**ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ**

**ПО МДК 03.02 Безопасность компьютерных сетей**

**для студентов 4 курса по специальности**

09.02.06 Сетевое и системное администрирование

**Теоретические вопросы:**

1. Понятие информационной безопасности
2. Важность и сложность проблемы информационной безопасности
3. Основные составляющие информационной безопасности
4. Категории информационной безопасности
5. Основные определения и критерии классификации угроз
6. Компьютерные преступления. Основные технологии, использующиеся при совершении компьютерных преступлений.
7. Объекты защиты информации. Защита информации ограниченного доступа: государственная тайна, коммерческая тайна
8. Правовые средства защиты
9. Причины, виды и каналы утечки информации.
10. Классификация криптоалгоритмов
11. Симметричные криптосистемы
12. Асимметричные криптосистемы.
13. Обзор и классификация методов шифрования информации

### Цифровая подпись

1. \*Аутенфикация и индефикация
2. \*Протоколы аутентификации
3. Биометрическая аутенфикация
4. Компьютерные вирусы

### Структура и классификация компьютерных вирусов

1. Механизмы вирусной атаки
2. Антивирусные программы
3. Профилактические мероприятия для защиты компьютерных сетей от вредоносного ПО
4. Защита данных в автономном компьютере.
5. ПО и информационная безопасность
6. \*Резервное копирование
7. Проблема защиты электронной информации.
8. Место программно-математических методов в комплексной системе защиты информации.
9. Классификация угроз безопасности информации и возможные методы зашиты.
10. Резервное копирование данных: суть, устройства для хранения копии, рекомендации по резервному копированию.
11. Общий обзор программного обеспечения для профилактического обслуживания носителей информации и восстановления данных.
12. Эффектные меры, повышающие шансы восстановления информации на магнитных носителях.
13. Защита локального компьютера паролем включения: суть, алгоритм настройки, способы преодоления защиты.
14. Загрузка локального компьютера с использованием оригинальной дискеты: суть, программный пример, способы преодоления защиты.
15. Защита локального компьютера паролем заставки экрана, суть, алгоритм настройки, способы преодоления защиты.
16. Защита информации скрытием файлов и папок, изменением имени и расширения, атрибутом «только для чтения»: алгоритмы настройки, способы преодоления защиты.
17. MS Office: алгоритмы защиты документов от несанкционированного доступа и использования. Правила задания пароля. Способы преодоления защиты.
18. Особенности строения файлов текстовых процессоров. Алгоритмы уничтожения удалённого и исправленного текста в теле файла текстового процессора.
19. Применение программ-архиваторов для скрытия и защиты файлов. Правила задания пароля. Способы преодоления защиты.
20. Генератор паролей, алгоритмы генерации. Оценка стойкости пароля.
21. Временные файлы, причины появления временных файлов. Удаление временных файлов программными методами и вкруговую.
22. Программное обеспечение для полного уничтожения удалённых файлов. Алгоритмы работы программ.
23. Алгоритмы настройки защиты дисков, папок, файлов в локальной сети. ПО для защиты компьютера от проникновения из внешней среды. Суть работы программ....
24. Электронная почта: алгоритм отправки сообщении, возможность перехвата, способы защиты. Отправка анонимных сообщении.
25. Опасность программ-апплетов Java, JavaScript. ActiveX. Алгоритмы настроим защиты браузеров. Опасность файлов «cookie». Методы контроле записи файлов «cookie» на жесткий диск.
26. \*Принцип работы прокси-сервера. Безопасные узлы. алгоритмы проверки безопасности.
27. Классификация компьютерных вирусов с позиции программно-математических методов, краткая характеристика каждого вида. Общие признаки заражения. Файловые вирусы: краткая характеристика перезаписывающего и паразитного вирусов
28. Файловые вирусы: наиболее общий алгоритм работы, алгоритм обнаружения вирусов, возможность восстановления файлов.
29. Загрузочный вирус, алгоритм получения управления вирусом. Алгоритмы предотвращения заражения, обнаружения заражения, удаления вируса.
30. Макровирусы, принципы устройства и функционирования. Алгоритмы обнаружения вирусов и обезвреживания файлов.
31. Вирусы, передающиеся по сети (сетевые, HTML-вирусы, вирусы-апплеты, троянские кони) и способы защиты от них.
32. Резидентные вирусы: краткая характеристика алгоритмов работы.
33. Резидентные вирусы, обнаружение и обезвреживание, возможность восстановления файлов.
34. Последовательность действий при обнаружении заражения вирусом. Правила предотвращения заражения вирусом

**Практические вопросы:**

1. Необходимо сохранить резервную копию документов не на физическом носителе. Создайте резервную копию 2 документов из папки в «облачном пространстве» на «яндекс диске».
2. Необходимо сохранить резервную копию документов не на физическом носителе. Создайте резервную копию 2 документов из папки в «облачном пространстве» на «mega.co».
3. Необходимо сохранить резервную копию документов не на физическом носителе. Создайте резервную копию 2 документов из папки в «облачном пространстве» на «Mail.ru».
4. \*Придумайте новую концепцию обеспечения информационной безопасности предприятия с заданными условиями:

А. На персональных компьютерах хранится секретная информация

Б. Предприятие готово использовать любые финансовые вложения для обеспечения своей информационной безопасности.

1. Используя средства криптографической защиты зашифровать системой шифрования Цезаря свою фамилию, имя, отчество.
2. Используя средства криптографической защиты зашифровать алгоритмом двойных перестановок свою фамилию, имя, отчество.
3. Используя средства криптографической защиты используя шифр перестановки зашифровать название своей специальности и название изучаемого модуля.
4. Используя средства криптографической защиты зашифровать системой шифрования Цезаря название своей специальности и название изучаемого модуля.
5. Используя средства криптографической защиты зашифровать алгоритмом двойных перестановок название своей специальности и название изучаемого модуля.
6. Используя средства криптографической защиты используя шифр перестановки зашифровать название своей специальности и название изучаемого модуля.
7. \*Используя программное обеспечение TrueCrypt зашифровать файл, который содержит названия 3 антивирусных программ
8. Используя программное обеспечение TrueCrypt зашифровать файл, который содержит информацию о вредоносных программах
9. \*Придумайте новую концепцию обеспечения информационной безопасности предприятия с заданными условиями:

А. На персональных компьютерах хранится важная информация

Б. Пользователи имеют неограниченный доступ в интернет

В. Пользователи не имеют достаточной подготовки для работы с персональными компьютерами.

**СПИСОК ЛИТЕРАТУРЫ И ИСТОЧНИКОВ**

**Основная:**

1. Т.Л. Партыка. И.И. Попов, Информационная безопасность, Москва, ИД «Форум», ИНФРА-М, 2012
2. Мельников В.П., Клейменов С.А., Петраков А.М., Информационная безопасность: учебное пособие для сред. проф. Образования, Москва, «Академия», 2011
3. Аверченков В.И., Аудит информационной безопасности, Флинта, 2011
4. Бабаш А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие, Москва, КноРус, 2013

**Дополнительная:**

1. Гафнер В.В., Информационная безопасность: Учебное пособие, Феникс, 2010
2. Громов Ю.Ю., Информационная безопасность и защита информации: Учебное пособие, Ст. Оскол, ТНТ, 2010
3. Ефримова Л.Л, Информационная безопасность детей. Российский и зарубежный опыт: Монография, Москва, ЮНИТИДАНА, 2013
4. Партыка Т.Л, Информационная безопасность: Учебное пособие, Москва, «ФОРУМ», 2012
5. Шаньгин В.Ф., Информационная безопасность компьютерных систем и сетей: Учебное пособие, Москва, «ФОРУМ», 2013
6. Партыка Т.Л., Попов И.И. Операционные системы, среды и оболочки: учебное пособие. – М.: ФОРУМ: ИНФРА-М, 2014. – 400с
7. Степаненко О.С. Настройки персонального компьютера. Установки BIOS. : самоучитель. - М.: Изд. дом «Вильямс», 2011. – 336 с.
8. Костырев М.Л., Абрамов Н.В., Ганичкин О.В., Мотовиов Н.В., Мягков Ф.Н.:Учебное пособие. Самара: Самар. гос.тех ун-т. 2012-112с.