

|  |
| --- |
|  |

**КОМПЛЕКТ**

**ОЦЕНОЧНЫХ СРЕДСТВ**

по междисциплинарному курсу

**МДК 03.02. Программно-аппаратные средства защиты информации**

специальность 090905 Организация и технология защиты информации

по программе базовой подготовки

Москва 2015

|  |  |
| --- | --- |
| РАССМОТРЕНЫ  Предметной цикловой комиссией  Протокол № \_\_\_1\_\_  Председатель ПЦК  \_\_\_\_\_\_\_\_\_\_\_  « 31 » августа 2015г. | УТВЕРЖДАЮ  Зам. директора по УМР  ГБПОУ КС № 54  \_\_\_\_\_\_\_\_\_\_И.Г. Бозрова  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_2015 г. |

Разработчик:

Бастрыкин К.М., преподаватель ГБПОУ Колледж связи №54 ОП6

СОДЕРЖАНИЕ

1.Паспорт фонда оценочных средств

2.Приложения

2.1 Комплект тестов

2.2 Перечень лабораторных работ и практических занятий

2.4 Вопросы для устного (письменного опроса)

2.5 Перечень самостоятельных работ

**Паспорт**

**комплекта оценочных средств**

по междисциплинарному курсу **МДК 03.02. Программно-аппаратные средства защиты информации**

Комплект оценочных средств представляет собой совокупность контрольно-оценочных средств для определения качества освоения студентом междисциплинарного курса.

В результате освоения междисциплинарного курса обучающийся должен обладать предусмотренными ФГОС по специальности следующими умениями и знаниями:

**уметь:**

* ра­бо­тать с тех­ни­че­ски­ми сред­ст­ва­ми за­щи­ты ин­фор­ма­ции; (У1)
* ра­бо­тать с за­щи­щен­ны­ми ав­то­ма­ти­зи­ро­ван­ны­ми сис­те­ма­ми; (У2)
* пе­ре­да­вать ин­фор­ма­цию по за­щи­щен­ным ка­на­лам свя­зи; (У3)

**знать:**

* ви­ды, ис­точ­ни­ки и но­си­те­ли за­щи­щае­мой ин­фор­ма­ции; (З1)
* струк­ту­ру, клас­си­фи­ка­цию и ос­нов­ные ха­рак­те­ри­сти­ки тех­ни­че­ских ка­на­лов утеч­ки ин­фор­ма­ции; (З2)
* клас­си­фи­ка­цию тех­ни­че­ских раз­ведок и методы про­ти­во­дей­ст­вия им; (З3)
* ме­то­ды и средства ин­же­нер­но-тех­ни­че­ской за­щи­ты ин­фор­ма­ции; (З4)

Формой аттестации по учебной дисциплине является **зачет**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Контролируемые умения, знания | Контролируемые разделы (темы) учебной дисциплины | Наименование  оценочного средства |
|  |  | **Раздел 2. Программно-аппаратная защита информации** |  |
|  |  | **Тема 2.1. Общие принципы защиты операционных систем** |  |
|  | У1,З1 | **Функционирование операционных систем.**  Назначение, функции и типы операционных систем. Принципы внутреннего функционирования. |  |
|  | У1,  З1 | **Атаки на сетевые службы.**  Возможные атаки и методы взлома операционной системы. Классификация атак по основным механизмам реализации угроз. Локальные атаки. Удаленные атаки. | УО |
|  |  | **Удаленный доступ к сети.**  Основные уязвимости удаленного доступа. DoS-атаки на серверы удаленного доступа. Автоматические программы. | УО, тесты |
|  | З1, У2 | **Тема 2.2. Базовый уровень безопасности** |  |
|  | З2, У2 | **Безопасность в ОС**  Набор настроек, применяемый к ОС для повышения ее защищенности. Шаблон безопасности. Основные проблемы с безопасностью и возможные решения в Unix-подобных системах. | УО |
|  |  | **Защита ОС.**  Защитные механизмы операционных систем. Основные задачи системы защиты операционных систем. | СР.1.2 |
|  | З1, У2 | **Доступ к элементам системы.**  Способы управления доступом. Права доступа к элементам файловой системы. | СР.1.2 |
|  | У2,З1 | **Тема 2.3. Комплексный подход к обеспечению информационной безопасности ОС.** |  |
|  | З2,У2 | **Защита информации в ОС.**  Уровни реализации защиты информации: защита операционной системы, приложений и локальных служб. Защита от изменения и контроль целостности. | УО |
|  | У1,З1 | **Компоненты безопасности локальной сети организации.**  Зоны безопасности и их компоненты: внутренняя локальная сеть организации, интернет. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. | УО |
|  | У1,  З1 | **Атаки на программное обеспечение.**  Атаки на программное обеспечение: атака на настройки безопасности по умолчанию, злоупотребление привилегиями, атаки на пароли. Обнаружения атак. | УО,СР 1.3 |
|  | У1,З1 | **Обеспечение информационной безопасности организации.**  Методы обеспечения информационной безопасности организации. Основные требования к политике безопасности. | СР 1.3 |
|  | У1,  З1 | **Практическое занятие 1**  Разработка подсистемы защиты операционной системы Linux | СР.1.1, ПЗ1 |
|  | З3, | **Практическое занятие 2**  Разработка подсистемы защиты операционной системы Linux (продолжение) | СР.1.1, ПЗ2 |
|  | У1,З1 | **Практическое занятие**  **3**  Реализация подсистемы защиты операционной системы Windows | СР.1.1, ПЗ3 |
|  | У1,З1 | **Практическое занятие 4**  Реализация подсистемы защиты операционной системы Windows (продолжение) | СР.1.1,ПЗ4 |
|  | У2,З3 | **Практическое занятие** **5**  Обеспечение защиты вычислительной сети | СР.1.1,ПЗ5 |
|  | З3. | **Практическое занятие** **6**  Управление доступом в операционных системах | СР 1.1,ПЗ6 |
|  | З1,З2, З3 | **Практическое занятие** **7**  Идентификация и аутентификация пользователей операционных систем | СР 1.1, ПЗ7 |
|  | У1,  З1 | **Понятия безопасности БД**  Угрозы безопасности БД: общие и специфичные. Требования безопасности БД. Защита от несанкционированного доступа. Защита от вывода. Целостность БД. Аудит. |  |
|  | З3, | **Критерии защищенности БД**  Критерии оценки надежных компьютерных систем. Понятие политики безопасности. Современное применение различных политик безопасности в рамках единой модели. | СР 1.4 |
|  | У1,З1 | **Модели безопасности в СУБД**  Классификация моделей. Аспекты исследования моделей безопасности. Особенности применения моделей безопасности в СУБД. Дискреционные (избирательные) и мандатные (полномочные) модели безопасности. БД с многоуровневой секретностью (MLS). | СР 1.4 |
|  | У1,З1 | **Механизмы обеспечения целостности СУБД**  Основные виды и причины возникновения угроз целостности. Способы противодействия. Режимы блокировок. Правила согласования блокировок. Двухфазный протокол синхронизационных блокировок. | УО |
|  | У2,З3 | **Механизмы обеспечения конфиденциальности в СУБД**  Причины, виды, основные методы нарушения конфиденциальности. Типы утечки конфиденциальной информации из СУБД. Организация взаимодействия СУБД и базовой ОС. Подотчетность действий пользователя и аудит связанных с безопасностью событий. |  |
|  | З3. | **Практическое занятие 8**  Организация защиты данных СУБД SQL Server 2008 | СР.1.1, ПЗ8 |
|  | З1,З2, З3 | **Практическое занятие 9**  Создание Web страниц. | СР.1.1,ПЗ9 |
|  |  | **Практическое занятие 10**  Создание БД Access с помощью SQL.  ЗАЧЕТ | СР.1.1,ПЗ10, тесты |

**Условные обозначения: ЛР –** лабораторная работа**, ПЗ** – практическое занятие, **СР** – самостоятельная работа, **УО** – устный ответ, **Т** – тестирование

Приложение 1

**КОМПЛЕКТ ТЕСТОВ**

**МДК 03.02. Программно-аппаратные средства защиты информации**

Специальность 090905 Организация и технология защиты информации

КОНТРОЛИРУЕМЫЕ ПАРАМЕТРЫ

|  |  |
| --- | --- |
| Темы | Номера тестовых заданий |
| **Тема 2.1. Общие принципы защиты операционных систем** | 1,2,3,4,5,6,7,8 |
| **Тема 2.2. Базовый уровень безопасности** | 9,10,11,12,13 |
| **Тема 2.3. Комплексный подход к обеспечению информационной безопасности ОС.** | 14,15,16,17,18 |
| **Тема 2.4. Защита информации в системах управления базами данных** | 19,20 |

Критерии оценки:

|  |  |  |
| --- | --- | --- |
| Количество правильных ответов | Процент выполнения | Оценка |
| 19-20 | более 90% | Отлично |
| 17-18 | 80-90% | Хорошо |
| 14-16 | 60-79% | Удовлетворительно |
| До 13 | менее 60% | Неудовлетворительно |

ТЕСТОВЫЕ ЗАДАНИЯ

|  |  |
| --- | --- |
| Тестовое задание | Вариант ответа |
| **1. Защита информации это-** | А) потенциальная возможность неправомерного преднамеренного или случайного воздействия , приводящее к потере или разглашению информации.  Б) реализация права на государственную тайну и конфиденциальную информацию  В) устранение или нейтрализация негативных источников, причин и условий воздействия на информацию  **Г) правовые, организационные и технические меры, направленные на обеспечение защиты информации** |
| **2. Каналы утечки информации - это** | А) это комплексы специального технического и программного обеспечения, предназначенные для предотвращения утечки информации  **Б) методы и пути утечки информации из информационной системы**  В) потенциальная возможность неправомерного преднамеренного или случайного воздействия  Г) соблюдение конфиденциальности информации ограниченного доступа |
| **3. Существуют следующие виды ПО (добавьте недостающее).** | А) Прикладное ПО  Б) Системное ПО  В) **Инструментальное ПО** |
| **4. К функциям ОС относится :** | А) поддержка работы всех программ, обеспечение их взаимодействия с аппаратурой  **Б) управление процессором путем чередования выполнения программ;**  В)обработка прерываний и синхронизация доступа к ресурсам вычислительной системы;  **Г)управление памятью путем выделения программам на время их выполнения требуемой памяти;** |
| **5. Операционная система Windows является :** | **А) многозадачной**  Б) однозадачной  **В) многопользовательской**  Г) однопользовательской |
| **6. Атаки на ОС бывают:** | **А) Локальными**  Б) Глобальными  **В) Удаленными**  Г) Близкими |
| **7. Профессиональный взлом имеет следующую структуру (восстановите последовательность)** | А) попытка внедрения вредоносных программ  Б) поиск уязвимостей в ПО ЗИ  В) тщательный анализ ПО  Г) анализ выбранной политики безопасности  **Ответ Г,В,Б,А** |
| **8. Когда пользователь знает что-то, что подтверждает его подлинность, то существуют следующие способы аутентификации:** | **А) парольная аутентификация**  Б) аутентификация по магнитному носителю  В) модель рукопожатия  Г) аутентификация по характеристикам работы пользователя |
| **9. Когда пользователь что-то имеет, что подтверждает его подлинность, то существуют следующие способы аутентификации:** | А) парольная аутентификация  **Б) аутентификация по магнитному носителю**  В) модель рукопожатия  Г) аутентификация по характеристикам работы пользователя |
| **10. К защите от удаленного НСД можно отнести:** | **А) модель рукопожатия**  **Б) Протокол Kerberos**  В) Аутентификация по биометрическим характеристикам  Г) Аутентификация по росписи мьшью |
| **11. Целью защиты информации является:** | А) предотвращение хищения, утечки, искажения, утраты и подделки информации;  **Б) предотвращение несанкционированных действий по уничтожению, модификации, копированию и блокированию информации;**  В) реализация права на государственную тайну и конфиденциальную информацию  Г) выявление правил и норм поведения человека, направленные на обеспечение безопасности информации |
| **12. К основным видам средств защиты информации относится:** | **А) нормативно-правовые**  **Б) Технические**  В) Экологические  Г) Этнические |
| **13. Технические средства защиты – это** | А) правила, меры и мероприятия, регламентирующие вопросы доступа, хранения, применения и передачи информации  **Б) это комплексы специального технического и программного обеспечения**  В) правила и нормы поведения, направленные на обеспечение безопасности информации  Г) законы и другие правовые акты, а также механизмы их реализации, регламентирующие информационные отношения в обществе |
| **14. К каналам утечки информации относится:** | **А) Магнитный канал**  **Б) Виброакустический канал**  **В) Лазерный канал**  Г) Специальный канал |
| **15. К назначению ОС относится:** | А)управление процессором путем чередования выполнения программ;  Б)обработка прерываний и синхронизация доступа к ресурсам вычислительной системы;  В)управление памятью путем выделения программам на время их выполнения требуемой памяти;  **Г)поддержка работы всех программ, обеспечение их взаимодействия с аппаратурой;** |
| **16. Многопроцессорная обработка в ОС бывает:** | **А) Симметричной**  Б) Квадратичной  В) Полной  **Г) Ассиметричной** |
| **17. К локальной защите от НСД относится:** | **А) Аутентификация на основе биометрических характеристик**  Б) Протокол CHAP  **В) Парольная аутентификация**  Г) Проток PAP |
| **18. Когда пользователь и есть то лицо, за которое себя выдает то существуют следующие способы аутентификации:** | А) парольная аутентификация  Б) аутентификация по магнитному носителю  В) модель рукопожатия  **Г) аутентификация по характеристикам работы пользователя** |
| **19. Какой протокол направленный для защиты от удаленного НСД основан на использовании одноразовых паролей.** | А) PAP  Б) CHAP  **В) S/KEY**  Г) Kerberos |
| **20. К недостаткам дискреционного управления доступом относится:** | **А) нельзя контролировать утечку конфиденциальной информации**  Б) неудобство для пользователя  В) нет опасности утечки конфиденциальной информации  Г) слабая защита от вредоносных программ |

Рассмотрены на заседании ПЦК ОПД и ПМ специальности 10.02.01 ОТЗ

Протокол № \_\_\_\_ от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Председатель ПЦК \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Н.В.Селиванова

Приложение 2

**Перечень практических занятий:**

|  |
| --- |
| ПЗ1.Разработка подсистемы защиты операционной системы Linux |
| ПЗ2. Разработка подсистемы защиты операционной системы Linux |
| ПЗ3Реализация подсистемы защиты операционной системы Windows |
| ПЗ4. Реализация подсистемы защиты операционной системы Windows |
| ПЗ5. Обеспечение защиты вычислительной сети |
| ПЗ6. Управление доступом в операционных системах |
| ПЗ 7Идентификация и аутентификация пользователей операционных систем |
| ПЗ8.Организация защиты данных СУБД SQL Server 2008 |
| ПЗ9.Создание Web страниц. |
| ПЗ10.Создание БД Access с помощью SQL |

Выполнение заданий к лабораторным работам и практическим занятиям, ответы на контрольные вопросы к ним способствуют контролю **умений** студентов по дисциплине.

Цели, задачи, задания, порядок проведения, контрольные вопросы, а также критерии оценки лабораторных работ и практических занятий представлены в методических указаниях к выполнению ЛПЗ по дисциплине

Приложение3

**Перечень вопросов для устного опроса**

КОНТРОЛИРУЕМЫЕ ПАРАМЕТРЫ

|  |  |
| --- | --- |
| Темы | Номера вопросов |
| **Тема 2.1. Общие принципы защиты операционных систем** | 1-5 |
| **Тема 2.2. Базовый уровень безопасности** | 6-11 |
| **Тема 2.3. Комплексный подход к обеспечению информационной безопасности ОС.** | 11-16 |
| **Тема 2.4. Защита информации в системах управления базами данных** | 17-18 |

ПЕРЕЧЕНЬ ВОПРОСОВ

1. Концепция информационной безопасности.

2. Каналы утечки информации.

3. Виды ПО. Назначение и функции ОС.

4. Классификация операционных систем.

5. Локальные и удаленные атаки и методы взлома ОС.

6. Защита от локального НСД.

7. Протокол Kerberos.

8. Протокол S/key

9. Идентификация и аутентификация.

10.Подсистема аутентификации Windows.

11. Разграничение доступа.

12. Избирательный и мандатный метод разграничения доступа.

13. Аудит.

14. Политика аудита.

15. Фрагментарный и комплексный подход к построению ОС.

16. Методы анализа сетевой информации.

17. Защищенность БД

18. Модели безопасности БД

Приложение 4

**Перечень самостоятельных работ:**

СР1.1. Подготовка к практическим занятиям, оформление отчета по ПЗ

СР1.2. Подбор материала и создание презентации по теме: Защита ОС от сетевых атак

СР1.3. Подготовить реферат по теме: Информационная безопасность организаций.

СР1.4 Подбор материала и создание презентации по теме: Защита баз данных в организации

В методических рекомендациях по выполнению самостоятельной работы студентов указаны цели, количество отведенного на них времени, содержание работы и критерии оценки.