МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование ф-та полностью)
М.О. Таныгин
(подпись, инициалы, фамилия)
« *29* » *августа* 2022 г.

ОЦЕНОЧНЫЕ СРЕДСТВА
для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Методы и средства зашиты компьютерной информации
(наименование учебной дисциплины)

09.03.04 Программная инженерия, направленность (профиль) «Разработка программно-информационных систем»
(код и наименование ОПОП ВО)

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

Тема 1. Основные понятия и анализ угроз информационной безопасности.

1. Основные понятия защиты информации и информационной безопасности.
2. Понятие угрозы информационной безопасности.
3. Анализ и классификация угроз информационной безопасности.
4. Угроза раскрытия параметров автоматизированной системы.
5. Угрозы нарушения конфиденциальности информации, целостности информации, доступности информации.

Тема 2. Проблемы информационной безопасности сетей.

1. Модель ISO/OSI и стек протоколов TCP/IP.
2. Проблемы безопасности IP- сетей.
3. Основные виды сетевых атак.
4. Угрозы и уязвимости проводных корпоративных сетей.
5. Угрозы и уязвимости беспроводных сетей.
6. Пути решения проблем защиты информации в сетях

Тема 3. Политика безопасности.

1. Основные понятия политики безопасности.
2. Верхний, средний и нижний уровни политики безопасности.
3. Структура политики безопасности организации.
4. Базовая политика безопасности.
5. Специализированные политики безопасности.
6. Основные этапы разработки политики безопасности организации.

Тема 4. Криптографическая защита информации.

1. Основные понятия криптографической защиты информации.
2. Требования к криптографическим системам.
3. Симметричные и ассиметричные криптосистемы шифрования.
4. Криптографическая защита информации.
5. Блочные и потоковые шифры.
6. Обзор программных и программно-аппаратных средств криптографической защиты.
7. Стандарт шифрования AES.
8. Алгоритм шифрования RSA.

Тема 5. Технологии аутентификации.

1. Аутентификация, авторизация и администрирование действий пользователей.
2. Строгая аутентификация, основанная на симметричных алгоритмах.
3. Биометрическая аутентификация пользователя.

4. Аппаратно-программные системы идентификации и аутентификации.

5. Аутентификация на основе PIN-кода.

Тема 6. Технологии межсетевых экранов.

1. Функции межсетевых экранов: фильтрация трафика, выполнение функций посредничества.

2. Варианты исполнения межсетевых экранов.

3. Особенности функционирования межсетевых экранов на различных уровнях модели OSI.

4. Формирование политики межсетевого взаимодействия.

5. Основные схемы подключения межсетевых экранов.

6. Персональные и распределенные межсетевые экраны.

7. Проблемы безопасности межсетевых экранов.

Тема 7. Технологии защиты от вирусов.

1. Классификация компьютерных вирусов.

2. Жизненный цикл вирусов.

3. Основные каналы распространения вредоносных программ.

4. Обзор современных антивирусных программ.

5. Построение системы антивирусной защиты корпоративной сети.

Тема 8. Требования к системам защиты информации.

1. Проблемы информационной безопасности сетей.

2. Показатели защищенности средств вычислительной техники от несанкционированного доступа.

3. Классы защищенности автоматизированных систем.

4. Требования к защите информации при работе с системами управления базами данных.

5. Требования к защите информации при взаимодействии абонентов с сетями общего пользования.

6. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных.

Критерии оценки:

4-3балла (или оценка «отлично») выставляется обучающемуся, если ондемонстрирует глубокое знание содержания вопроса; дает точные определения основныхпонятий; аргументированно и логически стройно излагает учебный материал; иллюстрируетсвой ответ актуальными примерами (типовыми и нестандартными), в том числесамостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросахпреподавателя.

2 балла (или оценка «хорошо») выставляется обучающемуся, если он владеетсодержанием вопроса, но допускает некоторые недочеты при ответе; допускаетнезначительные неточности при определении основных понятий; недостаточноаргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свойответ типовыми примерами.

1 балл (или оценка «удовлетворительно») выставляется обучающемуся, если оносвоил основные положения контролируемой темы, но недостаточно четко дает определениеосновных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа;нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если онне владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основныеопределения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе наних грубые ошибки.

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ЛАБОРАТОРНЫХ РАБОТ

Лабораторная работа № 1 Разработка криптографической программы «Алгоритм RSA»

1. В чём заключается алгоритм RSA?
2. Для чего и почему используют комбинированные криптоалгоритмы?
3. В чём заключаются достоинства и недостатки асимметричных алгоритмов?
4. В чём заключаются достоинства и недостатки симметричных алгоритмов?
5. Какие параметры блочных шифров влияют на его криптостойкость?

Лабораторная работа № 2 Разработка криптографической программы «Шифр Виженера»

1. Заданы две подстановки Вижинера с периодами d1=56 и d2=33, применяемые последовательно. Каков будет общий период такого шифра?
2. Каким способом осуществляется подавление телефонных закладок в устройстве, описанном в файле DEV3.doc.?
3. Какова зона подавления, которое обеспечивает устройство, описанном в файле DEV31.doc.?
4. Какой текст называется открытым?
5. Какой текст называется закрытым?
6. Что такое ключ?

Лабораторная работа № 3 «Настройка межсетевого экрана в операционной системе Windows»

1) Дайте определение межсетевого экрана?
2) В чем заключается механизм межсетевого экранирования?
3) В чем отличия программных и программно-аппаратных МЭ?
4) От каких угроз не может защитить МЭ?
5) Если на ПК будет установлено два МЭ, будут ли они конфликтовать?
6) С какими трудностями встретится пользователь при наличии двух МЭ

на ПК?

7) Какие достоинства и недостатки есть при наличии установленного программного МЭ на ПК?

Лабораторная работа №4 «Шифрование с помощью программы TrueCrypt»

1. Для какой цели используются группы в программе TrueCrypt?
2. Какие поля по умолчанию используются в записях? Можно ли добавить дополнительные поля в записях?
3. Какие типы паролей можно создавать с помощью генератора паролей? Дайте их краткую характеристику.
4. Объясните, что такое пасскарта в программе TrueCrypt?
5. В каком виде хранятся пароли в программе TrueCrypt по умолчанию?

Критерии оценки:

6-5 баллов (или оценка «отлично») выставляется обучающемуся, если ондемонстрирует глубокое знание содержания вопроса; дает точные определения основныхпонятий; аргументированно и логически стройно излагает учебный материал; иллюстрируетсвой ответ актуальными примерами (типовыми и нестандартными), в том числесамостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросахпреподавателя.

4-3 балла (или оценка «хорошо») выставляется обучающемуся, если он владеетсодержанием вопроса, но допускает некоторые недочеты при ответе; допускаетнезначительные неточности при определении основных понятий; недостаточноаргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свойответ типовыми примерами.

2-1 балла (или оценка «удовлетворительно») выставляется обучающемуся, если оносвоил основные положения контролируемой темы, но недостаточно четко дает определениеосновных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа;нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если онне владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основныеопределения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе наних грубые ошибки.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1.Законы, нормативные акты, стандарты относятся к мерам защиты субъектов информационных отношений:
1) административным
2) законодательным
3) процедурным

2.Качество передачи сигналов передачи данных оцениваются
1) искажениями формы сигналов
2) отсутствием искажения в принятой информации
3) числом ошибок в принятой информации, т.е. верностью передачи.

3. Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления — это
1) данные
2) информация
3) знания

4. Угроза безопасности – это:
1) совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации
2) нарушение целостности информации
комплекс мероприятий, проводимых для взлома информации

5. К параметрам системы защиты информации не относится:
1) входы и выходы системы
2) процессы внутри системы, занимающиеся преобразованием информации
цели и задачи

6.К важным свойствам информации относится:
1) полезность
2) доступность
новизна

7.Конфиденциальность информации – это:
1) действия, проводимые с целью закрытия доступа к информации субъектов, не имеющих на это право
2) состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право
состояние информации, при котором доступ к ней субъектами, не имеющими на это права, осуществляется лишь в некоторых случаях

8. Состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно?
1) допустимость
2) доступность
3) целостность

9. Что представляет собой предотвращение пассивных атак для передаваемых или хранимых данных:
1) конфиденциальность
2) контроль доступа
3) аутентификация

10. Принцип Кирхгофа:
1) секретность ключа определена секретностью открытого сообщения
2) секретность информации определена скоростью передачи данных
3) секретность закрытого сообщения определяется секретностью ключа

11. ЭЦП – это:
1) электронно-цифровой преобразователь
2) электронно-цифровая подпись
3) электронно-цифровой процессор

12. Какие существуют основные средства защиты данных?
1) резервное копирование наиболее ценных данных
2) аппаратные средства
3) программные средства

13. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
1. а) Сотрудники
2. б) Хакеры
3. в) Атакующие
4. г) Контрагенты (лица, работающие по договору)

14. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
1) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
2) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
3) Улучшить контроль за безопасностью этой информации
4) Снизить уровень классификации этой информации

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

1) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
2) Необходимый уровень доступности, целостности и конфиденциальности
3) Оценить уровень риска и отменить контрмеры
4) Управление доступом, которое должно защищать данных

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

1) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
2) Когда риски не могут быть приняты во внимание по политическим соображениям
3) Когда необходимые защитные меры слишком сложны
4) Когда стоимость контрмер превышает ценность актива и потенциальные потери

17. Эффективная программа безопасности требует сбалансированного

1) Технических и нетехнических методов
2) Контрмер и защитных механизмов
3) Физической безопасности и технических средств защиты
4) Процедур безопасности и шифрования

18. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

1) Много информации нужно собрать и ввести в программу
2) Руководство должно одобрить создание группы
3) Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
4) Множество людей должно одобрить данные

19. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

Варианты ответа:

1) Много информации нужно собрать и ввести в программу
2) Руководство должно одобрить создание группы
3) Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
4) Множество людей должно одобрить данные

20. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?
1) Список стандартов, процедур и политик для разработки программы безопасности
2) Текущая версия ISO 17799
3) Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
4) Открытый стандарт, определяющий цели контроля

21. Из каких четырех доменов состоит CobiT?
1) Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
2) Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
3) Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
4) Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

22. Что представляет собой стандарт ISO/IEC 27799?
1) Стандарт по защите персональных данных о здоровье
2) Новая версия BS 17799
3) Определения для новой серии ISO 27000
4) Новая версия NIST 800-60

23. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?
1) COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам
2) COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень
3) COSO учитывает корпоративную культуру и разработку политик
4) COSO – это система отказоустойчивости

24.Что лучше всего описывает цель расчета ALE:
1)количественно оценить уровень безопасности среды
2)оценить потенциальные потери от угрозы в год
3) количественно оценить уровень безопасности среды

25. К конфиденциальной информации относятся документы, содержащие
1) государственную тайну
2) законодательные акты
3) "ноу-хау"
4) сведения о золотом запасе страны

26. Запрещено относить к информации ограниченного доступа
1) информацию о чрезвычайных ситуациях
2) информацию о деятельности органов государственной власти
3) документы открытых архивов и библиотек
4) все, перечисленное в остальных пунктах

27. К конфиденциальной информации не относится
1) коммерческая тайна
2) персональные данные о гражданах
3) государственная тайна
4) "ноу-хау"

28. Для успешной реализации концепции комплексной защиты при построении автоматизированной системы ...
1) необходимо создать нескольких последовательных зон безопасности, чтобы наиболее важная зона безопасности объекта находилась внутри других зон
2) следует установить некоторый приемлемый уровень безопасности без попыток создать абсолютную защиту
3) должны быть разработаны и регулярно использоваться все необходимые механизмы гарантированного обеспечения требуемого уровня защищенности информации
4) требуется предварительное ранжирование угроз по степени их важности с точки зрения влияния на технико-экономические показатели

29. Исходным пунктом проектирования систем защиты информации является ...
1) формирование требований к защите информации
2) определение значений важнейших параметров защищаемой информации
3) построение математической модели системы защиты
4) разработка процедур оперативного реагирования на непредвиденные ситуации

30. Для долгосрочного управления комплексной системой защиты характерно ...
1) использование только средств защиты, которые включены в состав системы защиты информации и находятся в работоспособном состоянии
2) большое внимание развитию и совершенствованию концепции защиты
3) преобладание процедур оперативного реагирования в случае возникновения непредвиденных ситуаций над иными процедурами управления

4) отсутствие изменений в архитектуре средств защиты и автоматизированной системы

31. Непрерывное слежение за функционированием механизмов защиты относится к показателям
1) планирования управлением защиты
2) календарно-планового руководства защитой информации
3) обеспечения повседневной деятельности средств защиты
4) оперативно-диспетчерского управления

32. Имеет целью организацию и обеспечение выполнения плановых мероприятий по защите информации
1) планирование управлением защиты
2) календарно-плановое руководство защитой информации
3) обеспечение повседневной деятельности средств защиты
4) оперативно-диспетчерское управление

33. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?
1) Анализ связующего дерева
2) AS/NZS
3) NIST
4) Анализ сбоев и дефектов

34. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?
1) Безопасная OECD
2) ISOIEC
3) OECD

35. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:
1) гаммирования
2) подстановки
3) кодирования
4) перестановки
5) аналитических преобразований

36. 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

37. Икусственные 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

38. 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

39. 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

40. 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

41. 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

42. 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.

43. 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

44. Перехват, который осуществляется путем использования оптической техники называется:
1) активный перехват
2) пассивный перехват
3) аудиоперехват
4) видеоперехват
5) просмотр мусора.

45. 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

46. Организационная структура службы информационной безопасности определяется?

1. требованиями законодательства
2. требованиями государственных и международных стандартов
3. потребностями в защите информационных ресурсах и возможностями в соответствии с оценками руководителей предприятия

47. В состав службы информационной безопасности предприятия могут быть включены?

1. отдел нормативной документации
2. отдел технической поддержки пользователей
3. отдел внутреннего аудита информационной безопасности
4. отдел персонала

48. Отбор персонала при назначении на должности, связанные с обработкой конфиденциальной информации, включает в себя?

1. психологическую оценку
2. проверку знания внутренних регламентов работы с информацией
3. оценку навыков использования средств обнаружения вторжений

49. В методологии работы с персоналом фигурируют такие понятия как?

1. социальная инженерия, человеческий фактор, человеко-машинная система
2. моделирование, анализ
3. контроль, система обработки данных

50. К задачам обучения и информационной работы с персоналом предприятия относится?

1. недопущение утечек информации с использованием уязвимостей в сетях и ПО
2. ознакомление с требованиями законодательства и локальных регламентов
3. противодействие методам "социальной инженерии"

51. Приемы социотехники основаны на?

1. особенностях человеческой психологии
2. недостатках организационных структур
3. недостатках программных и аппаратных средств защиты информации

52. Обучение персонала, ответственного за обработку информации, включает в себя?

1. изучение автоматизированных систем обнаружения вторжений
2. изучение приемов и методов защиты информации, необходимых для выполнения должностных обязанностей
3. ознакомление с возможными мерами ответственности в случае нарушения требований информационной безопасности

53. Основным противодействием методам "социальной инженерии" является?

1. повышение надежности криптографических алгоритмов
2. информационная работа с персоналом предприятия
3. страхование информационных ресурсов

54. "Социальная инженерия" — это?

1. метод нарушения информационной безопасности
2. метод защиты от нарушений информационной безопасности
3. метод осуществления общественных связей

55. Нарушения информационной безопасности с использованием социотехники предполагают?

1. социологическое обследование персонала предприятия
2. использование недостатков в организационной структуре предприятия
3. обман сотрудников предприятия

56. Регламент реагирования на инциденты должен предусматривать?

1. регламент круглосуточного дежурства технического персонала
2. распределение функций персонала в процессе реагирования на инциденты
3. соглашение с поставщиками ИТ-платформ о срочной поставке компонент, вышедших из строя в результате инцидентов

57. Обнаружение вторжений осуществляется на основе?

1. косвенных признаков, сигнатур и сообщений пользователей
2. внутренних признаков и сообщений администратора
3. внешних признаков

58. К косвенным признакам, по которым могут быть выявлены нарушения информационной безопасности, относятся?

1. опубликование конфиденциальной информации в открытых источниках
2. использование баз данных и учетных записей в нехарактерное время
3. резкое повышение нагрузки на информационные системы предприятия

59. На персонал, отвечающий за обнаружение вторжений, оказывает влияние такой негативный психологический фактор как?

1. круглосуточный режим дежурства
2. необходимость постоянно изучать новые методы анализа вирусов
3. частые ложные сообщения пользователей о предполагаемом заражении вирусами

60. Высокий уровень полномочий необходим для локализации длящихся нарушений в связи с тем, что?

1. локализация нарушений требует дорогостоящих услуг сторонних аналитиков
2. для локализации нарушений может потребоваться временное оперативное отключение важных информационных систем предприятия
3. для локализации нарушений может потребоваться проинформировать о нарушениях большое число пользователей информационных систем

61. Ущерб от нарушения информационной безопасности включает в себя?

1. уменьшение рыночной капитализации
2. упущенную выгоду
3. штрафные санкции за разглашение конфиденциальной информации

62. Расследование нападений, совершенных из корпоративной сети, по сравнению с нападением, совершенным из внешней сети, является?

1. более легким
2. более сложным
3. аналогичным по сложности

63. Выявление вторжения в процессе его совершения по сравнению с выявлением уже завершенного нарушения?

1. упрощает выявление нарушителя
2. усложняет выявление нарушителя
3. никак не влияет на сложность выявления нарушителя

64. Анализ действий нарушителя необходим для?

1. проверки правильности настроек систем защиты информации
2. установления сведений, известных нарушителю до нападения
3. установления круга контактов, которые могли быть у нарушителя до нападения

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

1. руководитель среднего звена
2. высшее руководство
3. владелец
4. пользователь

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

1. сотрудники
2. хакеры
3. атакующие
4. контрагенты (лица, работающие по договору)

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

1. снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
2. требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
3. улучшить контроль за безопасностью этой информации
4. снизить уровень классификации этой информации

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

1. типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
2. необходимый уровень доступности, целостности и конфиденциальности
3. оценить уровень риска и отменить контрмеры
4. управление доступом, которое должно защищать данные

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

1. владельцы данных
2. пользователи
3. администраторы
4. руководство

70. Что такое процедура?

1. правила использования программного и аппаратного обеспечения в компании
2. пошаговая инструкция по выполнению задачи
3. руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
4. обязательные действия

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

1. поддержка высшего руководства
2. эффективные защитные меры и методы их внедрения
3. актуальные и адекватные политики и процедуры безопасности
4. проведение тренингов по безопасности для всех сотрудников

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

1. никогда, для обеспечения хорошей безопасности нужно учитывать и снижать все риски
2. когда риски не могут быть приняты во внимание по политическим соображениям
3. когда необходимые защитные меры слишком сложны
4. когда стоимость контрмер превышает ценность актива и потенциальные потери

73. Что такое политики безопасности?

1. пошаговые инструкции по выполнению задач безопасности
2. общие руководящие требования по достижению определенного уровня безопасности
3. широкие, высокоуровневые заявления руководства
4. детализированные документы по обработке инцидентов безопасности

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

1. анализ рисков
2. анализ затрат / выгоды
3. результаты ALE
4. выявление уязвимостей и угроз, являющихся причиной риска

75. Что лучше всего описывает цель расчета ALE?

1. количественно оценить уровень безопасности среды
2. оценить возможные потери для каждой контрмеры
3. количественно оценить затраты / выгоды
4. оценить потенциальные потери от угрозы в год

76. Тактическое планирование – это?

1. среднесрочное планирование
2. долгосрочное планирование
3. ежедневное планирование
4. планирование на 6 месяцев

77.Что является определением воздействия (exposure) на безопасность?

1. нечто, приводящее к ущербу от угрозы
2. любая потенциальная опасность для информации или систем

3. любой недостаток или отсутствие информационной безопасности
4. потенциальные потери от угрозы

78. Эффективная программа безопасности требует сбалансированного применения?

1. технических и нетехнических методов
2. контрмер и защитных механизмов
3. физической безопасности и технических средств защиты
4. процедур безопасности и шифрования

79. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют?

1. внедрение управления механизмами безопасности
2. классификацию данных после внедрения механизмов безопасности
3. уровень доверия, обеспечиваемый механизмом безопасности
4. соотношение затрат / выгод

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

1. только военные имеют настоящую безопасность
2. коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
3. военным требуется больший уровень безопасности, т.к. их риски существенно выше
4. коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

81. Как рассчитать остаточный риск?

1. угрозы * риски * ценность актива
2. (угрозы * ценность актива * уязвимости) * риски
3. SLE * частоту ALE
4. (угрозы * уязвимости * ценность актива) * недостаток контроля

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

1. делегирование полномочий
2. количественная оценка воздействия потенциальных угроз
3. выявление рисков

4. определение баланса между воздействием риска и стоимостью необходимых контрмер

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

1. поддержка
2. выполнение анализа рисков
3. определение цели и границ
4. делегирование полномочий

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

1. чтобы убедиться, что проводится справедливая оценка
2. это не требуется, для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
3. поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
4. поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

85. Что является наилучшим описанием количественного анализа рисков?

1. анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
2. метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
3. метод, сопоставляющий денежное значение с каждым компонентом оценки рисков
4. метод, основанный на суждениях и интуиции

86. Почему количественный анализ рисков в чистом виде не достижим?

1. он достижим и используется
2. он присваивает уровни критичности. их сложно перевести в денежный вид
3. это связано с точностью количественных элементов
4. количественные измерения должны применяться к качественным элементам

87. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

1. много информации нужно собрать и ввести в программу
2. руководство должно одобрить создание группы
3. анализ рисков не может быть автоматизирован, что связано с самой природой оценки
4. множество людей должно одобрить данные

88. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?

1. стандарты
2. должный процесс (Due process)
3. должная забота (Due care)
4. снижение обязательств

89. Наиболее распространены средства воздействия на сеть офиса?

1. слабый трафик, информационный обман, вирусы в интернет
2. вирусы в сети, логические мины (закладки), информационный перехват
3. компьютерные сбои, изменение администрирования, топологии

90. Утечкой информации в системе называется ситуация, характеризуемая?

1. потерей данных в системе
2. изменением формы информации
3. изменением содержания информации

91. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются?

1. целостность
2. доступность
3. актуальность

92. Угроза информационной системе (компьютерной сети) — это?

1. вероятное событие
2. детерминированное (всегда определенное) событие
3. событие, происходящее периодически

93. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется?

1. регламентированной
2. правовой
3. защищаемой

94. Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке?

1. программные, технические, организационные, технологические
2. серверные, клиентские, спутниковые, наземные
3. личные, корпоративные, социальные, национальные

95. Окончательно, ответственность за защищенность данных в компьютерной сети несет?

1. владелец сети
2. администратор сети
3. пользователь сети

96. Политика безопасности в системе (сети) — это комплекс?

1. руководств, требований обеспечения необходимого уровня безопасности
2. инструкций, алгоритмов поведения пользователя в сети
3. нормы информационного права, соблюдаемые в сети

97. Наиболее важным при реализации защитных мер политики безопасности является?

1. аудит, анализ затрат на проведение защитных мер
2. аудит, анализ безопасности
3. аудит, анализ уязвимостей, риск-ситуаций

98. Основная масса угроз информационной безопасности приходится на?

1. троянские программы
2. шпионские программы
3. черви

99. Какой вид идентификации и аутентификации получил наибольшее распространение?

1. системы PKI
2. постоянные пароли
3. одноразовые пароли

100. Какие угрозы безопасности информации являются преднамеренными?

1. ошибки персонала
2. открытие электронного письма, содержащего вирус
3. не авторизованный доступ

Задания в открытой форме

1. Конфиденциальностью информации называется……
2. К коммерческой тайне относится информация……
3. Информационной безопасностью предприятия является……
4. В состав системы защиты информации входят обеспечивающие подсистемы……
5. Под угрозой безопасности информации понимается……
6. Причинами информационных угроз являются……
7. Основные компьютерные вирусы……
8. К основным законам информационной безопасности РФ относятся законы……
9. Основными принципами политики безопасности являются……
10. Политика безопасности верхнего уровня включает……
11. Удаленный доступ к сервису организован……
12. Политика управления паролями включает……
13. Системный подход к защите информации базируется на принципах……
14. В состав организационно-технических мер входит……
15. Межсетевые экраны применяют для……
16. Технические средства противодействия классифицируются……
17. В состав службы безопасности входят подразделения……
18. К мерам по защите информации в интернете относятся……
19. Для защиты электронной почты используется……
20. Для защиты от вирусов можно использовать……
21. К антивирусным программам относятся……
22. План защиты включает……
23. Ответственным за определение уровня классификации информации является……
24. Политики безопасности – это……
25. К посторонним лицам - нарушителям информационной безопасности относятся……

Задания на установление соответствия

1. Установите взаимно однозначное соответствие

1	Информационная система (ИС)	А	предназначена для эффективной эксплуатации экономической ИС
2	Автоматизированная ИС	Б	система сбора, хранения, накопления, поиска и передачи информации, применяемая в процессе управления или принятия решений.
3	Автоматизированная ИС	В	совокупность информ., экономико-математических методов и моделей, аппаратных, программных, организационных, технологических средств и специалистов

2. Установите взаимно однозначное соответствие

1	ИС управления технологическими процессами	А	предназначены для автоматизации функций инженеров-проектировщиков, конструкторов, архитекторов, дизайнеров при создании новой техники или технологии.
2	ИС автоматизированного проектирования	Б	используются для автоматизации всех функций фирмы и охватывают весь цикл работ от планирования деятельности до сбыта продукции.
3	Интегрированные (корпоративные) ИС	В	оказывает устойчивую тенденцию роста спроса на информационные системы организационного управления.
4	Анализ современного состояния рынка ИС	Г	служат для автоматизации функций производственного персонала по контролю и управлению производственными операциями.

3. Установите взаимно однозначное соответствие

1	Гибкость системы-	А	определяется как частное от деления фактического

			количества группировок на величину емкости системы.
2	Емкость системы-	Б	это способность допускать включение новых признаков, объектов без разрушения структуры классификатора.
3	Степень заполненности системы-	В	это наибольшее количество классификационных группировок, допускаемое в данной системе классификации.

4. Установите взаимно однозначное соответствие

1.	Выявление критически важной информации	А	на этом этапе выполняется непосредственно специалистами, проводящими аудит. От результатов этой работы зависит выбор схемы построения информационной безопасности
2	Выявление слабых мест в корпоративной безопасности	Б	Это завершающий этап аудита, в ходе которого на основании проведенного анализа составляется список конкретных мер, которые необходимо принять для охраны корпоративных секретов компании
3	Оценка возможностей защиты информации	В	на этом этапе происходит определение тех документов и данных, безопасность которых имеет огромное значение для компании, а утечка – несет огромные убытки.

5. Установите взаимно однозначное соответствие

1	Конфиденциальный аспект	А	Это комплексная работа при защите данных, которая обеспечит защиту от сбоев в работе и уничтожения самих данных.
2	Целостностный аспект	Б	Включает в себя обеспечение надежного и эффективного доступа к защищаемой информации только

			проверенных лиц.
2	Аспект доступности	В	Означает, что нужно тщательно контролировать работу с данными, чтобы устранить возможность их утечки, а также предотвратить несанкционированный доступ к ним со стороны неизвестных людей

6. Установите взаимно однозначное соответствие

1	Аппаратная угроза	А	есть вероятность некорректной работы программного обеспечения
2	Вероятность утечки	Б	существует вероятность нарушения работоспособности оборудования
3	Нестабильность ПО	В	возможен несанкционированный доступ к данным и их потеря

7. Установите взаимно однозначное соответствие

1	Антивирусная программа-	А	специализированное программное обеспечение, предназначенное для защиты компании от утечек информации
2	CloudAV-	Б	специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ .
3	DLP-решения-	В	заключается в преобразовании ее составных частей (слов, букв, слогов, цифр) с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении ее к неявному виду
4	Криптографическое преобразование-	Г	одно из облачных решений информационной безопасности, что применяет легкое программное обеспечение

			агента на защищенном компьютере, выгружая большую часть анализа информации в инфраструктуру провайдер

8. Установите взаимно однозначное соответствие

1.	Защита информации-	А	это желаемый результат защиты информации. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.
2	Объект защиты-	Б	это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
3	Цель защиты информации-	В	степень соответствия результатов защиты информации поставленной цели
4	Эффективность защиты информации-	Г	информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации

9. Установите взаимно однозначное соответствие

1	Защита информации от утечки-	А	деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или

			собственником либо владельцем информации прав или правил доступа к защищаемой информации.
2	Защита информации от разглашения-	Б	деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.
3	Защита информации от НСД-	В	Деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
4	Система защиты информации -	Г	совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

10. Установите взаимно однозначное соответствие

1	Доступ к информации -	А	это способность информации или некоторого информационного ресурса быть доступными для конечного пользователя в соответствии с его оперативными потребностями.
2	Оперативность доступа к	Б	субъект, осуществляющий

	информации-		владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.
3	Собственник информации-	В	получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.
4	Владелец информации -	Г	субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.

11. Установите взаимно однозначное соответствие

1	Способ защиты информации -	А	совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения информационной безопасности системы (сети).
2	Средство защиты информации-	Б	порядок и правила применения определенных принципов и средств защиты информации.
3	Комплекс средств защиты (КСЗ)-	В	средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.
4	Техника защиты информации-	Г	Техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации

12. Установите взаимно однозначное соответствие

1	Операционная гарантированность	А	охватывает весь жизненный цикл ИС, то есть периоды

			проектирования, реализации, тестирования, продажи и сопровождения.
2	Технологическая гарантированность	Б	это совокупность защитных механизмов ИС
3	Доверенная вычислительная база	В	относится к архитектурным и реализационным аспектам системы

13. Установите взаимно однозначное соответствие

1	Произвольное управление доступом-	А	Представляют собой свойства (характеристики) объектов и (или) субъектов доступа
2	Безопасность повторного использования объектов-	Б	основано на сопоставлении меток безопасности субъекта и объекта.
3	Метки безопасности-	В	это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит.
4	Принудительное (или мандатное) управление доступом-	Г	важное дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения конфиденциальной информации из "мусора"

14. Установите взаимно однозначное соответствие

1	Ядро безопасности-	А	проверка подлинности идентификаторов сущностей с помощью различных (преимущественно криптографических) методов.
2	Аутентификация-	Б	показатель реально обеспечиваемого уровня безопасности, отражающий степень эффективности и надежности реализованных

			средств защиты и их соответствия поставленным задачам
3	Идентификация-	В	совокупность аппаратных, программных и специальных компонентов ВС, реализующих функции защиты и обеспечения безопасности.
4	Адекватность-	Г	процесс распознавания сущностей путем присвоения им уникальных меток

15. Установите взаимно однозначное соответствие

1	Математическое и программное обеспечение (МО, ПО)-	А	совокупность правовых норм, определяющих создание, юридический статус и функционирование информационных систем, регламентирующих порядок получения, преобразования и использования информации
2	Организационное обеспечение (ОО)-	Б	совокупность математических методов, моделей, алгоритмов и программ для реализации целей и задач информационной системы, а также нормального функционирования комплекса технических средств
3	Правовое обеспечение (Пр.О) -	В	совокупность методов и средств, регламентирующих взаимодействие работников с техническими средствами и между собой в процессе разработки и эксплуатации информационной системы.

16. Установите взаимно однозначное соответствие

1	Сопровождение-	А	проверка функционального соответствия системы

			показателям, определенным на этапе анализа
2	Функционирование-	Б	обеспечение штатного процесса эксплуатации системы на предприятии заказчика.
3	Внедрение-	В	штатный процесс эксплуатации в соответствии с основными целями и задачами ИС
4	Тестирование-	Г	установка и ввод системы в действие

17. Установите взаимно однозначное соответствие

1	Принцип интеграции	А	заключается в том, что при декомпозиции должны быть установлены такие связи между структурными компонентами системы, которые обеспечивают цельность корпоративной системы и ее взаимодействие с другими системами
2	Принцип системности	Б	предполагает рассмотрение всех сторон объекта исследования в его связи и зависимости с другими процессами и явлениями
3	Принцип комплексности	В	заключается в том, что обрабатываемые данные (документы) вводятся в систему только один раз и затем многократно используются для решения возможно большего числа задач

18. Установите взаимно однозначное соответствие

1	CRM-	А	программная система, охватывающая ключевые процессы деятельности и

			управления, позволяющая получить самый общий взгляд на работу предприятия
2	SCM-	Б	система планирования потребностей в материалах, одна из наиболее популярных в мире логистических концепций, на основе которой разработано и функционирует большое число микрологистических систем
3	MRP-	В	управления цепочками поставок
4	ERP-	Г	управление отношениями с клиентами - бизнес-стратегия, предназначенная для оптимизации доходов, прибыльности и удовлетворенности клиентов

19. Установите взаимно однозначное соответствие

1	Специальные категории ПДн-	А	данные, характеризующие биологические или физиологические особенности субъекта и используемые для установления личности, например, фотография или отпечатки пальцев
2	Биометрические ПДн-	Б	обработка персональных данных субъектов, не являющихся работниками вашей организации
3	Общедоступные ПДн-	В	относятся информация о национальной и расовой принадлежности субъекта, о религиозных, философских либо политических убеждениях, информацию о здоровье и интимной жизни субъекта
4	Иные категории ПДн-	Г	сведения о субъекте, полный и неограниченный доступ к которым предоставлен

			самим субъектом

20. Установите взаимно однозначное соответствие

1	Соответствие направлению импортозамещения-	А	наличие и состав индивидуально настраиваемых параметров, гибкость настройки позволят оценить применимость решения к принятой парадигме развития процессов обеспечения ИБ
2	Функциональные особенности-	Б	наличие развитых встроенных и интегрируемых подсистем позволит в начальном периоде эксплуатации ограничиться использованием одного продукта, без увеличения количества используемых интерфейсов
3	Интеграционные возможности-	В	отчетность, и удобство, и глубина погружения при навигации в рамках интерфейса системы
4	Дополнительные критерии-	Г	позволит оценить, можно ли использовать решение в рамках государственных инициатив по поддержке отечественного производителя и борьбе с санкциями.

Задания на установление правильной последовательности

1. Выберите правильную последовательность этапов работы по обеспечению режима ИБ:

1. Выявление максимально полного множества потенциальных угроз, способов и каналов их осуществления;

2. Определение и выработка политики информационной безопасности;

3. Определение совокупности целей создания системы иб и сферы (границ) ее функционирования;

4. Выявление уязвимостей, проведение оценки рисков, формирование методик управление рисками;

2. Установить этапы защиты от угроз безопасности:

1. Предоставление персоналу защищенный удаленный доступ к информационным ресурсам

2. Обеспечение безопасного доступа к открытым ресурсам внешних сетей и Internet

3. Защита внешних каналов передачи информации

4. Разработка политики информационной безопасности

5. Анализ угрозы безопасности

3. Установить этапы стадии исполнения компьютерных вирусов:

1. Выполнение деструктивных функций

2. Передача управления программе-носителю вируса

3. Поиск жертвы

4. Заражение найденной жертвы

4. Загрузка вируса в память

4. Установить этапы построения системы антивирусной защиты сети:

1. Реализация плана антивирусной безопасности

2. Проведение анализа объекта защиты и определение основных принципов обеспечения антивирусной безопасности

3. Разработка политики антивирусной безопасности

4. Разработка плана обеспечения антивирусной безопасности

5. Выберите последовательность приоритетных этапов защиты информации:

1. Защита информации от несанкционированного доступа;

2. Защита информации в системах связи;

3. Защита юридической значимости электронных документов;

4. Защита конфиденциальной информации от утечки по каналам побочных электромагнитных излучений и наводок;

5. Защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ;

6. Защита от несанкционированного копирования и распространения программ и ценной компьютерной информации.

6. Установить этапы построения программы обеспечения безопасности:

1. Проведение разъяснительных мероприятий и обучения персонала для поддержки требуемых мер безопасности

2. Регулярный контроль пошаговой реализации плана безопасности

3. Установление уровня безопасности

4. Формирование политики безопасности организации

5. Определение ценности технологических и информационных активов организации

7. Установить действия этапа анализа рисков:

1. Оценка вероятности того, что угроза будет реализована на практике

2. Оценка рисков технологических и информационных активов

3. Идентификация и оценка стоимости технологических и информационных активов

4. Анализ угроз, для которых технологические и информационные активыявляются целевым объектом

8. Установить последовательность процессов для обнаружения и выдачи сигнала тревоги:

1. Одно системное событие не является неизбежно достаточным, чтобы утверждать, что это опасность

2. Если результат этой совокупности превышает пороговую величину, выдается сигнал тревоги

3. Совокупность событий должна сравниваться с заранее установленной пороговой величиной

4. Каждое нарушение безопасности должно генерировать системное событие

9. Расположить параметры для группировки данных на сервере сбора информации об атаке:

1. Дата, время

2. Протокол

3. Порт получателя

4. Номер агента

5. IP-адрес атакующего

6. Тип атаки

10. Расположить в порядке возрастания даты разработки стандартов информационной безопасности:

1. ISO 27001:2005

2. ISO/IEC 17799

3. ISO/IEC 15408

4. «Критерии оценки доверенных компьютерных систем»

11. Расположить этапы процесса управления рисками информационной безопасности:

1. Классификация рисков, выбор методологии оценки рисков и проведение оценки

2. Анализ угроз и их последствий, определение слабостей в защите

3. Выбор, реализация и проверка защитных мер

4. Оценка остаточного риска

5. Идентификация активов и ценности ресурсов, нуждающихся в защите

6. Выбор анализируемых объектов и степени детальности их рассмотрения

12. Расположить этапы проведения аудита информационной безопасности:

1. Разработка рекомендаций по повышению уровня защиты автоматизированной системы
2. Анализ полученных данных
3. Сбор исходных данных
4. Разработка регламента проведения аудита

14. Расположите в правильном порядке объекты защиты

1. __класс. Ценность данных определяется их собственником (коммерческая тайна)
2. __класс. Данные имеют ограниченный доступ на основании федеральных законов (персональные данные, банковская тайна)
3. __класс — государственная тайна. Информационные объекты, имеющие ценность, присутствуют в жизни организации в виде

15. Расположить этапы процесса комплекса превентивных мер

1.подача и рассмотрение заявки;
2. предварительное ознакомление специалистов с аттестуемыми объектами;
3.разработка программы и методики испытаний;
4. запрос и получение специалистами необходимой технической документации;
5. проведение испытаний;
6. оформление, регистрация и выдача аттестата (сертификата соответствия) на оборудование и помещения.

16. Восстановите алгоритм испытаний

1. анализ информационных потоков, информационной системы в целом и отдельных объектов, технических средств, программного обеспечения, технической документации на внедренную систему защиты ИС в целом и от утечек по техническим каналам (ТКУИ);
2.оценка правильности классификации информационных объектов, выбора и применения технических средств защиты для блокирования опасных ТКУИ, возможных угроз несанкционированного доступа к информации и специальных воздействий на информацию (носители);
3. проверка сертификатов на программное обеспечение и техническое оборудование для защиты информации;
4. проведение аттестационных испытаний и оформление протоколов;

5.оформление заключения по результатам проверок.

17. Выберите последовательность проведения моделирования угроз:

1. Определение негативных последствий от угроз безопасности информации.
2. Определение объектов воздействия угроз безопасности информации.
3. Оценка возможности реализации угроз и их актуальности.

18. Установить этапы реализации в ОС механизмов безопасности в порядке их внедрения:

1. Создание кольцевой системы защиты процессора
2. Реализация аутентификации пользователя
3. Реализация многозадачности
4. Создание виртуальных контейнеров для запуска приложений

19. Выберите правильную последовательность этапов по созданию системы защиты персональных данных:

1. Опытная и промышленная эксплуатация
2. Проектный этап
3. Аттестация или декларирование
4. Предпроектный этап

20. Выберите правильную последовательность этапов разработки профиля защиты.

1. Анализ среды применения ИТ-продукта с точки зрения
2. безопасности.
3. Выбор профиля-прототипа.
4. Синтез требований.

Шкала оценивания результатов тестирования: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 баллов (установлено положением П 02.016).

Максимальный балл за тестирование представляет собой разность двух чисел: максимального балла по промежуточной аттестации для данной формы обучения (36) и максимального балла за решение компетентностно-ориентированной задачи (6).

Балл, полученный обучающимся за тестирование, суммируется с баллом, выставленным ему за решение компетентностно-ориентированной задачи.

Общий балл по промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

2.2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

1. Зашифровать строку «Стремитесь не к успеху, а к ценностям, которые он дает», используя шифрование с помощью таблицы Виженера
2. Зашифровать строку «Лучшая месть – огромный успех», используя шифр RSA
3. Зашифровать строку «Упади семь раз и восемь раз поднимись.», используя алгоритм шифрования Эль-Гамаля
4. Зашифровать строку «Я не жертва обстоятельств, я - результат моих решений.», используя алгоритм шифрования Деффи-Хеллмана
5. Зашифровать строку «Надо любить жизнь больше, чем смысл жизни», используя шифрование с помощью таблицы Виженера
6. Зашифровать строку «Лучшая месть – огромный успех», используя шифр RSA
7. Зашифровать строку «Если нет ветра, беритесь за вёсла.», используя алгоритм шифрования Эль-Гамаля
8. Зашифровать строку «Я не провалил тест. Я просто нашел сто способов написать его неправильно.», используя алгоритм шифрования Деффи-Хеллмана
9. Включите шифрование твердотельного накопителя используя операционную систему Windows 10
10. Воспользовавшись операционной системой Linux произведите сканирование локальной сети на поиск подозрительных устройств
11. Зашифровать строку «Научитесь говорить “Я не знаю”, и это уже будет прогресс.», используя шифр RSA
12. Зашифровать строку «Жизнь - это то, что с тобой происходит, пока ты строишь планы.», используя шифрование с помощью таблицы Виженера

13. Зашифровать строку «Мы становимся тем, о чем мы думаем.», используя алгоритм шифрования Эль-Гамаля
14. Опишите модель поведения нарушителя для административного корпуса завода ООО «СтройМаш»
15. Зашифровать строку «Стоит только поверить, что вы можете – и вы уже на полпути к цели.», используя шифр RSA
16. Зашифровать строку «Я не провалил тест. Я просто нашел сто способов написать его неправильно.», используя алгоритм шифрования Деффи-Хеллмана
17. Не имея непосредственного доступа к персональному компьютеру, совершите удаленный запуск приложений на нём
18. Зашифровать строку «Неудача – это просто возможность начать снова, но уже более мудро.» используя шифрование с помощью таблицы Виженера
19. Произведите установку антивирусного программного обеспечения на персональный компьютер
20. Зашифровать строку «Ты становишься тем, во что веришь.», используя алгоритм шифрования Деффи-Хеллмана

Шкала оценивания решения компетентностно-ориентированной задачи: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 (установлено положением П 02.016).

Максимальное количество баллов за решение компетентностно-ориентированной задачи – 6 баллов.

Балл, полученный обучающимся за решение компетентностно-ориентированной задачи, суммируется с баллом, выставленным ему по результатам тестирования. Общий балл промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

Критерии оценивания решения компетентностно-ориентированной задачи (нижеследующие критерии оценки являются примерными и могут корректироваться):

6-5 баллов выставляется обучающемуся, если решение задачи демонстрирует глубокое понимание обучающимся предложенной проблемы и разностороннее ее рассмотрение; свободно конструируемая работа представляет собой логичное, ясное и при этом краткое, точное описание хода решения задачи (последовательности (или выполнения) необходимых трудовых действий) и формулировку доказанного, правильного вывода (ответа); при этом обучающимся предложено несколько вариантов решения или оригинальное, нестандартное решение (или наиболее эффективное, или наиболее рациональное, или оптимальное, или единственно правильное решение); задача решена в установленное преподавателем время или с опережением времени.

4-3 балла выставляется обучающемуся, если решение задачи демонстрирует понимание обучающимся предложенной проблемы; задача решена типовым способом в установленное преподавателем время; имеют место общие фразы и (или) несущественные недочеты в описании хода решения и (или) вывода (ответа).

2-1 балла выставляется обучающемуся, если решение задачи демонстрирует поверхностное понимание обучающимся предложенной проблемы; осуществлена попытка шаблонного решения задачи, но при ее решении допущены ошибки и (или) превышено установленное преподавателем время.

0 баллов выставляется обучающемуся, если решение задачи демонстрирует непонимание обучающимся предложенной проблемы, и (или) значительное место занимают общие фразы и голословные рассуждения, и (или) задача не решена.