Приложение

Министерство образования и науки Российской Федерации
Муромский институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»**

Кафедра ИС

УТВЕРЖДАЮ
Заведующий кафедрой ИС

подпись Андрианов Д. Е.
инициалы, фамилия

«24» 05 2016 г.

Основание:
решение кафедры ИС
от «24» 05 2016 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИЗУЧЕНИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность
наименование дисциплины

09.03.03 Прикладная информатика
код и наименование направления подготовки

_____
наименование профиля подготовки

бакалавриат
уровень высшего образования

Муром, 2016 г.

ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств (ФОС) для текущего контроля успеваемости и промежуточной аттестации по дисциплине «Информационная безопасность» разработан в соответствии с рабочей программой, входящей в ОПОП направления подготовки 09.03.03 Прикладная информатика.

№№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Введение. Основы информационной безопасности	ОПК-4	тест
2	Принципы криптографической защиты информации	ОПК-4	тест
3	Современные симметричные криптосистемы	ОПК-4	тест
4	Асимметричные криптосистемы	ОПК-4	тест
5	Идентификация и проверка подлинности	ОПК-4	тест
6	Электронная цифровая подпись	ОПК-4	тест
7	Управление криптографическими ключами	ОПК-4	тест
8	Резервное хранение информации. RAID-массивы	ОПК-4	тест
9	Биометрические методы защиты	ОПК-4	тест
10	Защита от копирования	ОПК-4	тест
11	Сетевая защита	ОПК-4	тест

Фонд оценочных средств по дисциплине «Информационная безопасность» предназначен для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям образовательной программы, в том числе рабочей программы дисциплины «Информационная безопасность», для оценивания результатов обучения: знаний, умений, владений и уровня приобретенных компетенций.

Фонд оценочных средств по дисциплине «Информационная безопасность» включает:

1. Оценочные средства для проведения текущего контроля успеваемости:

- комплект заданий репродуктивного уровня для выполнения на лабораторных занятиях, позволяющих оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, распознавание объектов изучения в рамках определенного раздела дисциплины;

- тесты как система стандартизированных знаний, позволяющая провести процедуру измерения уровня знаний и умений обучающихся

2. Оценочные средства для проведения промежуточной аттестации в форме:
- итогового теста для проведения зачета;
- итогового теста для проведения экзамена.

Перечень компетенций, формируемых в процессе изучения дисциплины «Информационная безопасность» при освоении образовательной программы по направлению подготовки 09.03.03 Прикладная информатика:

ОПК-4: способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		
Знать	***Уметь***	***Владеть***
Виды угроз информационных систем и методы обеспечения информационной безопасности	Проводить оценку работоспособности программного продукта Создавать резервные копии программ и данных, выполнять восстановление, обеспечивать целостность программного продукта и данных Осуществлять криптографическую защиту данных	-

В результате освоения дисциплины «Информационная безопасность» завершается освоение компетенции ОПК-4: способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Показатели, критерии и шкала оценивания компетенций текущего контроля знаний по учебной дисциплине «Информационная безопасность»

Текущий контроль знаний, согласно положению о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся (далее Положение) в рамках изучения дисциплины «Информационная безопасность» предполагает тестирование и выполнение заданий по лабораторным работам.

Регламент проведения и оценивание тестирования студентов

В целях закрепления практического материала и углубления теоретических знаний по разделам дисциплины «Информационная безопасность» предполагается выполнение тестирования студентов, что позволяет углубить процесс познания, раскрыть понимание прикладной значимости осваиваемой дисциплины.

Регламент проведения мероприятия

№	Вид работы	Продолжительность
1.	Объяснение правил прохождения теста	5 мин.
2.	Прохождение теста	60 мин.
3.	Оценка результатов тестирования	5 мин.
	Итого (в расчете на тест)	70 мин.

Критерии оценки тестирования студентов

Оценка выполнения тестов	**Критерии оценки**
1 балл за правильный ответ на 1 вопрос	*правильно выбранный вариант ответа (в случае закрытого теста),* *правильно вписанный ответ (в случае открытого теста)*

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ <u>ТЕКУЩЕГО</u> КОНТРОЛЯ ЗНАНИЙ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ «Информационная безопасность»

Семестр 7

Рейтинг-контроль №1.

Блок ЗНАТЬ

1. Кто является основным ответственным за определение уровня классификации информации?

- Руководитель среднего звена
- Высшее руководство
- Владелец
- Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

-Сотрудники
- Хакеры
- Атакующие
-Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

- Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
- Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
- Улучшить контроль за безопасностью этой информации
- Снизить уровень классификации этой информации

4. Что самое главное должно продумать руководство при классификации данных?

A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

B. Необходимый уровень доступности, целостности и конфиденциальности

C. Оценить уровень риска и отменить контрмеры

D. Управление доступом, которое должно защищать данные

5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

A. Владельцы данных

B. Пользователи

C. Администраторы

D. Руководство

6. Что такое процедура?

A. Правила использования программного и аппаратного обеспечения в компании

B. Пошаговая инструкция по выполнению задачи

C. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

D. Обязательные действия

7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

A. Поддержка высшего руководства

B. Эффективные защитные меры и методы их внедрения

C. Актуальные и адекватные политики и процедуры безопасности

D. Проведение тренингов по безопасности для всех сотрудников

8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

A. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски

B. Когда риски не могут быть приняты во внимание по политическим соображениям

C. Когда необходимые защитные меры слишком сложны

D. Когда стоимость контрмер превышает ценность актива и потенциальные потери

9. Что такое политики безопасности?

A. Пошаговые инструкции по выполнению задач безопасности

B. Общие руководящие требования по достижению определенного уровня безопасности

C. Широкие, высокоуровневые заявления руководства

D. Детализированные документы по обработке инцидентов безопасности

10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

A. Анализ рисков

B. Анализ затрат / выгоды

C. Результаты ALE

D. Выявление уязвимостей и угроз, являющихся причиной риска

11. Что лучше всего описывает цель расчета ALE?

A. Количественно оценить уровень безопасности среды

B. Оценить возможные потери для каждой контрмеры

C. Количественно оценить затраты / выгоды

D. Оценить потенциальные потери от угрозы в год

12. Тактическое планирование – это:

A. Среднесрочное планирование

B. Долгосрочное планирование

C. Ежедневное планирование

D. Планирование на 6 месяцев

13. 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

14. Эффективная программа безопасности требует сбалансированного применения:

A. Технических и нетехнических методов

B. Контрмер и защитных механизмов

C. Физической безопасности и технических средств защиты

D. Процедур безопасности и шифрования

15. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

A. Внедрение управления механизмами безопасности

B. Классификацию данных после внедрения механизмов безопасности

C. Уровень доверия, обеспечиваемый механизмом безопасности

D. Соотношение затрат / выгод

16. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

A. Только военные имеют настоящую безопасность

B. Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности

C. Военным требуется больший уровень безопасности, т.к. их риски существенно выше

D. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

17. Как рассчитать остаточный риск?

A. Угрозы x Риски x Ценность актива

B. (Угрозы x Ценность актива x Уязвимости) x Риски

C. SLE x Частоту = ALE

D. (Угрозы x Уязвимости x Ценность актива) x Недостаток контроля

18. Что из перечисленного не является целью проведения анализа рисков?

A. Делегирование полномочий

B. Количественная оценка воздействия потенциальных угроз

C. Выявление рисков

D. Определение баланса между воздействием риска и стоимостью необходимых контрмер

19. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

A. Поддержка

B. Выполнение анализа рисков

C. Определение цели и границ

D. Делегирование полномочий

20. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

A. Чтобы убедиться, что проводится справедливая оценка

B. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ

C. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа

D. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

21. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:

1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

22. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:

1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

23. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:

1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

24. Защита информации от утечки это деятельность по предотвращению:

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию,

блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

25 Защита информации это:

1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

26 Естественные угрозы безопасности информации вызваны:

1. деятельностью человека;

2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;

4. корыстными устремлениями злоумышленников;

5. ошибками при действиях персонала.

27 Искусственные угрозы безопасности информации вызваны:

1. деятельностью человека;

2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;

4. корыстными устремлениями злоумышленников;

5. ошибками при действиях персонала.

28 К основным непреднамеренным искусственным угрозам АСОИ относится:

1. физическое разрушение системы путем взрыва, поджога и т.п.;

2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;

3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

5. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов

системы.

29. К посторонним лицам нарушителям информационной безопасности относится:

1. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
2. персонал, обслуживающий технические средства;
3. технический персонал, обслуживающий здание;
4. пользователи;
5. сотрудники службы безопасности.
6. представители конкурирующих организаций.
7. лица, нарушившие пропускной режим;

Блок (УМЕТЬ):

1. Что понимают под набором норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации?

А Политика безопасности

Б Законная политика

В Свод правил

Г Стратегия предприятия

2. В каких шифрах в качестве ключа используют таблицы?

А Шифрующие таблицы

Б метод Цезаря

В Магические квадраты

Г Полибианский квадрат

3. Самый первый шифр перестановки?

А Метод скитала

Б метод Цезаря

В Магические квадраты

Г Полибианский квадрат

4. В каком шифре каждая буква заменялась на другую букву того же алфавита по следующему правилу: заменяющая буква определялась путем смещения по алфавиту от исходной буквы на К букв.?

А шифрующие таблицы

Б метод Цезаря

В Магические квадраты

Г Полибианский квадрат

5. Какой шифр основан на подсчете частот появления букв в шифртексте..?

А шифр Трисемуса

Б система омофонов

В алгоритм Вернама

Г гаммирование

6. Какой шифр сложной замены представляет собой модификацию шифра Цезаря числовым ключом?

А Шифр Гронсфельда

Б система омофонов

В алгоритм Вернама

Г гаммирование

7. Какой шифр сложной замены описывается таблицей шифрования, и где ключ шифрования меняется от буквы к букве.?

А шифр Трисемуса

Б система Вижинера

В алгоритм Вернама

Г гаммирование

8. Какой шифр является абсолютно надежным?

А шифр Трисемуса

Б одноразовая система шифрования

В алгоритм Вернама

Г гаммирование

9. Какой шифр является в сущности частным случаем системы шифрования Вижинера при значении модуля m = 2.?

А шифр Трисемуса

Б одноразовая система шифрования

В алгоритм Вернама

Г гаммирование

10. Псевдослучайная последовательность, выработанная по заданному алгоритму для зашифрования открытых данных и расшифрования зашифрованных данных это?

А альфа шифра

Б бета шифра

В гамма шифра

Г лямбда шифра

11. Псевдослучайная последовательность, выработанная по заданному алгоритму для зашифрования открытых данных и расшифрования зашифрованных данных это?

А альфа шифра

Б бета шифра

В гамма шифра

Г лямбда шифра

Рейтинг-контроль №2. Блок ЗНАТЬ

1. К посторонним лицам нарушителям информационной безопасности относится:

- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;

-персонал, обслуживающий технические средства;

-технический персонал, обслуживающий здание;

-пользователи;

-сотрудники службы безопасности.

- представители конкурирующих организаций.

- лица, нарушившие пропускной режим;

2. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

3. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

4. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

5. Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

6. Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

7 . Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

8. Активный перехват информации это перехват, который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;

3. неправомерно использует технологические отходы информационного процесса;

4. осуществляется путем использования оптической техники;

5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

9. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

10. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;

5.просмотр мусора.

11 . Перехват, который осуществляется путем использования оптической техники называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

12. К внутренним нарушителям информационной безопасности относится:

1. клиенты;
2. пользователи системы;
3. посетители;
4. любые лица, находящиеся внутри контролируемой территории;
5. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.
6. персонал, обслуживающий технические средства.
7. сотрудники отделов разработки и сопровождения ПО;
8. технический персонал, обслуживающий здание

12. Как называется умышленно искаженная информация?

- Дезинформация
- Информативный поток
- Достоверная информация
- Перестает быть информацией

13. Как называется информация, к которой ограничен доступ?

- Конфиденциальная

- Противозаконная
- Открытая
- Недоступная

14. Какими путями может быть получена информация?

-проведением, покупкой и противоправным добыванием информации научных исследований

- захватом и взломом ПК информации научных исследований
- добыванием информации из внешних источников и скремблированием информации научных исследовании
- захватом и взломом защитной системы для информации научных исследований

15. Как называются компьютерные системы, в которых обеспечивается безопасность информации?

- защищенные КС
- небезопасные КС
- Само достаточные КС
- Саморегулирующиеся КС

16. Основной документ, на основе которого проводится политика информационной безопасности?

- программа информационной безопасности
- регламент информационной безопасности
- политическая информационная безопасность
- Протекторат

17. В зависимости от формы представления информация может быть разделена на?

- Речевую, документированную и телекоммуникационную
- Мысль, слово и речь
- цифровая, звуковая и тайная
- цифровая, звуковая

18. К каким процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации

- Информационным процессам
- Мыслительным процессам
- Машинным процессам
- Микропроцессам

19. Что называют защитой информации?

- Все ответы верны
- Называют деятельность по предотвращению утечки защищаемой информации
- Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
- Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию

20. Под непреднамеренным воздействием на защищаемую информацию понимают?

- Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений

- Процесс ее преобразования, при котором содержание информации изменяется на ложную

- Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию

- Не ограничения доступа в отдельные отрасли экономики или на конкретные производства

21. Шифрование информации это

- Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов

- Процесс преобразования, при котором информация удаляется

- Процесс ее преобразования, при котором содержание информации изменяется на ложную

- Процесс преобразования информации в машинный код

22. Основные предметные направления Защиты Информации?

- охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности

- Охрана золотого фонда страны

- Определение ценности информации

- Усовершенствование скорости передачи информации

23. Государственная тайна это

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны

- ограничения доступа в отдельные отрасли экономики или на конкретные производства

- защищаемые банками и иными кредитными организациями сведения о банковских операциях

- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

24. Коммерческая тайна это….

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны

- ограничения доступа в отдельные отрасли экономики или на конкретные производства

- защищаемые банками и иными кредитными организациями сведения о банковских операциях

- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

25. Банковская тайна это….

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и

оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны

- ограничения доступа в отдельные отрасли экономики или на конкретные производства

- защищаемые банками и иными кредитными организациями сведения о банковских операциях

- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

26. Профессиональная тайна

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны

- ограничения доступа в отдельные отрасли экономики или на конкретные производства

- защищаемые банками и иными кредитными организациями сведения о банковских операциях

- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

27. К основным объектам банковской тайны относятся следующие:

- Все ответы верны

- Тайна банковского счета

- Тайна операций по банковскому счету

- Тайна банковского вклада

28. Как называется тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений?

- Тайна связи

- Нотариальная тайна

- Адвокатская тайна

- Тайна страхования

29. Как называются сведения, доверенные нотариусу в связи с совершением нотариальных действий?

- Нотариальная тайна

- Общедоступные сведения

- Нотариальный секрет

- Нотариальное вето

30. Элемент аппаратной защиты, где используется установка источников бесперебойного питания (UPS)?

- защита от сбоев в электропитании

- защита от сбоев серверов, рабочих станций и локальных компьютеров

- защита от сбоев устройств для хранения информации

- защита от утечек информации электромагнитных излучений

31.Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам,

которые на это имеют право

- управление доступом
- конфиденциальность
- аутентичность
- целостность
- доступность

Блок УМЕТЬ:

1. По мнению К. Шеннона, в практических шифрах необходимо использовать два общих принципа:

- рассеивание
- перемешивание
- встряска
- перестановка

2. Ключ какой длины используется в алгоритме DES:

- 56 бит
- 64 бит
- 128 бит
- 32 бит

3. Блок какой длины обрабатывается в алгоритме DES:

- 64 бит
- 56 бит
- 128 бит
- 32 бит

4. Сколько основных итераций в алгоритме DES:

- 16
- 14
- 20
- 8

5. Первым этапом алгоритма DES является:

- начальная перестановка битов исходного блока
- конечная перестановка битов исходного блока
- начальное рассеивание битов исходного блока
- начальная замена битов исходного блока

6. Какая операция используется в алгоритме DES:

- сложение по модулю два
- сложение
- битовая инверсия
- битовое умножение

7. Какая операция используется в алгоритме DES при вычислении ключей:

- сдвиг влево
- сдвиг вправо
- битовая инверсия
- битовое умножение

8. Сколько ключей используется в алгоритме DES:

- 16

- 12
- 20
- 32

9. При каком режиме DES длинный файл разбивают на 64-битовые отрезки (блоки) по 8 байтов. Каждый из этих блоков шифруют независимо с ис¬пользованием одного и того же ключа шифрования?

- электронная кодовая книга ECB (Electronic Code Book);
- сцепление блоков шифра CBC (Cipher Block Chaining);
- обратная связь по шифртексту CFB (Cipher Feed Back);
- обратная связь по выходу OFB (Output Feed Back).

10. При каком режиме DES исходный файл M разбивается на 64-битовые блоки: M = M(1)M(2)...M(n). Первый блок M(1) складывается по модулю 2 с 64-битовым начальным вектором IV, который меняется ежедневно и держится в секрете. Полученная сумма затем шифруется с использованием ключа DES, известного и отправителю, и получателю информации. Полученный 64-битовый блок шифртекста C(1) складывается по модулю 2 со вторым блоком исходного текста, результат шифруется и получается второй 64-битовый блок шифртекста C(2) и т.д.

-электронная кодовая книга ECB (Electronic Code Book);
-сцепление блоков шифра CBC (Cipher Block Chaining);
-обратная связь по шифртексту CFB (Cipher Feed Back);
-обратная связь по выходу OFB (Output Feed Back).

11. При каком режиме DES размер блока может отличаться от 64. Исходный файл M считывается последовательными t-битовыми блоками (t <= 64): M = M(1)M(2)...M(n) (остаток дописывается нулями или пробелами).

-электронная кодовая книга ECB (Electronic Code Book);
- сцепление блоков шифра CBC (Cipher Block Chaining);
- обратная связь по шифртексту CFB (Cipher Feed Back);
- обратная связь по выходу OFB (Output Feed Back).

Рейтинг-контроль №3. Блок ЗНАТЬ

1. Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем

- защита от сбоев в электропитании

защита от сбоев серверов, рабочих станций и локальных компьютеров

- защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

2. Элемент аппаратной защиты, где используется организация надежной и эффективной системы резервного копирования и дублирования данных

- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров

-защита от сбоев устройств для хранения информации

- защита от утечек информации электромагнитных излучений

3. Элемент аппаратной защиты, где используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений.

- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
-защита от утечек информации электромагнитных излучений

4. Какая из перечисленных атак на поток информации является пассивной:
- перехват.
- имитация.
- модификация.
- фальсификация.
- прерывание.

5. К открытым источникам информация относятся.
-Газеты, Радио, Новости
- Информация украденная у спецслужб
- Из вскрытого сейфа
- Украденная из правительственной организации

6. Технические каналы утечки информации делятся на…
- Все перечисленное
- Акустические и виброакустические
- Электрические
- Оптические

7. Какой технический канал утечки отвечает за распространение звуковых колебаний в любом звукопроводящем материале или среде?
- Акустические и виброакустические
- Электрические
- Оптические
- Радиоканалы

8. Какой технический канал утечки отвечает за напряжение и токи в различных токопроводящих коммуникациях?
- Акустические и виброакустические
- Электрические
- Оптические
- Радиоканалы

9. Какой технический канал утечки отвечает за электромагнитные излучения радиодиапазона?
- Акустические и виброакустические
- Электрические
- Оптические
-Радиоканалы

10. Какой технический канал утечки отвечает за электромагнитные излучения в видимой, инфракрасной и ультрафиолетовой частях спектра?
- Акустические и виброакустические
- Электрические
- Оптические
- Радиоканалы

11. Учет всех возможных коммуникационных каналов, обеспечения физической безопасности, шифрования резервных копий и информации, покидающей

корпоративный периметр, и других организационных мероприятий это?

- Индивидуальный подход к защите
- Комплексный подход к защите
- Смешанный подход к защите
- Рациональный подход к защите

12. Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе

- Информационная безопасность
- Защитные технологии
- Заземление
- Конфиденциальность

13. Можно выделить следующие направления мер информационной безопасности

- Правовые
- Организационные
- Все ответы верны
- Технические

14. Что можно отнести к правовым мерам информационной безопасности?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
- охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра итд
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое
- охрану вычислительного центра, установку сигнализации и многое другое

15. Что можно отнести к организационным мерам ИБ?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.
- Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем.
- Охрану работоспособности отдельных звеньев и организацию вычислительных сетей с возможностью перераспределения ресурсов.
- Принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

16. Что можно отнести к техническим мерам ИБ?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства

- Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.

- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев и многое другое

- Простые и доступные меры защиты от хищений, саботажа, диверсий, взрывов

- В административных местах установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

17. Потенциальные угрозы, против которых направлены технические меры защиты информации

- Потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей

- Потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения

- Потери информации из-за не достаточной установки резервных систем электропитании и оснащение помещений замками.

- Потери информации из-за не достаточной установки сигнализации в помещении.

- Процессы преобразования, при котором информация удаляется

Блок УМЕТЬ

1. Блоками какого размера оперирует алгоритм шифрования IDEA?
- 64 бит
- 56 бит
- 128 бит
- 32 бит

2. Сколько итераций цикла использует алгоритм шифрования IDEA?
- 8
- 16
- 5
- 24

3. Ключ какого размера использует алгоритм шифрования IDEA?
- 128 бит
- 56 бит
- 64 бита
- 32 бит

4. Какие режимы использует отечественный стандарт шифрования?
- простая замена;
- гаммирование;

- гаммирование с обратной связью;
- выработка имитовставки.
- Все перечисленные

5. Чем отличаются ассиметричные шифры от симметричных?
- Простотой реализации;
- наличием постоянного ключа
- наличием трех секретных ключей;
- Наличием двух ключей

6. Какая процедура устанавливает, является ли данный объект именно таким, каким он себя объявляет.
- авторизация
- идентификация
-коммутация
-аутентификация

7. Какая процедура устанавливает сферу действия объекта и доступ¬ные ему ресурсы сети?
- авторизация
- идентификация
-коммутация
-аутентификация

8. Для проверки подлинности применяют:
-механизм запроса-ответа;
-механизм отметки времени.
-Механизм ответа-ответа
-Механизм запроса-запроса

9. Какую процедуру используют для взаимной проверки подлинности ?
- «рукопожатия»
-механизм отметки времени.
-Механизм ответа-ответа
-Механизм запроса-запроса

18. Какие сбои оборудования бывают?
- потери при заражении системы компьютерными вирусами
- несанкционированное копирование, уничтожение или подделка информации
- сбои работы серверов, рабочих станций, сетевых карт и тд - ознакомление с конфиденциальной информацией

19.Какие сбои оборудования, при которых теряется информация, бывают?
- случайное уничтожение или изменение данных
- перебои электропитания
- некорректное использование программного и аппаратного обеспечения, ведущее к уничтожению или изменению данных
- несанкционированное копирование, уничтожение или подделка информации

20. Какие потери информации бывают из-за некорректной работы программ?
- сбои работы серверов, рабочих станций, сетевых карт и тд
- перебои электропитания
-потеря или изменение данных при ошибках ПО
- ознакомление с конфиденциальной информацией

21. Какие потери информации бывают из-за некорректной работы программ?

- потери при заражении системы компьютерными вирусами
- сбои дисковых систем
- перебои электропитания
- сбои работы серверов, рабочих станций, сетевых карт и тд

22. Какие потери информации, связанные с несанкционированным доступом, бывают?

- несанкционированное копирование, уничтожение или подделка информации
- потери при заражении системы компьютерными вирусами
- случайное уничтожение или изменение данных
- сбои дисковых систем

23. Потери из-за ошибки персонала и пользователей бывают?

- несанкционированное копирование, уничтожение или подделка информации
- потери при заражении системы компьютерными вирусами
- случайное уничтожение или изменение данных
- сбои дисковых систем

24. Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии?

- установка источников бесперебойного питания (UPS)
- Такого средства не существует
- Каждую минуту сохранять данные
- Перекидывать информацию на носитель, который не зависит от энергии

25. Способ защиты от сбоев процессора?

- установка источников бесперебойного питания (UPS)
- симметричное мультипроцессирование
- Каждую минуту сохранять данные
- Перекидывать информацию на носитель, который не зависит от энергии

Семестр 8.

Рейтинг-контроль №1. Блок ЗНАТЬ

1.Виды защиты БД

-защита паролем, защита пользователем,

- учётная запись группы администратора
- приложение, которое используется для управления базой данных
- группа Users

2.Виды защиты БД

-защита всех учетных записей, защита идентифицированных объектов

- защита учётной записи группы администратора
- приложение, которое используется для управления базой данных
- защита группы Users

3.Наибольшую угрозу для безопасности сети представляют.

- несанкционированный доступ, электронное подслушивание и преднамеренное или неумышленное повреждение
- вскрытие стандартной учётной записи пользователя
- вскрытие стандартной учётной группы администратора
- копирование файлов, которые были изменены в течение дня, без отметки о

резервном копировании

4.Защита через права доступа заключается.

-присвоении каждому пользователю определенного набора прав

-запереть серверы в специальном помещении с ограниченным доступом

-присвоить пароль каждому общедоступному ресурсу

- в наличии преобразователя микрофона

5.Дифференцированное резервное копирование это

-Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании

-Копирование всех выбранных файлов без отметки о резервном копировании

-Копирование и маркировка выбранных файлов, только если они были изменены со времени последнего копирования

-Копирование выбранных файлов, только если они были изменены со времени последнего резервного копирования, без отметки о резервном копировании

6.Полное копирование данных это

-Копирование и маркировка выбранных файлов, вне зависимости от того, изменялись ли они со времени последнего резервного копирования

-Копирование всех выбранных файлов без отметки о резервном копировании

-Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании

-Копирование и маркировка выбранных файлов, только если они были изменены со времени последнего копирования

7.Disk mirroring – это

-дублирование раздела и запись его копии на другом физическом диске

-это пара зеркальных дисков, каждым из которых управляет отдельный контроллер

-При записи данных делится на части и распределяется по серверу

- Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании

БЛОК УМЕТЬ

1.Наиболее распространенный криптографический код

-Код Хэмминга

-код Рида-Соломона

-код Морзе

-итеративный код

2.Помехоустойчивый код характеризуется тройкой чисел

- n,k,d0

-h,k,d0

-a,b,c

-x,y,z

3. Функция технологии RAID 4

-дисковый массив повышенной производительности с чередованием, без отказоустойчивости;

-зарезервирован для массивов, которые применяют код Хемминга

-хранит блок четности на одном физическом диске

-распределяет информацию о четности равномерно по всем дискам

4.Функция технологии RAID 5

-дисковый массив повышенной производительности с чередованием, без отказоустойчивости

-зарезервирован для массивов, которые применяют код Хемминга;

-хранит блок четности на одном физическом диске

-распределяет информацию о четности равномерно по всем дискам

5.Наиболее простой и недорогой метод предотвратить катастрофическую потерю данных

-Резервное копирование на магнитную ленту

-Шифрование данных

-Бездисковые компьютеры

-Все ответы верны

6.Какой способ защиты информации присваивает значение каждому пользователю соответствующие права доступа к каждому ресурсу

- Права группы

-Аудит

-Шифрование данных

-Модели защиты

7.Методы сохранение данных при чрезвычайных ситуаций

-резервное копирование на магнитную ленту;

-источники бесперебойного питания (UPS);

-отказоустойчивые системы

-Все ответы верны

8.Какой способ данные, дублируя и размещая их на различных физических носителях (например, на разных дисках).

-Журнал резервного копирования

-Отказоустойчивые системы

-Метод резервного копирования

-Шифрование данных

9.Disk duplexing это?

-дублирование раздела и запись его копии на другом физическом диске

-это пара зеркальных дисков, каждым из которых управляет отдельный контроллер

-При записи данных делится на части и распределяется по серверу

-Все ответы верны

Рейтинг-контроль №2. Блок ЗНАТЬ

1.Пароль доступа к ресурсам

-Доступ только для чтения

- такой пароль не существует

-Отказоустойчивые системы

-Метод резервного копирования

-Шифрование данных

2.Пароль доступа к ресурсам

- Полный доступ и доступ в зависимости от пароля (

- такой пароль не существует

-Отказоустойчивые системы

-Метод резервного копирования

-Шифрование данных

3.Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии?

- установка источников бесперебойного питания (UPS)

- Такого средства не существует

- Каждую минуту сохранять данные

- Перекидывать информацию на носитель, который не зависит от энергии

4.Ежедневное копирование данных это

-Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании

-Копирование всех выбранных файлов без отметки о резервном копировании

-Копирование и маркировка выбранных файлов, вне зависимости от того, изменялись ли они со времени последнего резервного копирования

-Копирование выбранных файлов, только если они были изменены со времени последнего резервного копирования, без отметки о резервном копировании

5.Способ защиты от сбоев процессора?

- установка источников бесперебойного питания (UPS)

- симметричное мультипроцессирование

- Каждую минуту сохранять данные

- Перекидывать информацию на носитель, который не зависит от энергии

6.Способ защиты от сбоев устройств для хранения информации?

- установка источников бесперебойного питания (UPS)

- симметричное мультипроцессирование

- Каждую минуту сохранять данные

- Организация надежной и эффективной системы резервного копирования и дублирования данных

7.Средства защиты данных, функционирующие в составе программного обеспечения.

- Программные средства защиты информации

- Технические средства защиты информации

- Источники бесперебойного питания (UPS)

- Смешанные средства защиты информации

8.Средством предотвращения потерь информации при кратковременном отключении электроэнергии является?

-источник бесперебойного питания (UPS)

-источник питания

-электро-переключатель

-все перечисленное

9.К наиболее важному элементу аппаратной защиты можно отнести?

- защита от сбоев серверов, рабочих станций и локальных компьютеров

-защиту от вирусов

-защиту от хакеров

-все перечисленное

10.Как связаны ключи шифрования между собой?

- математической функцией

-связкой

-шифром

-специальным паролем

11.Международным стандартным кодом является

- Unicode.

- CP866.

- ASCII.

- DOS.

- Altair.

12.Что относится к возможным сигнатурам?

- длина незаписанных участков магнитной ленты и неиспользованные дорожки на дискете

- дорожки дискеты и линии связи

- источник бесперебойного питания (UPS)

- источник питания и использованные дорожки на дискете

13.В чем заключается уникальность гибких дисков?

-в форматировании

- в быстродействии

- их защищенность

- в простоте обработки данных

14.При каком случае срабатывает сигнал самоуничтожения программы

-при несанкционированном копировании программы из ПЗУ в ОЗУ

-при несанкционированном копировании программы из ОЗУ в ПЗУ

- при непредвиденном включении преобразователя микрофона

-при непредвиденном отключении ПК

15.Что такое пароль?

-механизм управления доступом

-средство защиты

-безопасность личной информации

- Безопасность людей

16.Защита от сбоев серверов, рабочих станций и локальных компьютеров относится к?

-аппаратным средствам защиты

-программным средствам защиты

-техническим средствам защиты

-правовым средствам защиты

17.Для чего служат телефоны BF1, BF2?

-служат для преобразования электрических колебаний в звуковые

-служат для преобразования звуковых колебаний в электрические

-служат для преобразования магнитных колебаний в простые сигналы

-служат для преобразования магнитных колебаний в звуковые волны

18. Для чего служат микрофоны BM1, BM2?

-служат для преобразования звуковых колебаний в электрические

-служат для преобразования электрических колебаний в звуковые

-служат для преобразования магнитных колебаний в звуковые

- служат для преобразования магнитных колебаний в звуковые сигналы

19.Для осуществления телефонной связи в цепь микрофона необходимо включить?

- источник постоянного тока и подключить кабель связи
- источник переменного тока и программные средства защиты
- полевые телефонные аппараты и источник постоянного тока
- источник постоянного тока и полевые телефонные аппараты

Блок УМЕТЬ

1.Питание от местной батареи осуществляется в основном в?

- радио телефонах и полевых телефонных аппаратах
- городских АТС и ЛВС
- передатчиках П1,П2
- передатчиках П1,П2 и городских АТС

2.При наличии хорошего электромагнитного детектора, оптимальный перехват иной раз удается выполнять на расстоянии?

-10—80 см от телефонной линии
-20-80 см от телефонной линии
-30-70 см от телефонной линии
-0-100 см от телефонной линии

3.Как еще называют радиомикрофон с дистанционным (кодовым) включением через любой телефон?

-«электронное ухо»
-«электронный микрофон»
-«громкоговоритель»
-«электронный приемник»

4.Для развязки цепей микрофона и телефона по постоянному току служат?

-трансформаторы Т1,Т2
-передатчики П1,П2
-транзисторы
- ре трансляторы

5.К программным средствам защиты можно отнести?

-средства идентификации и аутентификации пользователей
-средства защиты авторских прав программистов
-неиспользованные дорожки на дискете
-дорожки дискеты

6.Защищаемые программы для ПК находятся в?

- ОЗУ и ЖМД
- ПЗУ и МГД
- МГД и Оп
- ПК и НГМД

7.К правовым мерам следует отнести?

- разработку норм, устанавливающих ответственность за компьютерные преступления и защиту авторских прав программистов

-охрану вычислительного центра и аппаратуры связи

- проектирование ЛВС и ГБС
- средства идентификации и аутентификации пользователей

8.Сбои дисковых систем относится к?

-техническим и организационным мерам защиты
- правовым мерам защиты
- мерам защиты от НДС и кражи
- к средствам идентификации и аутентификации

9.Потеря или изменение данных при ошибках ПО относится к

-техническим и правовым мерам защиты
-организационным мерам защиты
-правовым мерам защиты
-мерам защиты от НДС и кражи
-к средствам идентификации и аутентификации

10.Криптографические средства относится к?

-Программным средствам
-Аппаратным средствам
-Организационным средствам защиты
-Захвату данных

11.Чтобы установить парольную защиту в ОС Windows , необходимо выполнить следующую процедуру?

-Пуск->Панель управления->Учетные записи->Изменение пароля
-Пуск->Учетные записи->Изменение пароля
-Пуск->Справка->Учетные записи->Изменение пароля
-Пуск->Панель управления->Пароли и данные->Изменение пароля

12.Утилита Setup это - ?

-утилита входящая в состав BIOS
-утилита содержащее в себе BIOS
-BIOS не содержит ее
-настройка системы BIOS

13.При вводе пароля с клавиатуры его длина может достигать до?

-64 символов
-128 символов
-32 символов
-512 символов

14.С помощью каких клавиш можно переключать регистры?

- F1,F2, F3
- F1,F5, F8
- F2,F5, F8
- F1,F4, F5
- F3,F4, F9

15.При формировании трудно запоминаемого пароля большой длины используется система?

-Кобра
-Змея
-Ниндзя
-ЩИТ

16.Служат обеспечению сохранения целостности программного обеспечения в составе вычислительной системы

-пароль

-корпус вычислительной системы

-шифры

-сигналы

17.Устройство, которое генерирует последовательности чисел или букв в зависимости от данных, которые задает пользователь.

-преобразователь информации

-генератор

-взломщик пароля

-хакер

18.Назначение пароля в ИС?

- механизм управления доступом, средство защиты и безопасность личной информации

- скрытие копирования участков магнитной ленты из ОЗУ в ПЗУ

- технические меры защиты и средство защиты данных

- участки магнитной ленты скрытые шифром

- механизм управления средствами защиты и безопасность доступа к ОЗУ в ПЗУ

19.Какие атакующие средства включены в современные способы несанкционированного доступа?

-активные и пассивные

-положительные и отрицательные

-большие и маленькие

-объединенные и разъединенные

-односторонние и разносторонние

20.Какой скремблер обеспечивает более низкую степень защиты?

-статический

-аналоговый

-цифровой

-динамический

-блочный

Рейтинг – контроль №3. Блок ЗНАТЬ

1.Что относится к пассивным средствам защиты информации?

-Фильтры

-Детекторы поля

-Сканирующие приемники

-Комплекс радио контроля

-Нелинейные локаторы

2.Надежная защита от утечек информации за счет влияния побочных электромагнитных излучений и наводок (ПЭМИН) через цепи электропитания, заземления или по радио эфиру это?

-генераторы белого шума

-излучатели белого шума
-блокираторы белого шума
-кодеры
-декодеры

3.Система технических средств и среда распространения сигналов для односторонней передачи данных от источника к получателю.

-канал связи
-канал передачи
-средства защиты
-блокиратор связи
-де блокиратор связи

4.Представляет собой диэлектрический слоистый цилиндрический волновод круглого сечения, как правило, он находится внутри защитной оболочки

-оптическое волокно
-тонкий коаксиал
-толстый коаксиал
-витая пара
-дуга

5.Какой вид защищен от помех, создаваемых источниками электромагнитного излучения, стойки к колебаниям температуры и влажности?

-оптическое волокно
-тонкий коаксиал
-толстый коаксиал
-витая пара
-дуга

6.Генератор шума, корреляционные характеристики которого могут динамически меняться во время переговоров это?

-маскиратор речи
-блокатор сигнала
-кодер сигнала
-изолятор
-декодер сигнала

7.Что из ниже перечисленного работает по принципу подавления радиоканала между трубкой и базой?

-блокираторы сотовой связи
-генераторы белого шума
-излучатели
-кодеры
-волоконно-оптические каналы

8.Какой блокиратор утечки информации работает в диапазоне подавляемого канала?

-технический
-динамический
-статический
-цифровой
-аналоговый

9.Какие колебания воспринимает телескопическая антенна?

-высокочастотные электромагнитные

-низкочастотные электромагнитные

-среднечастотные электромагнитные

-низкочастотные магнитные

-среднечастотные магнитные

10.Какой категории относятся вирусы, не изменяющие заражаемых файлов. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т. е. вирус.

- companion
- parasitic
- cryptor
- exploit
- exp

11.Самый известный в России производитель систем защиты от вирусов, спама и хакерских атак.

-лаборатория Касперского

-Российский центр по защите от вредоносных программ

-компания McAfee Security

-лаборатория доктора Веб

-компания Тумар

Блок УМЕТЬ:

1.Запись определенных событий в журнал безопасности (security log) сервера.

-аудит

-журнал безопасности

-серверный журнал

-учет

-регистрация

2.Традиционный стандарт шифрования в сети

-Data Encryption Standard

-Data Standard

-Data Security

-Security Standard

-Security Encryption Standard

3.Метод резервного копирования, когда копирование и маркировка выбранных файлов, производится вне зависимости от того, изменялись ли они со времени последнего резервного копирования

- Полное копирование

-Копирование

-Ежедневное копирование

-Дифференцированное резервное копирование

-Резервное копирование с приращением

4.Метод резервного копирования когда, копирование всех выбранных файлов

производится без отметки о резервном копировании

-Полное копирование

-Копирование

-Ежедневное копирование

-Дифференцированное резервное копирование

-Резервное копирование с приращением

5.Метод резервного копирования, когда копирование и маркировка выбранных файлов, производится, только если они были изменены со времени последнего копирования

-Полное копирование

-Копирование

-Ежедневное копирование

-Дифференцированное резервное копирование

-Резервное копирование с приращением

6.Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании

-Полное копирование

-Копирование

-Ежедневное копирование

-Дифференцированное резервное копирование

-Резервное копирование с приращением

7.Копирование выбранных файлов, только если они были изменены со времени последнего резервного копирования, без отметки о резервном копировании

-Полное копирование

-Копирование

-Ежедневное копирование

- Дифференцированное резервное копирование

-Резервное копирование с приращением

8.Что определяют в вычислительной системе, пять основных средств секретности: конфиденциальность, аутентификация, лостность, управление доступом и контроль участников взаимодействия (nonrepudiation).

-архитектуру секретности

-конфиденциальность данных

-управление данными при защите ВС

-архитектуру конфендинциальности

-защитный модуль

9.Один из механизмов защиты использующих в сети для обеспечения конфиденциальности

-управление маршрутизацией

-генерация трафика

-защитный канал

-защитный механизм

-генерация данных

10.Механизм защиты, который обычно реализуются, используя асимметричную криптографию, хотя был разработан ряд технологий, использующих симметричную криптографию.

-цифровая сигнатура
-управление маршрутизацией
-генерация трафика
-защитный канал
-защитный механизм

11.Развитие современных средств безбумажного документооборота, средств электронных платежей немыслимо без развития средств доказательства подлинности и целостности документа. Таким средством является

-электронно-цифровая подпись
-протокол секретности
-аутентификация
-биометрия
-идентификация пользователя
-водяные знаки

12.При генерации электронно – цифровой подписи используются…

-общие параметры, секретный ключ и открытый ключ
-открытый ключ, закрытый ключ
-общие параметры, секретный ключ и закрытый ключ
-общие параметры, секретный ключ и конверт защиты
-один секретный ключ

Регламент проведения и оценивание лабораторных работ

В целях закрепления практического материала и углубления теоретических знаний по разделам дисциплины «Информационная безопасность» предполагается выполнение лабораторных работ, что позволяет углубить процесс познания, раскрыть понимание прикладной значимости осваиваемой дисциплины.

Регламент проведения мероприятия

№	Вид работы	Продолжительность
1.	Предел длительности лабораторной работы	170 мин.
2.	Защита отчета	10 мин.
	Итого (в расчете на одну лабораторную работу)	180 мин.

Критерии оценки лабораторных работ

Оценка	Критерии оценивания
5 баллов	Задание выполнено полностью, в представленном отчете обоснованно получено правильное выполненное задание.
4 балла	Задание выполнено полностью, но нет достаточного обоснования или при верном решении допущена незначительная ошибка, не влияющая на правильную

	последовательность рассуждений.
3 балла	Задания выполнены частично.
2 балла	Задание не выполнено.

Общее распределение баллов текущего контроля по видам учебных работ для студентов (в соответствии с Положением)

Рейтинг-контроль 1	тесты	До 10 баллов
Рейтинг-контроль 2	тесты	До 10 баллов
Рейтинг-контроль 3	тесты	До 10 баллов
Посещение занятий студентом	Отметка в журнале посещений	1 балл за каждое занятие
Дополнительные баллы (бонусы)		0
Выполнение семестрового плана самостоятельной работы	Защита лабораторных работ	До 30 баллов за каждую лабораторную работу

Показатели, критерии и шкала оценивания компетенций <u>промежуточной</u> аттестации знаний по учебной дисциплине «Информационная безопасность»

На основе типовых заданий из предыдущего раздела программным комплексом информационно-образовательного портала МИ ВлГУ формируются в автоматическом режиме тестовые задания для студентов: 15 вопросов в тесте (8 вопросов Блока 1, 7 вопросов Блока 2). Программный комплекс формирует индивидуальные задания для каждого зарегистрированного в системе студента и устанавливает время прохождения тестирования. Результатом тестирования является процент правильных ответов, с учетом индивидуального семестрового рейтинга студента проставляется зачет за семестр 7.
На основе типовых заданий из предыдущего раздела программным комплексом информационно-образовательного портала МИ ВлГУ формируются в автоматическом режиме тестовые задания для студентов: 15 вопросов в тесте (8 вопросов Блока 1, 7 вопросов Блока 2). Программный комплекс формирует индивидуальные задания для каждого зарегистрированного в системе студента и устанавливает время прохождения тестирования. Результатом тестирования является процент правильных ответов, с учетом индивидуального семестрового рейтинга студента формируется экзаменационная оценка за семестр 8.

Максимальное количество баллов, которое студент может получить на экзамене, в соответствии с Положением составляет 40 баллов.

Оценка в баллах	**Критерии оценивания компетенций**
30-40 баллов	Студент 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 монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач, подтверждает полное освоение компетенций, предусмотренных программой экзамена.
20-29 баллов	Студент 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, допуская некоторые неточности; демонстрирует хороший уровень освоения материала, информационной и коммуникативной культуры и в целом подтверждает освоение компетенций, предусмотренных программой экзамена.
10-19 баллов	Студент показывает знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, в целом, не препятствует усвоению последующего программного материала, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ, подтверждает освоение компетенций, предусмотренных программой экзамена на минимально допустимом уровне.
Менее 10 баллов	Студент не знает значительной части программного материала (менее 50% правильно выполненных заданий от общего объема работы), допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, не подтверждает освоение компетенций, предусмотренных программой экзамена.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ <u>ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ</u> ПО УЧЕБНОЙ ДИСЦИПЛИНЕ «Информационная безопасность»

Семестр 7.

ОПК-4

Блок ЗНАТЬ

1. Кто является основным ответственным за определение уровня классификации информации?

- Руководитель среднего звена
- Высшее руководство
- Владелец
- Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения

вероятного мошенничества и нарушения безопасности?

-Сотрудники

- Хакеры

- Атакующие

-Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

- Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования

- Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

- Улучшить контроль за безопасностью этой информации

- Снизить уровень классификации этой информации

4. Что самое главное должно продумать руководство при классификации данных?

A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

B. Необходимый уровень доступности, целостности и конфиденциальности

C. Оценить уровень риска и отменить контрмеры

D. Управление доступом, которое должно защищать данные

5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

A. Владельцы данных

B. Пользователи

C. Администраторы

D. Руководство

6. Что такое процедура?

A. Правила использования программного и аппаратного обеспечения в компании

B. Пошаговая инструкция по выполнению задачи

C. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

D. Обязательные действия

7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

A. Поддержка высшего руководства

B. Эффективные защитные меры и методы их внедрения

C. Актуальные и адекватные политики и процедуры безопасности

D. Проведение тренингов по безопасности для всех сотрудников

8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

A. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски

B. Когда риски не могут быть приняты во внимание по политическим соображениям

C. Когда необходимые защитные меры слишком сложны

D. Когда стоимость контрмер превышает ценность актива и потенциальные потери

9. Что такое политики безопасности?

A. Пошаговые инструкции по выполнению задач безопасности

B. Общие руководящие требования по достижению определенного уровня безопасности

C. Широкие, высокоуровневые заявления руководства

D. Детализированные документы по обработке инцидентов безопасности

10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

A. Анализ рисков

B. Анализ затрат / выгоды

C. Результаты ALE

D. Выявление уязвимостей и угроз, являющихся причиной риска

11. Что лучше всего описывает цель расчета ALE?

A. Количественно оценить уровень безопасности среды

B. Оценить возможные потери для каждой контрмеры

C. Количественно оценить затраты / выгоды

D. Оценить потенциальные потери от угрозы в год

12. Тактическое планирование – это:

A. Среднесрочное планирование

B. Долгосрочное планирование

C. Ежедневное планирование

D. Планирование на 6 месяцев

13. 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

14. Эффективная программа безопасности требует сбалансированного применения:

A. Технических и нетехнических методов

B. Контрмер и защитных механизмов

C. Физической безопасности и технических средств защиты

D. Процедур безопасности и шифрования

15. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

A. Внедрение управления механизмами безопасности

B. Классификацию данных после внедрения механизмов безопасности

C. Уровень доверия, обеспечиваемый механизмом безопасности

D. Соотношение затрат / выгод

16. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

A. Только военные имеют настоящую безопасность

B. Коммерческая компания обычно больше заботится о целостности и

доступности данных, а военные – о конфиденциальности

C. Военным требуется больший уровень безопасности, т.к. их риски существенно выше

D. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

17. Как рассчитать остаточный риск?

A. Угрозы x Риски x Ценность актива

B. (Угрозы x Ценность актива x Уязвимости) x Риски

C. SLE x Частоту = ALE

D. (Угрозы x Уязвимости x Ценность актива) x Недостаток контроля

18. Что из перечисленного не является целью проведения анализа рисков?

A. Делегирование полномочий

B. Количественная оценка воздействия потенциальных угроз

C. Выявление рисков

D. Определение баланса между воздействием риска и стоимостью необходимых контрмер

19. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

A. Поддержка

B. Выполнение анализа рисков

C. Определение цели и границ

D. Делегирование полномочий

20. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

A. Чтобы убедиться, что проводится справедливая оценка

B. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ

C. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа

D. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

21. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:

1.гаммирования;

2.подстановки;

3.кодирования;

4.перестановки;

5.аналитических преобразований.

22. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:

1.гаммирования;

2. подстановки;

3. кодирования;

4. перестановки;

5. аналитических преобразований.

23. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:

1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

24. Защита информации от утечки это деятельность по предотвращению:

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

25 Защита информации это:

1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

26 Естественные угрозы безопасности информации вызваны:

1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

27 Искусственные угрозы безопасности информации вызваны:

1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;

4. корыстными устремлениями злоумышленников;

5. ошибками при действиях персонала.

28 К основным непреднамеренным искусственным угрозам АСОИ относится:

1. физическое разрушение системы путем взрыва, поджога и т.п.;

2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;

3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

5. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

29. К посторонним лицам нарушителям информационной безопасности относится:

1. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;

2. персонал, обслуживающий технические средства;

3. технический персонал, обслуживающий здание;

4. пользователи;

5. сотрудники службы безопасности.

6. представители конкурирующих организаций.

7. лица, нарушившие пропускной режим;

30. К посторонним лицам нарушителям информационной безопасности относится:

- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;

-персонал, обслуживающий технические средства;

-технический персонал, обслуживающий здание;

-пользователи;

-сотрудники службы безопасности.

- представители конкурирующих организаций.

- лица, нарушившие пропускной режим;

31. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:

1. черный пиар;

2. фишинг;

3. нигерийские письма;

4. источник слухов;

5. пустые письма.

32. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

1. черный пиар;

2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

33 Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

34 Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

35 Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

36 Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

37 Активный перехват информации это перехват, который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

38 Перехват, который заключается в установке подслушивающего устройства в

аппаратуру средств обработки информации называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

39 Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;

5.просмотр мусора

40 Перехват, который осуществляется путем использования оптической техники называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

41. К внутренним нарушителям информационной безопасности относится:

1. клиенты;
2. пользователи системы;
3. посетители;
4. любые лица, находящиеся внутри контролируемой территории;
5. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.
6. персонал, обслуживающий технические средства.
7. сотрудники отделов разработки и сопровождения ПО;
8. технический персонал, обслуживающий здание

42. Как называется умышленно искаженная информация?

- Дезинформация
- Информативный поток
- Достоверная информация
- Перестает быть информацией

43. Как называется информация, к которой ограничен доступ?

- Конфиденциальная
- Противозаконная
- Открытая
- Недоступная

44. Какими путями может быть получена информация?

-проведением, покупкой и противоправным добыванием информации научных исследований

- захватом и взломом ПК информации научных исследований
- добыванием информации из внешних источников и скремблированием

информации научных исследовании

- захватом и взломом защитной системы для информации научных исследований

45. Как называются компьютерные системы, в которых обеспечивается безопасность информации?

- защищенные КС
- небезопасные КС
- Само достаточные КС
- Саморегулирующиеся КС

46. Основной документ, на основе которого проводится политика информационной безопасности?

- программа информационной безопасности
- регламент информационной безопасности
- политическая информационная безопасность
- Протекторат

47. В зависимости от формы представления информация может быть разделена на?

- Речевую, документированную и телекоммуникационную
- Мысль, слово и речь
- цифровая, звуковая и тайная
- цифровая, звуковая

48. К каким процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации

- Информационным процессам
- Мыслительным процессам
- Машинным процессам
- Микропроцессам

49. Что называют защитой информации?

- Все ответы верны
- Называют деятельность по предотвращению утечки защищаемой информации
- Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
- Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию

50. Под непреднамеренным воздействием на защищаемую информацию понимают?

- Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений
- Процесс ее преобразования, при котором содержание информации изменяется на ложную
- Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию
- Не ограничения доступа в отдельные отрасли экономики или на конкретные производства

51. Шифрование информации это

- Процесс ее преобразования, при котором содержание информации становится

непонятным для не обладающих соответствующими полномочиями субъектов

- Процесс преобразования, при котором информация удаляется
- Процесс ее преобразования, при котором содержание информации изменяется на ложную
- Процесс преобразования информации в машинный код

52. Основные предметные направления Защиты Информации?

- охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности
- Охрана золотого фонда страны
- Определение ценности информации
- Усовершенствование скорости передачи информации

53. Государственная тайна это

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
- ограничения доступа в отдельные отрасли экономики или на конкретные производства
- защищаемые банками и иными кредитными организациями сведения о банковских операциях
- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

54. Коммерческая тайна это….

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
- ограничения доступа в отдельные отрасли экономики или на конкретные производства
- защищаемые банками и иными кредитными организациями сведения о банковских операциях
- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

55. Банковская тайна это….

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
- ограничения доступа в отдельные отрасли экономики или на конкретные производства
- защищаемые банками и иными кредитными организациями сведения о банковских операциях
- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных

обязанностей

56. Профессиональная тайна

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны

- ограничения доступа в отдельные отрасли экономики или на конкретные производства

- защищаемые банками и иными кредитными организациями сведения о банковских операциях

- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

57. К основным объектам банковской тайны относятся следующие:

- Все ответы верны

- Тайна банковского счета

- Тайна операций по банковскому счету

- Тайна банковского вклада

58. Как называется тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений?

- Тайна связи

- Нотариальная тайна

- Адвокатская тайна

- Тайна страхования

59. Как называются сведения, доверенные нотариусу в связи с совершением нотариальных действий?

- Нотариальная тайна

- Общедоступные сведения

- Нотариальный секрет

- Нотариальное вето

60. Элемент аппаратной защиты, где используется установка источников бесперебойного питания (UPS)?

- защита от сбоев в электропитании

- защита от сбоев серверов, рабочих станций и локальных компьютеров

- защита от сбоев устройств для хранения информации

- защита от утечек информации электромагнитных излучений

61.Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право

- управление доступом

- конфиденциальность

- аутентичность

- целостность

- доступность

62. Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем

- защита от сбоев в электропитании

защита от сбоев серверов, рабочих станций и локальных компьютеров

- защита от сбоев устройств для хранения информации

- защита от утечек информации электромагнитных излучений

63. Элемент аппаратной защиты, где используется организация надежной и эффективной системы резервного копирования и дублирования данных

- защита от сбоев в электропитании

- защита от сбоев серверов, рабочих станций и локальных компьютеров

-защита от сбоев устройств для хранения информации

- защита от утечек информации электромагнитных излучений

64. Элемент аппаратной защиты, где используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений.

- защита от сбоев в электропитании

- защита от сбоев серверов, рабочих станций и локальных компьютеров

- защита от сбоев устройств для хранения информации

-защита от утечек информации электромагнитных излучений

65. Какая из перечисленных атак на поток информации является пассивной:

- перехват.

- имитация.

- модификация.

- фальсификация.

- прерывание.

66. К открытым источникам информация относятся.

-Газеты, Радио, Новости

- Информация украденная у спецслужб

- Из вскрытого сейфа

- Украденная из правительственной организации

67. Технические каналы утечки информации делятся на…

- Все перечисленное

- Акустические и виброакустические

- Электрические

- Оптические

68. Какой технический канал утечки отвечает за распространение звуковых колебаний в любом звукопроводящем материале или среде?

- Акустические и виброакустические

- Электрические

- Оптические

- Радиоканалы

69. Какой технический канал утечки отвечает за напряжение и токи в различных токопроводящих коммуникациях?

- Акустические и виброакустические

- Электрические

- Оптические

- Радиоканалы

70. Какой технический канал утечки отвечает за электромагнитные излучения

радиодиапазона?

- Акустические и виброакустические
- Электрические
- Оптические
-Радиоканалы

71. Какой технический канал утечки отвечает за электромагнитные излучения в видимой, инфракрасной и ультрафиолетовой частях спектра?

- Акустические и виброакустические
- Электрические
- Оптические
- Радиоканалы

72. Учет всех возможных коммуникационных каналов, обеспечения физической безопасности, шифрования резервных копий и информации, покидающей корпоративный периметр, и других организационных мероприятий это?

- Индивидуальный подход к защите
- Комплексный подход к защите
- Смешанный подход к защите
- Рациональный подход к защите

73. Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе

- Информационная безопасность
- Защитные технологии
- Заземление
- Конфиденциальность

74. Можно выделить следующие направления мер информационной безопасности

- Правовые
- Организационные
- Все ответы верны
- Технические

75. Что можно отнести к правовым мерам информационной безопасности?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
- охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра итд
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое
- охрану вычислительного центра, установку сигнализации и многое другое

76. Что можно отнести к организационным мерам ИБ?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.

- Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.

- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем.

- Охрану работоспособности отдельных звеньев и организацию вычислительных сетей с возможностью перераспределения ресурсов.

- Принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

77. Что можно отнести к техническим мерам ИБ?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства

- Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.

- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев и многое другое

- Простые и доступные меры защиты от хищений, саботажа, диверсий, взрывов

- В административных местах установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

ОПК-4

Блок УМЕТЬ

1. Что понимают под набором норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации?

А Политика безопасности

Б Законная политика

В Свод правил

Г Стратегия предприятия

2. В каких шифрах в качестве ключа используют таблицы?

А Шифрующие таблицы

Б метод Цезаря

В Магические квадраты

Г Полибианский квадрат

3. Самый первый шифр перестановки?

А Метод скитала

Б метод Цезаря

В Магические квадраты

Г Полибианский квадрат

4. В каком шифре каждая буква заменялась на другую букву того же алфавита по следующему правилу: заменяющая буква определялась путем смещения по алфавиту от исходной буквы на К букв.?

А шифрующие таблицы

Б метод Цезаря

В Магические квадраты

Г Полибианский квадрат

5. Какой шифр основан на подсчете частот появления букв в шифртексте..?

А шифр Трисемуса

Б система омофонов

В алгоритм Вернама

Г гаммирование

6. Какой шифр сложной замены представляет собой модификацию шифра Цезаря числовым ключом?

А Шифр Гронсфельда

Б система омофонов

В алгоритм Вернама

Г гаммирование

7. Какой шифр сложной замены описывается таблицей шифрования, и где ключ шифрования меняется от буквы к букве.?

А шифр Трисемуса

Б система Вижинера

В алгоритм Вернама

Г гаммирование

8. Какой шифр является абсолютно надежным?

А шифр Трисемуса

Б одноразовая система шифрования

В алгоритм Вернама

Г гаммирование

9. Какой шифр является в сущности частным случаем системы шифрования Вижинера при значении модуля m = 2.?

А шифр Трисемуса

Б одноразовая система шифрования

В алгоритм Вернама

Г гаммирование

10. Псевдослучайная последовательность, выработанная по заданному алгоритму для зашифрования открытых данных и расшифрования зашифрованных данных это?

А альфа шифра

Б бета шифра

В гамма шифра

Г лямбда шифра

11. Псевдослучайная последовательность, выработанная по заданному алгоритму для зашифрования открытых данных и расшифрования зашифрованных данных это?

А альфа шифра

Б бета шифра

В гамма шифра

Г лямбда шифра

12 По мнению К. Шеннона, в практических шифрах необходимо использовать два общих принципа:

- рассеивание
- перемешивание
- встряска
- переставка

13 Ключ какой длины используется в алгоритме DES:

- 56 бит
- 64 бит
- 128 бит
- 32 бит

14.Блок какой длины обрабатывается в алгоритме DES:

- 64 бит
- 56 бит
- 128 бит
- 32 бит

15.Сколько основных итераций в алгоритме DES:

- 16
- 14
- 20
- 8

16.Первым этапом алгоритма DES является:

- начальная перестановка битов исходного блока
- конечная перестановка битов исходного блока
- начальное рассеивание битов исходного блока
- начальная замена битов исходного блока

17.Какая операция используется в алгоритме DES:

- сложение по модулю два
- сложение
- битовая инверсия
- битовое умножение

18.Какая операция используется в алгоритме DES при вычислении ключей:

- сдвиг влево
- сдвиг вправо
- битовая инверсия
- битовое умножение

19.Сколько ключей используется в алгоритме DES:

- 16
- 12
- 20
- 32

20. При каком режиме DES длинный файл разбивают на 64-битовые отрезки (блоки) по 8 байтов. Каждый из этих блоков шифруют независимо с ис¬пользованием

одного и того же ключа шифрования?

- электронная кодовая книга ECB (Electronic Code Book);
- сцепление блоков шифра CBC (Cipher Block Chaining);
- обратная связь по шифртексту CFB (Cipher Feed Back);
- обратная связь по выходу OFB (Output Feed Back).

21.При каком режиме DES исходный файл M разбивается на 64-битовые блоки: M = M(1)M(2)...M(n). Первый блок M(1) складывается по модулю 2 с 64-битовым начальным вектором IV, который меняется ежедневно и держится в секрете. Полученная сумма затем шифруется с использованием ключа DES, известного и отправителю, и получателю информации. Полученный 64-битовый блок шифртекста C(1) складывается по модулю 2 со вторым блоком исходного текста, результат шифруется и получается второй 64-битовый блок шифртекста C(2) и т.д.

-электронная кодовая книга ECB (Electronic Code Book);

-сцепление блоков шифра CBC (Cipher Block Chaining);

-обратная связь по шифртексту CFB (Cipher Feed Back);

-обратная связь по выходу OFB (Output Feed Back).

22 При каком режиме DES размер блока может отличаться от 64. Исходный файл M считывается последовательными t-битовыми блоками (t <= 64): M = M(1)M(2)...M(n) (остаток дописывается нулями или пробелами).

-электронная кодовая книга ECB (Electronic Code Book);

- сцепление блоков шифра CBC (Cipher Block Chaining);
- обратная связь по шифртексту CFB (Cipher Feed Back);
- обратная связь по выходу OFB (Output Feed Back).

23.Блоками какого размера оперирует алгоритм шифрования IDEA?

- 64 бит
- 56 бит
- 128 бит
- 32 бит

24.Сколько итераций цикла использует алгоритм шифрования IDEA?

- 8
- 16
- 5
- 24

25.Ключ какого размера использует алгоритм шифрования IDEA?

- 128 бит
- 56 бит
- 64 бита
- 32 бит

26.Какие режимы использует отечественный стандарт шифрования?

- простая замена;
- гаммирование;
- гаммирование с обратной связью;
- выработка имитовставки.
- Все перечисленные

27.Чем отличаются ассиметричные шифры от симметричных?

- Простотой реализации;

- наличием постоянного ключа
- наличием трех секретных ключей;
- Наличием двух ключей

28.Какая процедура устанавливает, является ли данный объект именно таким, каким он себя объявляет.

- авторизация
- идентификация
-коммутация
-аутентификация

29.Какая процедура устанавливает сферу действия объекта и доступ¬ные ему ресурсы сети?

- авторизация
- идентификация
-коммутация
-аутентификация

30.Для проверки подлинности применяют:

-механизм запроса-ответа;
-механизм отметки времени.
-Механизм ответа-ответа
-Механизм запроса-запроса

31.Какую процедуру используют для взаимной проверки подлинности ?

- «рукопожатия»
-механизм отметки времени.
-Механизм ответа-ответа
-Механизм запроса-запроса

32. Какие сбои оборудования бывают?

- потери при заражении системы компьютерными вирусами
- несанкционированное копирование, уничтожение или подделка информации
- сбои работы серверов, рабочих станций, сетевых карт и тд - ознакомление с конфиденциальной информацией

33.Какие сбои оборудования, при которых теряется информация, бывают?

- случайное уничтожение или изменение данных
- перебои электропитания
- некорректное использование программного и аппаратного обеспечения, ведущее к уничтожению или изменению данных
- несанкционированное копирование, уничтожение или подделка информации

34 Какие потери информации бывают из-за некорректной работы программ?

- сбои работы серверов, рабочих станций, сетевых карт и тд
- перебои электропитания
-потеря или изменение данных при ошибках ПО
- ознакомление с конфиденциальной информацией

35. Какие потери информации бывают из-за некорректной работы программ?

- потери при заражении системы компьютерными вирусами
- сбои дисковых систем
- перебои электропитания
- сбои работы серверов, рабочих станций, сетевых карт и тд

36. Какие потери информации, связанные с несанкционированным доступом, бывают?

- несанкционированное копирование, уничтожение или подделка информации
- потери при заражении системы компьютерными вирусами
- случайное уничтожение или изменение данных
- сбои дисковых систем

37. Потери из-за ошибки персонала и пользователей бывают?

- несанкционированное копирование, уничтожение или подделка информации
- потери при заражении системы компьютерными вирусами
- случайное уничтожение или изменение данных
- сбои дисковых систем

38. Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии?

- установка источников бесперебойного питания (UPS)
- Такого средства не существует
- Каждую минуту сохранять данные
- Перекидывать информацию на носитель, который не зависит от энергии

39. Способ защиты от сбоев процессора?

- установка источников бесперебойного питания (UPS)
- симметричное мультипроцессирование
- Каждую минуту сохранять данные
- Перекидывать информацию на носитель, который не зависит от энергии

Семестр 8.

ОПК-4:

Блок ЗНАТЬ

1.Виды защиты БД

-защита паролем, защита пользователем,

- учётная запись группы администратора
- приложение, которое используется для управления базой данных
- группа Users

2.Виды защиты БД

-защита всех учетных записей, защита идентифицированных объектов

- защита учётной записи группы администратора
- приложение, которое используется для управления базой данных
- защита группы Users

3.Наибольшую угрозу для безопасности сети представляют.

- несанкционированный доступ, электронное подслушивание и преднамеренное или неумышленное повреждение
- вскрытие стандартной учётной записи пользователя
- вскрытие стандартной учётной группы администратора
- копирование файлов, которые были изменены в течение дня, без отметки о резервном копировании

4.Защита через права доступа заключается.

-присвоении каждому пользователю определенного набора прав

-запереть серверы в специальном помещении с ограниченным доступом

-присвоить пароль каждому общедоступному ресурсу

- в наличии преобразователя микрофона

5.Дифференцированное резервное копирование это

-Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании

-Копирование всех выбранных файлов без отметки о резервном копировании

-Копирование и маркировка выбранных файлов, только если они были изменены со времени последнего копирования

-Копирование выбранных файлов, только если они были изменены со времени последнего резервного копирования, без отметки о резервном копировании

6.Полное копирование данных это

-Копирование и маркировка выбранных файлов, вне зависимости от того, изменялись ли они со времени последнего резервного копирования

-Копирование всех выбранных файлов без отметки о резервном копировании

-Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании

-Копирование и маркировка выбранных файлов, только если они были изменены со времени последнего копирования

7.Disk mirroring – это

-дублирование раздела и запись его копии на другом физическом диске

-это пара зеркальных дисков, каждым из которых управляет отдельный контроллер

-При записи данных делится на части и распределяется по серверу

- Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании

8.Пароль доступа к ресурсам

-Доступ только для чтения

- такой пароль не существует

-Отказоустойчивые системы

-Метод резервного копирования

-Шифрование данных

9.Пароль доступа к ресурсам

- Полный доступ и доступ в зависимости от пароля (

- такой пароль не существует

-Отказоустойчивые системы

-Метод резервного копирования

-Шифрование данных

10.Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии?

- установка источников бесперебойного питания (UPS)

- Такого средства не существует

- Каждую минуту сохранять данные

- Перекидывать информацию на носитель, который не зависит от энергии

11.Ежедневное копирование данных это

-Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании

-Копирование всех выбранных файлов без отметки о резервном копировании

-Копирование и маркировка выбранных файлов, вне зависимости от того, изменялись ли они со времени последнего резервного копирования

-Копирование выбранных файлов, только если они были изменены со времени последнего резервного копирования, без отметки о резервном копировании

12.Способ защиты от сбоев процессора?

- установка источников бесперебойного питания (UPS)
- симметричное мультипроцессирование
- Каждую минуту сохранять данные
- Перекидывать информацию на носитель, который не зависит от энергии

13.Способ защиты от сбоев устройств для хранения информации?

- установка источников бесперебойного питания (UPS)
- симметричное мультипроцессирование
- Каждую минуту сохранять данные
- Организация надежной и эффективной системы резервного копирования и дублирования данных

14.Средства защиты данных, функционирующие в составе программного обеспечения.

- Программные средства защиты информации
- Технические средства защиты информации
- Источники бесперебойного питания (UPS)
- Смешанные средства защиты информации

15.Средством предотвращения потерь информации при кратковременном отключении электроэнергии является?

-источник бесперебойного питания (UPS)
-источник питания
-электро-переключатель
-все перечисленное

16.К наиболее важному элементу аппаратной защиты можно отнести?

- защита от сбоев серверов, рабочих станций и локальных компьютеров
-защиту от вирусов
-защиту от хакеров
-все перечисленное

17.Как связаны ключи шифрования между собой?

- математической функцией
-связкой
-шифром
-специальным паролем

18.Международным стандартным кодом является

- Unicode.
- CP866.
- ASCII.
- DOS.
- Altair.

19.Что относится к возможным сигнатурам?

- длина незаписанных участков магнитной ленты и неиспользованные дорожки

на дискете

- дорожки дискеты и линии связи
- источник бесперебойного питания (UPS)
- источник питания и использованные дорожки на дискете

20.В чем заключается уникальность гибких дисков?

-в форматировании
- в быстродействии
- их защищенность
- в простоте обработки данных

21.При каком случае срабатывает сигнал самоуничтожения программы

-при несанкционированном копировании программы из ПЗУ в ОЗУ
-при несанкционированном копировании программы из ОЗУ в ПЗУ
- при непредвиденном включении преобразователья микрофона
-при непредвиденном отключении ПК

22.Что такое пароль?

-механизм управления доступом
-средство защиты
-безопасность личной информации
- Безопасность людей

23.Защита от сбоев серверов, рабочих станций и локальных компьютеров относится к?

-аппаратным средствам защиты
-программным средствам защиты
-техническим средствам защиты
-правовым средствам защиты

24.Для чего служат телефоны BF1, BF2?

-служат для преобразования электрических колебаний в звуковые
-служат для преобразования звуковых колебаний в электрические
-служат для преобразования магнитных колебаний в простые сигналы
-служат для преобразования магнитных колебаний в звуковые волны

25. Для чего служат микрофоны BM1, BM2?

-служат для преобразования звуковых колебаний в электрические
-служат для преобразования электрических колебаний в звуковые
-служат для преобразования магнитных колебаний в звуковые
- служат для преобразования магнитных колебаний в звуковые сигналы

26.Для осуществления телефонной связи в цепь микрофона необходимо включить?

- источник постоянного тока и подключить кабель связи
- источник переменного тока и программные средства защиты
- полевые телефонные аппараты и источник постоянного тока
- источник постоянного тока и полевые телефонные аппараты

27.Что относится к пассивным средствам защиты информации?

-Фильтры
-Детекторы поля
-Сканирующие приемники
-Комплекс радио контроля

-Нелинейные локаторы

28.Надежная защита от утечек информации за счет влияния побочных электромагнитных излучений и наводок (ПЭМИН) через цепи электропитания, заземления или по радио эфиру это?

-генераторы белого шума

-излучатели белого шума

-блокираторы белого шума

-кодеры

-декодеры

29.Система технических средств и среда распространения сигналов для односторонней передачи данных от источника к получателю.

-канал связи

-канал передачи

-средства защиты

-блокиратор связи

-де блокиратор связи

30.Представляет собой диэлектрический слоистый цилиндрический волновод круглого сечения, как правило, он находится внутри защитной оболочки

-оптическое волокно

-тонкий коаксиал

-толстый коаксиал

-витая пара

-дуга

31.Какой вид защищен от помех, создаваемых источниками электромагнитного излучения, стойки к колебаниям температуры и влажности?

-оптическое волокно

-тонкий коаксиал

-толстый коаксиал

-витая пара

-дуга

32.Генератор шума, корреляционные характеристики которого могут динамически меняться во время переговоров это?

-маскиратор речи

-блокатор сигнала

-кодер сигнала

-изолятор

-декодер сигнала

33.Что из ниже перечисленного работает по принципу подавления радиоканала между трубкой и базой?

-блокираторы сотовой связи

-генераторы белого шума

-излучатели

-кодеры

-волоконно-оптические каналы

34.Какой блокиратор утечки информации работает в диапазоне подавляемого канала?

-технический
-динамический
-статический
-цифровой
-аналоговый
35.Какие колебания воспринимает телескопическая антенна?
-высокочастотные электромагнитные
-низкочастотные электромагнитные
-среднечастотные электромагнитные
-низкочастотные магнитные
-среднечастотные магнитные
36.Какой категории относятся вирусы, не изменяющие заражаемых файлов. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т. е. вирус.
- companion
- parasitic
- cryptor
- exploit
- exp
37.Самый известный в России производитель систем защиты от вирусов, спама и хакерских атак.
-лаборатория Касперского
-Российский центр по защите от вредоносных программ
-компания McAfee Security
-лаборатория доктора Веб
-компания Тумар

ОПК-4:
Блок УМЕТЬ
1.Наиболее распространенный криптографический код
-Код Хэмминга
-код Рида-Соломона
-код Морзе
-итеративный код
2.Помехоустойчивый код характеризуется тройкой чисел
- n,k,d0
-h,k,d0
-a,b,c
-x,y,z
3. Функция технологии RAID 4
-дисковый массив повышенной производительности с чередованием, без отказоустойчивости;
-зарезервирован для массивов, которые применяют код Хемминга
-хранит блок четности на одном физическом диске

-распределяет информацию о четности равномерно по всем дискам

4.Функция технологии RAID 5

-дисковый массив повышенной производительности с чередованием, без отказоустойчивости

-зарезервирован для массивов, которые применяют код Хемминга;

-хранит блок четности на одном физическом диске

-распределяет информацию о четности равномерно по всем дискам

5.Наиболее простой и недорогой метод предотвратить катастрофическую потерю данных

-Резервное копирование на магнитную ленту

-Шифрование данных

-Бездисковые компьютеры

-Все ответы верны

6.Какой способ защиты информации присваивает значение каждому пользователю соответствующие права доступа к каждому ресурсу

- Права группы

-Аудит

-Шифрование данных

-Модели защиты

7.Методы сохранение данных при чрезвычайных ситуаций

-резервное копирование на магнитную ленту;

-источники бесперебойного питания (UPS);

-отказоустойчивые системы

-Все ответы верны

8.Какой способ данные, дублируя и размещая их на различных физических носителях (например, на разных дисках).

-Журнал резервного копирования

-Отказоустойчивые системы

-Метод резервного копирования

-Шифрование данных

9.Disk duplexing это?

-дублирование раздела и запись его копии на другом физическом диске

-это пара зеркальных дисков, каждым из которых управляет отдельный контроллер

-При записи данных делится на части и распределяется по серверу

-Все ответы верны

10.Питание от местной батареи осуществляется в основном в?

- радио телефонах и полевых телефонных аппаратах

- городских АТС и ЛВС

- передатчиках П1,П2

- передатчиках П1,П2 и городских АТС

11.При наличии хорошего электромагнитного детектора, оптимальный перехват иной раз удается выполнять на расстоянии?

-10—80 см от телефонной линии

-20-80 см от телефонной линии

-30-70 см от телефонной линии

-0-100 см от телефонной линии

12.Как еще называют радиомикрофон с дистанционным (кодовым) включением через любой телефон?

-«электронное ухо»

-«электронный микрофон»

-«громкоговоритель»

-«электронный приемник»

13.Для развязки цепей микрофона и телефона по постоянному току служат?

-трансформаторы Т1,Т2

-передатчики П1,П2

-транзисторы

- ре трансляторы

14.К программным средствам защиты можно отнести?

-средства идентификации и аутентификации пользователей

-средства защиты авторских прав программистов

-неиспользованные дорожки на дискете

-дорожки дискеты

15.Защищаемые программы для ПК находятся в?

- ОЗУ и ЖМД

- ПЗУ и МГД

- МГД и Оп

- ПК и НГМД

16.К правовым мерам следует отнести?

- разработку норм, устанавливающих ответственность за компьютерные преступления и защиту авторских прав программистов

-охрану вычислительного центра и аппаратуры связи

- проектирование ЛВС и ГБС

- средства идентификации и аутентификации пользователей

17.Сбои дисковых систем относится к?

-техническим и организационным мерам защиты

- правовым мерам защиты

- мерам защиты от НДС и кражи

- к средствам идентификации и аутентификации

18.Потеря или изменение данных при ошибках ПО относится к

-техническим и правовым мерам защиты

-организационным мерам защиты

-правовым мерам защиты

-мерам защиты от НДС и кражи

-к средствам идентификации и аутентификации

19.Криптографические средства относится к?

-Программным средствам

-Аппаратным средствам

-Организационным средствам защиты

-Захвату данных

20.Чтобы установить парольную защиту в ОС Windows , необходимо выполнить следующую процедуру?

-Пуск->Панель управления->Учетные записи->Изменение пароля
-Пуск->Учетные записи->Изменение пароля
-Пуск->Справка->Учетные записи->Изменение пароля
-Пуск->Панель управления->Пароли и данные->Изменение пароля
21.Утилита Setup это - ?
-утилита входящая в состав BIOS
-утилита содержащее в себе BIOS
-BIOS не содержит ее
-настройка системы BIOS
22.При вводе пароля с клавиатуры его длина может достигать до?
-64 символов
-128 символов
-32 символов
-512 символов
23.С помощью каких клавиш можно переключать регистры?
- F1,F2, F3
- F1,F5, F8
- F2,F5, F8
- F1,F4, F5
- F3,F4, F9
24.При формировании трудно запоминаемого пароля большой длины используется система?
-Кобра
-Змея
-Ниндзя
-ЩИТ
25.Служат обеспечению сохранения целостности программного обеспечения в составе вычислительной системы
-пароль
-корпус вычислительной системы
-шифры
-сигналы
26.Устройство, которое генерирует последовательности чисел или букв в зависимости от данных, которые задает пользователь.
-преобразователь информации
-генератор
-взломщик пароля
-хакер
27.Назначение пароля в ИС?
- механизм управления доступом, средство защиты и безопасность личной информации
- скрытие копирования участков магнитной ленты из ОЗУ в ПЗУ
- технические меры защиты и средство защиты данных
- участки магнитной ленты скрытые шифром
- механизм управления средствами защиты и безопасность доступа к ОЗУ в ПЗУ

28.Какие атакующие средства включены в современные способы несанкционированного доступа?

-активные и пассивные

-положительные и отрицательные

-большие и маленькие

-объединенные и разъединенные

-односторонние и разносторонние

29.Какой скремблер обеспечивает более низкую степень защиты?

-статический

-аналоговый

-цифровой

-динамический

-блочный

30.Запись определенных событий в журнал безопасности (security log) сервера.

-аудит

-журнал безопасности

-серверный журнал

-учет

-регистрация

31.Традиционный стандарт шифрования в сети

-Data Encryption Standard

-Data Standard

-Data Security

-Security Standard

-Security Encryption Standard

32.Метод резервного копирования, когда копирование и маркировка выбранных файлов, производится вне зависимости от того, изменялись ли они со времени последнего резервного копирования

- Полное копирование

-Копирование

-Ежедневное копирование

-Дифференцированное резервное копирование

-Резервное копирование с приращением

33.Метод резервного копирования когда, копирование всех выбранных файлов производится без отметки о резервном копировании

-Полное копирование

-Копирование

-Ежедневное копирование

-Дифференцированное резервное копирование

-Резервное копирование с приращением

34.Метод резервного копирования, когда копирование и маркировка выбранных файлов, производится, только если они были изменены со времени последнего копирования

-Полное копирование

-Копирование

-Ежедневное копирование

-Дифференцированное резервное копирование

-Резервное копирование с приращением

35.Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании

-Полное копирование

-Копирование

-Ежедневное копирование

-Дифференцированное резервное копирование

-Резервное копирование с приращением

36.Копирование выбранных файлов, только если они были изменены со времени последнего резервного копирования, без отметки о резервном копировании

-Полное копирование

-Копирование

-Ежедневное копирование

- Дифференцированное резервное копирование

-Резервное копирование с приращением

37.Что определяют в вычислительной системе, пять основных средств секретности: конфиденциальность, аутентификация, лостность, управление доступом и контроль участников взаимодействия (nonrepudiation).

-архитектуру секретности

-конфиденциальность данных

-управление данными при защите ВС

-архитектуру конфендинциальности

-защитный модуль

38.Один из механизмов защиты использующих в сети для обеспечения конфиденциальности

-управление маршрутизацией

-генерация трафика

-защитный канал

-защитный механизм

-генерация данных

39.Механизм защиты, который обычно реализуются, используя асимметричную криптографию, хотя был разработан ряд технологий, использующих симметричную криптографию.

-цифровая сигнатура

-управление маршрутизацией

-генерация трафика

-защитный канал

-защитный механизм

40.Развитие современных средств безбумажного документооборота, средств электронных платежей немыслимо без развития средств доказательства подлинности и целостности документа. Таким средством является

-электронно-цифровая подпись

-протокол секретности

-аутентификация

-биометрия

-идентификация пользователя
-водяные знаки
41.При генерации электронно – цифровой подписи используются…
-общие параметры, секретный ключ и открытый ключ
-открытый ключ, закрытый ключ
-общие параметры, секретный ключ и закрытый ключ
-общие параметры, секретный ключ и конверт защиты
-один секретный ключ

Максимальная сумма баллов, набираемая студентом по дисциплине «Информационная безопасность» равна 100.

Оценка в баллах	Оценка по шкале	Обоснование	Уровень сформированности компетенций
Более 80	«Отлично»	Содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному	***Высокий уровень***
66-80	«Хорошо»	Содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками	***Продвинутый уровень***
50-65	«Удовлетворительно»	Содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы	***Пороговый уровень***

		с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки	
Менее 50	«Неудовлетворительно»	Содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки	Компетенции не сформированы