

|  |
| --- |
| Рассмотрены на заседании ПЦК  Протокол № \_1\_\_\_ от «\_\_31\_\_» \_08\_ 20\_16\_ г.  Председатель ПЦК \_\_\_\_\_\_\_\_\_Н.В.Селиванова |

**КОМПЛЕКТ**

**ОЦЕНОЧНЫХ СРЕДСТВ**

**МДК 04.03 Комплексная система защиты информации**

специальность 090905Организация и технология защиты информации

по программе углубленной подготовки

Москва 2016

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

2.6 Комплект вопросов по экзамену

**Паспорт**

**фонда оценочных средств**

**по учебной дисциплине**МДК 04.03 Комплексная система защиты информации

Фонд оценочных средств представляет собой совокупность контрольно-оценочных средств для определения качества освоения студентом учебной дисциплины.

В результате освоения учебной дисциплины обучающийся должен обладать предусмотренными ФГОС по специальности следующими умениями и знаниями:

-про­во­дить ана­лиз и оцен­ку ме­ха­низ­мов за­щи­ты (У1);

-оп­ре­де­лять эф­фек­тив­ность сис­те­мы за­щи­ты ин­фор­ма­ции и уча­ст­во­вать в ее оцен­ке (У2);

-уча­ст­во­вать в раз­ра­бот­ке пред­ло­же­ний по со­вер­шен­ст­во­ва­нию и по­вы­ше­нию эф­фек­тив­но­сти ме­ро­прия­тий по ком­плекс­ной сис­те­ме за­щи­те объ­ек­та (У3);

-на­зна­че­ние ком­плекс­ной сис­те­мы за­щи­ты ин­фор­ма­ции, прин­ци­пы ее ор­га­ни­за­ции и эта­пы раз­ра­бот­ки, клас­си­фи­ка­цию и струк­ту­ру ком­плекс­ных сис­тем за­щи­ты ин­фор­ма­ции (З1);

-тех­но­ло­ги­че­ское и ор­га­ни­за­ци­он­ное по­строе­ние ком­плекс­ных сис­тем за­щи­ты ин­фор­ма­ции (З2);

-тре­бо­ва­ния к сис­те­мам ком­плекс­ной за­щи­ты ин­фор­ма­ции (З3).

Формой аттестации по учебной дисциплине является**экзамен**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Контролируемые умения, знания | Контролируемые разделы (темы) учебной дисциплины | Наименование  оценочного средства |
|  |  | **Раздел 3. Участие в планировании и организации работ по обеспечению защиты объекта** |  |
|  |  | Ввeдeниe |  |
|  | У1, З1 | **Тема 3.1**Сущность и задачи комплексной защиты информации | СР1.1, 1СР 1.3  ПЗ 1, ПЗ 2 |
|  | У1, З1 | **Тема 3.2** Принципы организации и этапы разработки КСЗИ | СР 1.2 СР 1.3  ПЗ 3, ПЗ 4 |
|  | У3, З3 | **Тема 3.3** Факторы, влияющие на организацию КСЗИ | СР 1.2 СР 1.4  ПЗ 5 |
|  | У1, З3 | **Тема 3.4** Определение и нормативное закрепление состава защищаемой информации | СР 1.1 СР 1.3  ПЗ 6 |
|  | У2, З1 | **Тема 3.5.** Определение объектов защиты | СР 1.1 СР 1.3 СР 1.5  ПЗ 7 |
|  | У3, З2 | **Тема 3.6.** Дестабилизирующие воздействия на информацию и их нейтрализация | СР 1.1 СР 1.3 СР 1.6  ПЗ 8 ПЗ 9 |
|  | У1, З1 | **Тема 3.7.** Определение потенциальных каналов и методов несанкционированного доступа к информации | СР 1.6 |
|  | З2 | **Тема 3.8** Определение возможности несанкционированного доступа к защищаемой информации | СР 1.2 СР 1.6  ПЗ 10 |
|  |  | **ЗАЧЕТ** | Тесты |
|  | У2, З2 | **Тема 3.9.** Определение компонентов КСЗИ | СР 2.1 СР 2.2 СР 2.6  ПЗ 11, ПЗ 12 |
|  | У1, З3 | **Тема 3.10** Определение условий функционирования КСЗИ | СР 2.1 СР 2.2 СР 2.5  ПЗ 13 |
|  | У3, З2 | **Тема 3.11** Разработка модели КСЗИ | СР 2.2 СР 2.3 СР 2.4 СР 2.5 СР 2.1  ПЗ 14 |
|  | З2 | **Тема 3.12** Технологическое и организационное построение КСЗИ | СР 2.1 СР 2.2 СР 2.5  ПЗ 14 |
|  | У3, З1 | **Тема 3.13** Кадровое обеспечение функционирования комплексной системы защиты информации | СР 2.2 СР 2.3 СР 2.5 |
|  |  | **Курсовая работа:** | СР 2.6 |
|  |  | ЭКЗАМЕН |  |

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

Приложение 1

**КОМПЛЕКТ ТЕСТОВ**

Учебная дисциплина МДК 04.03 Комплексная система защиты информации

Специальность 090905 Организация и технология защиты информации

КОНТРОЛИРУЕМЫЕ ПАРАМЕТРЫ

|  |  |
| --- | --- |
| Темы | Номера тестовых заданий |
| **Тема 3.1**Сущность и задачи комплексной защиты информации | 1,3 |
| **Тема 3.2**Принципы организации и этапы разработки КСЗИ | 2 |
| **Тема 3.3** Факторы, влияющие на организацию КСЗИ | 3,4 |
| **Тема 3.4**Определение и нормативное закрепление состава защищаемой информации | 5 |
| **Тема 3.5.** Определение объектов защиты | 6,7 |
| **Тема 3.6.**Дестабилизирующие воздействия на информацию и их нейтрализация | 8 |
| **Тема 3.7.**Определение потенциальных каналов и методов несанкционированного доступа к информации | 9 |
| **Тема 3.8**Определение возможности несанкционированного доступа к защищаемой информации | 10 |
| **Тема 3.9.** Определение компонентов КСЗИ | 11,12 |
| **Тема 3.10**Определение условий функционирования КСЗИ | 13,14 |
| **Тема 3.11**Разработка модели КСЗИ | 15 |
| **Тема 3.12** Технологическое и организационное построение КСЗИ | 16 |
| **Тема 3.13**Кадровое обеспечение функционирования комплексной системы защиты информации | 17,18,19,20 |

Критерии оценки:

|  |  |  |
| --- | --- | --- |
| Количество правильных ответов | Процент выполнения | Оценка |
|  | более 90% | Отлично |
|  | 80-90% | Хорошо |
|  | 60-79% | Удовлетворительно |
|  | менее 60% | Неудовлетворительно |

ТЕСТОВЫЕ ЗАДАНИЯ

|  |  |  |
| --- | --- | --- |
| **№ п/п**  **вопросов тестового задания** | **Содержание**  **тестового задания** | **Варианты ответов** |
| 1 | 2 | 3 |
| 1 | Главной целью КСЗИ является: | А) Предотвращение внешних и внутренних угроз;  **Б) Обеспечение непрерывности бизнеса, устойчивого**  **функционирования коммерческого предприятия и предотвращения угроз ее безопасности;**  В) Предотвращение несанкционированного доступа. |
| 2 | Создание СУИБ должно базироваться на: | А) Системе информационной безопасности;  Б) Управление безопасности предприятия;  **В) Требования и рекомендации нормативных и правовых актов.** |
| 3 | Аббревиатура КСЗИ означает: | А) Комплекс средств защиты информации;  **Б) Комплексная система защиты информации;**  В) Координирующая структура защиты информации. |
| 4 | Нарушения системы кондиционирования повлияет на: | **А) Целостность информации;**  Б) Конфиденциальность организации  **В) Работоспособность предприятия.**  **Г) Целостность и доступность активов ИТ.** |
| 5 | Установите соответствие:  **1. Международная сертификация**  *2. Международная стандартизация*  3. Стандартизация и сертификация в банковской сфере РФ | *А) Политика безопасности, организация ИБ, управление активами;*  **Б) Создание СУИБ, внедрение и эксплуатация СУИБ;**  В) Проверка и оценка ИБ, парадигма обеспечения ИБ. |
| 1 | 2 | 3 |
| 6 | Установите соответствие:   1. **Доступность** 2. *Целостность данных* 3. Целостность информации | *А) Способность данных не подвергаться изменению или аннулированию в результате несанкционированного доступа;*  Б) Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного или преднамеренного искажения;  **В) Такое состояние информации, когда она находится в виде и месте, необходимом пользователю, и в то время когда она необходима.** |
| 7 | Все разработанные документы должны определять работу КСЗИ: | А) В штатном режиме;  Б) При изменениях в штатном режиме;  **В) В нештатном режиме (аварийных ситуациях) удалить.** |
| 8 | Тактическое планирование – это: | **A. Среднесрочное планирование;** B. Долгосрочное планирование; C. Ежедневное планирование; D. Планирование на 6 месяцев. |
| 9 | Установите соответствие:  **1. Стратегия**  *2. Результаты операции*  3. Целевой эффект операции  4. Ресурсы | *А) Совокупность всех ее эффектов (последствий);*  Б) Запасы материи, энергии, информации времени;  **В) Определенная организация и способ проведения организации;**  Г) Результат, ради получения  которого проводится операция. |
| 10 | Важным фактором, влияющим на организацию КСЗИ, является: | А) Иностранная собственность;  Б) Российская собственность;  **В) Форма собственности предприятия.** |
| 11 | Средства защиты от утечки информации по техническим каналам можно разделить на две группы: | **А) Группа защищает от утечек компьютерной информации по каналам ПЭМИН, административная;**  **Б) Защищает от утечки речевой информации по виброакустическим каналам.** |
| 1 | 2 | 3 |
| 12 | В плане защиты информации территориальное расположение предприятий можно классифицировать по условиям функционирования КСЗИ, оценивая их как: | **А) Благоприятные;**  **Б) Обычные;**  **В) Особенные;**  Г) Не благоприятные. |
| 13 | Вставьте недостающий источник дестабилизирующего воздействия на информацию: | 1. Люди  2**. Природные явления**  3. Системы обеспечения функционирования технических средств отображения, хранения,  обработки, воспроизведения и передачи информации  4 Технологические процессы отдельных категорий промышленных объектов.  **5. Технические средства отображения (фиксации), хранения, обработки, воспроизведения, передачи информации** |
| 14 | Установите соответствие:  **1) Государственная тайна**  *2) Коммерческая тайна*  3) Служебная тайна | *А) Конфиденциальная информация, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы;*  Б) Сведения, доступ к которым ограничен органом государственной власти;  **В) Защищаемые сведения в области его военной, внешнеполитической, экономической.** |
| 15 | Установите соответствие: **1.5485-I ФЗ** *2. 98 - ФЗ*  3. 124871-4 ФЗ  4. 152- ФЗ | *А) « О коммерческой тайне»;*  Б) « О служебной тайне»;  **В) « О государственной тайне»;**  Г) « О персональных данных». |
| 1 | 2 | 3 |
| 16 | Угроза безопасности информации – это: | **А) Совокупность условий и факторов, создающих потенциальную или реальную существующую опасность, связанная с утечкой информации;**  Б) Анализ мер и средств обеспечения безопасности и идентификация уязвимостей;  В) Меры для компаний - производителей СЗИ, занимающихся, кроме того, и разработкой законченных проектов в области безопасности. |
| 17 | Что является определением воздействия (exposure) на безопасность? | **A. Нечто, приводящее к ущербу от угрозы;**  B. Любая потенциальная опасность для информации или систем; C. Любой недостаток или отсутствие информационной безопасности; D. Потенциальные потери от угрозы. |
| 18 | Напишите наименование каналов утечки информации: | **А) Акустически**  **Б) Вибрационный**  **В) Электроакустический**  **Г) ПЭМИН** |
| 19 | Установите соответствие:  **1.Организационное резервирование**  *2. Техническое резервирование*  3. Информационное резервирование | А) Заключается в создании резервных копий информационных  ресурсов;  *Б) Заключается в приобретении дополнительной техники, либо в*  *неполном использование ресурсов существующих;*  **В) Подразумевает распределение задач между работниками**  **предприятия таким образом, что в случае невозможности выполнять одним из работников**  **работу, ее бы могли выполнить другие.** |
| 20 | Способы несанкционированного доступа: | **А) Инициативное сотрудничество;**  **Б) Подслушивание;**  **В) Копирование, фотографирование**  **Г) Склонение к сотрудничеству** |

Рассмотрены на заседании ПЦК …

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

Председатель ПЦК \_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.О. Фамилии

Приложение 2

**Перечень лабораторных работ и практических занятий:**

ПЗ 1.Анализ Международных стандартов КЗИ

ПЗ 2.Анализ экономической эффективности

ПЗ 3Разработка этапов КСЗИ

ПЗ 4 Разработка политики безопасности и регламента безопасности предприятия

ПЗ 5 Создание структуры и территориальное расположение предприятия

ПЗ 6 Определение состава защищаемой информации

ПЗ 7 Анализ факторов, определяющие необходимость защиты периметры и здания предприятия

ПЗ 8 Выявление угрозы безопасности информации

ПЗ 9 Обеспечение безопасности информации в непредвиденных ситуациях

ПЗ 10 Определение возможности несанкционированного доступа к защищаемой информации

ПЗ 11 Определение компонентов КСЗИ

ПЗ 12 Определение важности параметров средств защиты информации

ПЗ 13 Определение основные угрозы безопасности информации

ПЗ 14 Анализ формального построения модели защиты

ПЗ 15 Работа с вопросами и тестами для самопроверки

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 3.1**Сущность и задачи комплексной защиты информации | 1-6 |
| **Тема 3.2**Принципы организации и этапы разработки КСЗИ | 7-15 |
| **Тема 3.3** Факторы, влияющие на организацию КСЗИ | 15-19 |
| **Тема 3.4**Определение и нормативное закрепление состава защищаемой информации | 19-21 |
| **Тема 3.5.** Определение объектов защиты | 21-24 |
| **Тема 3.6.**Дестабилизирующие воздействия на информацию и их нейтрализация | 25-30 |
| **Тема 3.7.**Определение потенциальных каналов и методов несанкционированного доступа к информации | 31-32 |
| **Тема 3.8**Определение возможности несанкционированного доступа к защищаемой информации | 33-39 |
| **Тема 3.9.** Определение компонентов КСЗИ | 40-43 |
| **Тема 3.10**Определение условий функционирования КСЗИ | 44-45 |
| **Тема 3.11**Разработка модели КСЗИ | 46 |
| **Тема 3.12** Технологическое и организационное построение КСЗИ | 47-48 |
| **Тема 3.13**Кадровое обеспечение функционирования комплексной системы защиты информации | 49-50 |

ПЕРЕЧЕНЬ ВОПРОСОВ

1. Главной целью КСЗИ является
2. Задачи КСЗИ
3. КСЗИ направлена на
4. На каких принципах должно основываться обеспечение безопасности предприятия
5. Перечислите основные требования к КСЗМ в АС
6. Что понимается под безопасностью ИТ
7. Перечислите три направления работ по созданию КСЗИ
8. Что такое политика безопасности
9. В каких режимах разработанные документы должны определять работу КСЗИ
10. Что такое сложная система КСЗИ
11. Какие типы устройств ввода информации вы знаете
12. Что такое задача системы
13. Что представляет собой целевой эффект операции
14. Перечислите основные направления деятельности СУИБ
15. Что является основными этапами работ по созданию КСЗИ
16. Какой важный фактор влияет на организацию КСЗИ
17. Назовите основные особенности ЗИ в зависимости от состава ЗИ (по видам)
18. Что такое персональные данные
19. В чем заключается принцип защищаемой информации
20. Какие бывают основные источники ЗИ
21. Что относится к источникам ЗИ
22. На какие три зоны по доступности разделены помещения предприятия
23. Что обозначает первый рубеж охраны
24. Что такое средства обеспечения объекта информатизации
25. На чем отражается подлежащая защита на предприятие
26. Перечислите основные причины утечки информации в АС
27. Что относится к объективным внутренним факторам
28. Что относится к объективным внешним факторам
29. Что такое угроза безопасности информации
30. Какие основные виды нарушения безопасности вы знаете
31. Что такое электрические каналы
32. Перечислите каналы утечек информации
33. За Какие бывают методы защиты данных
34. Что такое локальная аутентификация
35. Какие пароли бывают
36. Что такое разграничение доступа
37. Как используется криптография
38. Приведите пример совместного использования симметричных и асимметричных алгоритмов
39. В чем отличие шлюза сеансового уровня и прикладного уровня
40. Схема методики построения системы защиты АС
41. В чем заключается метод Саати
42. Какие методы измерений вы знаете
43. Чем характеризуется линейная структура
44. Назовите основные разделы концепции
45. Какие угрозы безопасности наиболее опасны
46. Что такое политика безопасности
47. Что обеспечивает КСЗИ
48. Что такое безопасность персонала
49. Какие основные направления работы с персоналом вы знаете
50. Что включает материально – технические обеспечение КСЗИ

Приложение 4

**Перечень самостоятельных работ:**

1.1 Подготовка к ПЗ и их защите

1.2 Подготовка докладов по темам:

Требования, предъявляемые к КСЗИ

- Влияние организационно - правовой формы предприятия на особенности защиты информации ограниченного доступа

- Состав, объекты и степень конфиденциальности защищаемой информации

- Классификация СЗИ НСД

- Разграничение доступа

1.3 Подготовка презентаций по темам:

- Управление безопасностью предприятия. Международные стандарты

- Методологические основы организации

- Нормативно - правовые аспекты определения состава защищаемой информации

- Факторы, определяющие необходимость защиты периметры и здания предприятия

- Модели нарушителей безопасности АС

1.4 Разработка режима функционирования предприятия

1.5 Состав средств обеспечения, подлежащих защите (таблица)

1.6 -Подходы к оценке ущерба от нарушений ИБ (схема)

- Разграничение доступа (схема)

- Технические каналы утечки информации (сравнительный анализ)

1.7 Подготовка к зачету

2.1.Подготовка к практическим занятиям, оформление практических занятий, отчетов и подготовка к их защите;

2.2 Подготовка презентаций по темам:

-Особенности синтеза СЗИ АС от НСД

- Проектирование системы защиты

- Цели и задачи обеспечения безопасности информации

Общее описание архитектуры АС, системы защиты информации и политики безопасности

- Первоочередные мероприятия по обеспечению безопасности информации АС организации

- Формальные модели безопасности и их анализ

- Описание объекта защиты

- Общее содержание работ по организации КСЗИ

- Распределение функций по защите информации

- Функции руководства предприятия

2.3. Подготовка докладов по теме:

- Формализация модели безопасности

- Обязанности пользователей защищаемой информации

2.4. Определение важности параметров средств защиты информации (схема)

- Процедура создания пары субъект-объект, наделение их атрибутами безопасности (обобщающая схема)

2.5. Сравнительный анализ по теме:

-Объекты защиты

- Формальное построение модели защиты: пример

- Предпроектное обследование, технический проект, рабочий проект

- Обеспечение взаимодействия между субъектами, защищающими и использующими информацию ограниченного доступа

2.6.Выполнение этапов КР

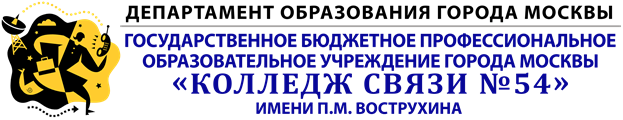
2.7. Подготовка к зачету

2.8. Подготовка к экзамену

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

.

Приложение 5

****

**ВОПРОСЫ К ЭКЗАМЕНУ**

**по МДК 04.03. «Комплексная система защиты информации»**

1.Цели, задачи и принципы построения КСЗИ

2.О понятиях безопасности и защищенности

3.Разумная достаточность и экономическая эффективность

4.Управление безопасностью предприятия. Международные стандарты

5.Цели и задачи защиты информации в автоматизированных системах.

6.Методологические основы организации

7.Разработка политики безопасности и регламента безопасности предприятия

8.Основные положения теории сложных систем

9.Система управления информационной безопасностью предприятия. Принципы построения и взаимодействие с другими пользователями

10.Требования, предъявляемые к КСЗИ

11.Этапы разработки КСЗИ

12.Влияние формы собственности на особенности защиты информации ограниченного доступа

13.Характер основной деятельности предприятия

14.Состав, объекты и степень конфиденциальности защищаемой информации

15.Структура и территориальное расположение предприятия

16.Режим функционирования предприятия

17.Классификация информации по видам тайны и степеням конфиденциальности

18.Нормативно - правовые аспекты определения состава защищаемой информации

19.Значение носителей защищаемой информации как объектов защиты

20.Факторы, определяющие необходимость защиты периметры и здания предприятия

21.Транспортные средства и особенности транспортировки

22.Состав средств обеспечения, подлежащих защите

23.Факторы, создающие угрозу информационной безопасности

24.Угрозы безопасности информации

25.Модели нарушителей безопасности АС

26.Обеспечение безопасности информации в непредвиденных ситуациях

27.Технические каналы утечки информации

28.Задачи КСЗИ по выявлению угроз

29.Особенности защиты речевой информации

30.Методы и способы защиты информации

31.Криптографическая подсистема

32.Межсетевое экранирование

33.Методика синтеза СЗИ

34.Общее описание архитектуры АС, системы защиты информации и политики безопасности

35.Выбор структуры СЗИ АС

36.Проектирование системы защиты информации для существующей АС

37.Содержание концепции построения КСЗИ

38.Цели и задачи обеспечения безопасности информации

39.Основные принципы построения КСЗИ

40.Общая характеристика задач моделирования КСЗИ