплуатации и обслуживания технических средств защиты информации | - Точность изложения правила применения, эксплуатации и обслуживания технических средств защиты информации. | Теоретический  вопрос 2 |
| Знать возможность утечки информации по техническим каналам и способы противодействия им | - Точность изложения структуры, классификации и основных характеристик технических каналов утечки информации и способов противодействия им | Теоретический  вопрос 2 |

**1.2 Система контроля и оценки освоения программы учебной дисциплины**

Текущий контроль освоения программы дисциплины предусматривает рейтинговую систему оценки и проводится в пределах учебного времени, отведенного на её изучение, с использованием таких методов, как написание самостоятельных работ, контрольных работ, выполнение тестов, проведение устного опроса, выполнение практических работ.

Оценка освоения программы дисциплины проводится в соответствии с «Положением о промежуточной аттестации» и рабочим учебным планом в форме экзамена.

* + 1. **Форма итоговой аттестации по ОПОП при освоении учебной дисциплины:**

Экзамен проводится в форме устного собеседования по билетам, содержащим два теоретических вопроса и задачу.

**1.2.2. Организация контроля и оценки освоения программы ОП**

Итоговый контроль освоения дисциплины «Информационной безопасность» осуществляется на экзамене. Условием допуска к экзамену является положительная текущая аттестация по всем практическим работам учебной дисциплины, ключевым теоретическим вопросам дисциплины (проверка выполняется текущим контролем).

**2. Комплект материалов для оценки освоенных умений и усвоенных знаний по дисциплине** *Информационной безопасность*

ЗАДАНИЯ ДЛЯ ЭКЗАМЕНУЮЩИХСЯ № 1,

**Условия выполнения задания:**

Задание выполняется в учебной аудитории.

Используемое оборудование: компьютеры с установленным необходимым программным обеспечением, оборудование для программно-технической защиты информации.

**Инструкция:**

1.Задание выполняется в два этапа:

- дайте ответ на предложенные Вам теоретические вопросы;

- решите предложенную задачу.

2. При выполнении решения задачи вы можете воспользоваться компьютером, калькулятором, необходимым оборудованием по программно-технической защите информации.

3. Максимальное время выполнения задания – 60 мин. (теоретическое задание – 30 мин., задача – 30 мин.)

**Образец экзаменационного билета**

|  |
| --- |
| 1. Раскройте сущность понятия информационная безопасность. 2. Охарактеризуйте парольные системы для защиты от несанкционированного доступа к информации. 3. Произведите установку и настройку оборудования - средства аутентификации «Рутокен». |

**Описание экзаменационного билета**

Весьтеоретический материал курса логически разделяется на части, представленные в рабочей программе:

Раздел I. Информационная безопасность. Основные положения, понятия, определения.

Раздел II: Сущность и понятие защиты информации.

Раздел III: Методы и средства борьбы с угрозами информационной безопасности систем обработки информации.

Первый теоретический вопрос билета относится к материалу, охватывающему разделы I-II дисциплины, второй вопрос билета – раздел III.

Практическое задание представлено задачами по применению программно-технических, криптографических методов и средств защиты информации. Данные темы являются наиболее важными для обеспечения безопасности информации в компьютерных системах.

ПРИЛОЖЕНИЕ 1. ЭКЗАМЕНАЦИОННЫЕ ВОПРОСЫ

**ПАКЕТ ЭКЗАМЕНАТОРА**

**А. УСЛОВИЯ**

Экзамен проводится в форме устного собеседования по билетам, содержащим два теоретических вопроса и задачу. Каждому студенту выдается свой вариант.

**Б. КРИТЕРИИ ОЦЕНКИ**

Выполнение заданий

|  |  |  |
| --- | --- | --- |
| **Действия** | | **Выполнил (максимально**  **50 баллов)** |
| Ответ на теоретический вопрос № 1 | | 15 |
| Ответ на теоретический вопрос № 2 | | 15 |
| Решение задачи:  - выбор метода, средства решения задачи и его реализация;  - полнота полученного ответа;  - проведение дополнительных рассуждений, в том числе ответы на дополнительные вопросы по решению задачи. | | 20  10  5  5 |
| Итоговое количество баллов: | | 50 |
| **5 «отлично»** | 44-50 баллов | |
| **4 «хорошо»** | 37-43 балла | |
| **3 «удовлетворительно»** | 28-35 баллов | |
| **2 «неудовлетворительно»** | 0-27 баллов | |
| **Итоговая оценка**  *Оценка «5»* выставляется в том случае, если студент продемонстрировал высокий уровень знании и умений по всем трем вопросам билета. Студент полностью раскрыл содержание теоретических вопросов, правильно выполнил практическое задание. Могут быть допущены недочеты в определении понятий или при решении задачи, исправленные студентом самостоятельно в процессе ответа.  *Оценка «4»* выставляется в том случае, если студент продемонстрировал понимание основного содержания всех вопросов билета. Ответ четко структурирован, логичен, изложен литературным языком. Допущена 1 ошибка при решении задачи. Могут быть допущены 2-3 неточности или незначительные ошибки при ответе на теоретические вопросы, исправленные студентом с помощью преподавателя.  *Оценка «3»* выставляется в том случае, если студент продемонстрировал понимание основного содержания вопросов билета. Могут быть допущены 2-3 неточности или незначительные ошибки при ответе на теоретические вопросы, исправленные студентом с помощью преподавателя. Допущены 2 ошибки при решении задачи.  *Оценка «2»* выставляется в том случае, если студент продемонстрировал не понимание основного содержания трех вопросов билета. Ответ представляет собой разрозненные знания с существенными ошибками по вопросам. Присутствуют фрагментарность, нелогичность изложения. Не решена задача. | | |

Количество вариантов (пакетов) заданий для студентов: 25 экзаменационных билетов.

Время выполнения задания:

*первый этап* (подготовка к ответу на теоретические вопросы) – 30 мин,

*второй этап* (выполнение практического задания) – 30 мин.  
Условия выполнения заданий:

*Задания выполняются в учебной аудитории.*

*Требования охраны труда*: инструктаж по технике безопасности при работе в компьютерном классе.

*Оборудование:* персональные компьютеры, комплект лицензионного программного обеспечения, оборудование для программно-технической защиты информации.

**Литература для учащегося:**

1. Мельников В.П. Информационная безопасность : учеб. пособие для спо / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. - 4-е изд., стереотип. - М. : Академия, 2009.
2. Анин Б.Ю. Защита компьютерной информации. Петербург, 2008. - 384с.
3. Анисимова И.Н., Стельмашонок Е.В. Защита информации. Учебное пособие. - 2008.
4. Галатенко В.А., Барсуков В.С., Водолазний В.В. Современные технологии безопасности. - М.: «Нолидж», 2009. - 496 с.

**Разработчики:**

ОГБОУ СПО СПЭК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ромашкова И.А.

преподаватель

**ЭКЗАМЕНАЦИОННЫЕ ВОПРОСЫ**

1. Раскройте сущность понятия информационной безопасность.
2. Перечислите основные требования по защите средств вычислительной техники и автоматизированных систем от НСД.
3. Дайте характеристику составляющих информационной безопасности.
4. Охарактеризуйте классы защищенности средств вычислительной техники от НСД и показатели защищенности.
5. Укажите национальные интересы Российской Федерации в информационной сфере.
6. Охарактеризуйте классы защищенности автоматизированных систем от НСД и показатели защищенности.
7. Дайте характеристику информационной безопасности в системе национальной безопасности РФ.
8. Раскройте содержание понятий идентификация и аутентификация.
9. Охарактеризуйте современную концепцию информационной безопасности Российской Федерации.
10. Укажите возможности разграничения доступа к элементам защищаемой информации.
11. Раскройте содержание понятий информационные ресурсы и информационные войны.
12. Дайте характеристику парольных систем для защиты от несанкционированного доступа к информации.
13. Укажите основные причины, создающие возможность применения информационного оружия против РФ.
14. Перечислите критерии выбора и хранения паролей.
15. Охарактеризуйте основные Стандарты в области обеспечения информационной безопасности.
16. Перечислите требования к системам криптографической защиты информации.
17. Охарактеризуйте законодательную базу РФ в области обеспечения информационной безопасности.
18. Классифицируйте методы криптографического закрытия.
19. Дайте характеристику государст­венной системы обеспечения информационной безопасности.
20. Охарактеризуйте способы применение криптографических методов и средств защиты информации.
21. Охарактеризуйте уровни доступа к информации с точки зрения законодательства.
22. Дайте характеристику стандартных алгоритмов шифрования.
23. Перечислите виды ответственности за нарушение законодательства в информационной сфере.
24. Раскройте содержание понятий безопасность и быстродействие криптосистемы.
25. Классифицируйте источники и носители защищаемой информации.
26. Охарактеризуйте отечественный стандарт шифрования данных и криптографический стандарт DES.
27. Раскройте содержание понятия конфиденциальная информация.
28. Перечислите программно-технические угрозы информационной безопасности ПК.
29. Классифицируйте конфиденциальную информацию по видам тайны и степеням конфиденциальности.
30. Охарактеризуйте средства вторжения в частную жизнь.
31. Дайте характеристику жизненных циклов конфиденциальной информации в процессе ее создания, обработки, передачи.
32. Перечислите виды вредоносного программного обеспечения.
33. Перечислите принципы отнесения циркулирующей в организации информации по видам тайн.
34. Дайте характеристику методов распространения компьютерных вирусов.
35. Раскройте содержание понятий угрозы безопасности информации, опасности и риски.
36. Дайте характеристику деструктивных возможностей компьютерных вирусов.
37. Дайте классификацию угроз безопасности информации.
38. Охарактеризуйте средства антивирусной защиты.
39. Охарактеризуйте виды утечки конфиденциальной информации.
40. Охарактеризуйте способы защиты информации при копировании и передаче информации.
41. Дайте характеристику методов выявления угроз объекту информатизации.
42. Опишите режимы функционирования межсетевых экранов и их основных компонент.
43. Дайте характеристику способов воздействия на системы обработки информации.
44. Опишите средства защиты информации: маршрутизаторы, шлюзы сетевого уровня.
45. Охарактеризуйте способы активного воздействия на объект атаки.
46. Перечислите основные схемы сетевой защиты на базе межсетевых экранов.
47. Опишите формы атак на информацию.
48. Охарактеризуйте классы защищенности межсетевых экранов.
49. Перечислите каналы несанкционированного получения информации.
50. Объясните суть управления правами пользователей и их привилегиями.

**Виды практических заданий к экзамену**

1. Настройте адекватную политику безопасности компьютера, удовлетворяющую обеспечению надежной защиты операционной системы.
2. Имея права администратора, восстановите пароль учетной записи с ограниченными правами сотрудника фирмы и войдите в систему.
3. Произведите установку и настройку персонального средства криптографической защиты (далее СКЗИ) «Шипка 1.5».
4. Произведите установку и настройку оборудования – биометрической флэш-памяти nTegrity Pro Vista.
5. Произведите установку и настройку оборудования - мышь со считывателем отпечатка пальца – EyeD Opti.
6. Произведите установку и настройку оборудования - комплекс СЗИ НСД «Аккорд - АМДЗ».
7. Произведите установку и настройку оборудования - АПМДЗ «КРИПТОН - ЗАМОК».
8. Произведите установку и настройку оборудования - средства аутентификации «Рутокен».
9. Произведите обеспечение безопасности файла и его компонент встроенными методами прикладной программы MS Access.
10. Произведите обеспечение безопасности файла и его компонент встроенными методами прикладной программы MS Word.
11. Произведите обеспечение безопасности файла и его компонент встроенными методами прикладной программы MS Excel.
12. Произведите установку и обновление баз данных антивирусных программ, настройте антивирусную защиту.
13. Произведите установку и настройку оборудования - аппаратного комплекса защиты конфиденциальной информации «Aladdin. SecretDisk».
14. Определите адекватную политику безопасности компьютера и произведите её настройку. На компьютере уже выполнены настройки, не позволяющие открывать консоль mmc даже в режиме Администратора.
15. Произведите установку и настройку оборудования - средства аутентификации «Рутокен».
16. Определите число G для создания электронной цифровой подписи по отечественному стандарту, если P=311, Q=31.
17. Расшифруйте текст "ГДТНЭМОАВЫКЕСРЕЙЗНУСН\_А", используя метод шифрующих таблиц, (ключ: 4х6).
18. Зашифруйте текст "ИСХОДНЫЕ ДАННЫЕ", используя метод перестановки с помощью ключа (ключевое слово: (ОСЕНЬ)).
19. Зашифруйте текст "ОДУВАНЧИК" с помощью генератора псевдослучайных чисел, описываемого соотношением: T(i) = (A\*T(i-1) + C) mod M, где Т(0)=5, А=7, С=17, М=32.
20. Найдите открытый ключ для секретного ключа Т=5, используя шифр Эль Гамаля, где Р=13 и G=7.
21. Расшифруйте текст "ЕЖОЮ.СЗНШН", используя биграммный шифр Плейфера, (ключевое слово: МОЛНИЯ, таблица: 5х7).
22. Зашифруйте текст "АБИТУРИЕНТ", используя шифр Трисемуса, (ключевое слово: ЗЕФИР, таблица: 5х7).
23. Зашифруйте текст "ЭКЗАМЕН", используя аффинную систему Цезаря, (ключ: a=4, b=7).