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

Оценка защищенности информационных систем
(наименование учебной дисциплины)

10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы»
(код и наименование ОПОП ВО)

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

Тема №1 «Нормативная база оценки защищенности ИТ»

1. Существующие стандарты и методологии проверки и оценки защищенности ИТ и СУИБ.
2. История развития. ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011 – оценка функционирования СУИБ
3. ISO/IEC 27006:2011 и ГОСТ Р ИСО/МЭК 27006-2008 – требования к органам, осуществляющим аудит и сертификацию СУИБ.
4. ISO/IEC 27007:2011 и ISO/IEC 27008:2011 – руководства по аудиту СУИБ и средств управления ИБ, реализованных в СУИБ.
5. Существующие стандарты и методологии проверки и оценки защищенности ИТ и СУИБ: их отличия, сильные и слабые стороны.
6. ISO 19011:2002 и ГОСТ Р ИСО 19011-2003 – рекомендации по аудиту систем менеджмента качества и/или окружающей среды.

Тема №2 «Основные аспекты построения системы информационной безопасности»

1. Назовите 3 основных аспекта построения системы информационной безопасности.
2. Административный уровень информационной безопасности. Политика безопасности информационных систем.
3. Что произойдет с организацией, если система не будет введена в эксплуатацию?
4. Программно-технические меры безопасности. Понятие сервиса информационной безопасности. Архитектурная безопасность.
5. Понятие сервиса информационной безопасности. протоколирование и аудит.
6. Понятие сервиса информационной безопасности. управление и анализ защищенности.
7. Понятие сервиса информационной безопасности. обеспечение высокой доступности и отказоустойчивости.
8. Понятие сервиса информационной безопасности. экранирование и туннелирование.

Тема №3 «Базовые вопросы проверки защищенности ИТ»

1. Назовите методы формализации процессов.
2. Назовите цели и задачи формализации процессов.
3. Важность процесса с точки зрения управления ИБ
4. Участники процесса. Связи с другими процессами СУИБ.
5. Назовите основные процессы методы проверки защищенности. Понятие процессного подхода.

6. Назовите цели и задачи процессов оценки защищенности ИТ и СУИБ.
7. Охарактеризуйте защитные оболочки и перечень преград, применяемые в учебной компьютерной лаборатории.
8. Какие основные методы контроля доступа используются в известных вам информационных системах? В чем их достоинства и недостатки?
9. Постройте неформальную модель нарушителя для учебной компьютерной лаборатории.

Тема №4 «Виды проверок»

1. Назовите внутренние аудиты ИБ.
2. Назовите внешние аудиты ИБ.
3. Мониторинг ИБ. Самооценка ИБ.
4. Как проверяется достоверность источника?
5. Гарантии безопасности компьютерных систем в системе общих критериев.
6. Проверка полномочий субъектов на доступ к ресурсам.
7. Понятие сервиса информационной безопасности. протоколирование и аудит.
8. Анализ журнала аудита ОС на рабочем месте.
9. Анализ СУИБ со стороны высшего руководства организации.

Тема №5 «Внутренний аудит ИБ»

1. Анализ журнала аудита ОС на рабочем месте.
2. Назовите средства и системы аудита информационной безопасности.
3. Средства администрирования сетевых программно-аппаратных комплексов защиты информации.
4. Инструментальные средства аудита безопасности компьютерных систем, их возможности и недостатки.
5. Средствами администрирования систем обнаружения компьютерных атак.
6. Методики проведения аудита информационной безопасности.
7. Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.
8. Средства автоматизации комплексного аудита информационной безопасности.
9. Методы мониторинга и аудита, выявления угроз информационной безопасности компьютерных сетей.

Тема №6 «Внешний аудит ИБ»

1. Цели и задачи, принципы проведения, управление программой, этапы проведения.

2. Аудит безопасности компьютерных систем. Цели, стандарты, подходы.
3. Компетентность аудиторов. Взаимоотношения представителей аудиторской группы и проверяемых организаций.
4. Угрозы доступности. Основные угрозы целостности. Угрозы конфиденциальности.
5. Понятие сервиса информационной безопасности. управление и анализ защищенности.
6. Понятие сервиса информационной безопасности. протоколирование и аудит.
7. Аудит прикладных служб.
8. Применение инструментальных средств аудита безопасности компьютерных систем

Тема №7 «Системы анализа защищенности»

1. Классификация защищенности компьютерной системы по требованиям безопасности информации в системе общих критериев.
2. Виды систем, решаемые задачи, использование в целях оценки защищенности ИТ.
3. Понятие сервиса информационной безопасности. управление и анализ защищенности.
4. Выявление и построение схемы информационных потоков защищаемой информации в компьютерной сети.
5. Ранжирование обнаруженных уязвимостей по степени воздействия на защищаемую информацию.
6. Разработка политик безопасности для защищенных компьютерных систем
7. Порядок сертификации средств защиты информации для разработчика СЗИ.
8. Порядок сертификации защищенных информационных систем.
9. Тестирование состояния защищенности компьютерных систем от несанкционированного доступа с использованием сканеров безопасности.

Тема №8 «Системы обнаружения и предотвращения вторжений»

1. Назначение систем обнаружения атак. Классификация систем обнаружения атак.
2. Прямые и косвенные признаки атак. Методы обнаружения атак.
3. Сигнатурный анализ и обнаружение аномалий.
4. Классификация систем обнаружения атак (СОА).
5. Сетевые и узловые СОА.
6. Варианты размещения СОА.
7. Размещение сенсоров СОА.
8. Требования, предъявляемые к СОА.
9. Стандартизация в области обнаружения атак. Архитектура СОА.

10. Система определения маршрутов прохождения сетевых пакетов, обнаружения объектов сети, построения схемы сети.

Критерии оценки:

2 балла выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

1 балл выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных 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 выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

1.2 ВОПРОСЫ И ЗАДАНИЯ В ТЕСТОВОЙ ФОРМЕ

Тема 1

1 Чем регулируется ответственность за нарушение информационной безопасности во внешней среде с целью нанести вред владельцу информации, а также вопросы взаимоотношений между различными субъектами?

1. Внутренними корпоративными документами
2. федеральными законами рф, региональными, муниципальными и пр. нормативными актами
3. Международными стандартами в области информационной безопасности
4. Доктриной информационной безопасности

2 Чем регулируется ответственность за причинение вреда и ответственность за реализацию мероприятий по разработке, внедрению и использованию систем ИБ во внутренней среде?

1. Внутренними корпоративными документами
2. Действующим законодательством рф и стран, с которыми осуществляется бизнес

3. Международными стандартами в области информационной безопасности
4. Доктриной информационной безопасности

3 Режим защиты информации не устанавливается в отношении сведений, относящихся к:
1. Государственной тайне
2. Конфиденциальной информации
3. Персональным данным
4. Деятельности государственных деятелей

4 Режим документированной информации – это:
1. Выделенная информация по определенной цели
2. Выделенная информация в любой знаковой форме
3. Электронная информация, позволяющая ее идентифицировать
4. Электронный документ с электронно-цифровой подписью

5 За что отвечает программа информационной безопасности верхнего уровня в организации?
1. Контроль за тем, чтобы действия организации не противоречили федеральным и региональным законам и нормативным актам
2. Выработка стратегии организации в области информационной безопасности
3. Обеспечение надежной и экономичной защиты информационных подсистем, конкретных сервисов или групп однородных сервисов

6 За что отвечает программа информационной безопасности нижнего уровня в организации?
1. Контроль за тем, чтобы действия организации не противоречили федеральным и региональным законам и нормативным актам
2. Выработка стратегии организации в области информационной безопасности
3. Обеспечение надежной и экономичной защиты информационных подсистем, конкретных сервисов или групп однородных сервисов

Тема 2

7 Эффективная система 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

8 Что дает использование нейронных сетей при построении системы защиты информации?
1. Комплексность
2. Минимизацию ошибок первого и второго рода
3. Адаптивность

4. Универсальность
5. Наследование

9 Какой термин определяет защищенность жизненно важных интересов государственного или коммерческого предприятия от внутренних и внешних угроз, защиту кадрового и интеллектуального потенциала, технологий, данных и информации, капитала и прибыли, которая обеспечивается системой мер правового, экономического, организационного, информационного, инженерно-технического и социального характера?

1. Стратегическая безопасность
2. Информационная безопасность
3. Экономическая безопасность
4. Корпоративная безопасность

10 За что отвечает программа информационной безопасности нижнего уровня в организации?

1. Контроль за тем, чтобы действия организации не противоречили федеральным и региональным законам и нормативным актам
2. Выработка стратегии организации в области информационной безопасности
3. Обеспечение надежной и экономичной защиты информационных подсистем, конкретных сервисов или групп однородных сервисов

11 Чем регулируется ответственность за причинение вреда и ответственность за реализацию мероприятий по разработке, внедрению и использованию систем ИБ во внутренней среде?

1. Внутренними корпоративными документами
2. Действующим законодательством рф и стран, с которыми осуществляется бизнес
3. Международными стандартами в области информационной безопасности
4. Доктриной информационной безопасности

12 На каком этапе построения комплексной системы защиты предприятия принято строить модель нарушителя?

1. На первом
2. На втором
3. На третьем
4. На четвертом

Тема 3

13 Признак, не относящийся к охраноспособной информации – это …:

1. Доступ к охраноспособной информации ограничен только законом
2. Защита охраноспособной информации устанавливается законом

3. Доступ к охраноспособной информации ограничен владельцем информационных ресурсов

4. Охране подлежит только документированная информация

14 Какие три основные свойства информации достигаются с помощью защиты информации?

1. Актуальность, достоверность, защищенность
2. Отчуждаемость, правильность, упругость
3. Конфиденциальность, целостность, доступность
4. Нет правильного ответа

15 Цели информационной безопасности – своевременное обнаружение, предупреждение:

1. Несанкционированного доступа, воздействия в сети
2. Инсайдерства в организации
3. Чрезвычайных ситуаций

16 Основные объекты информационной безопасности:

1. Компьютерные сети, базы данных
2. Информационные системы, психологическое состояние пользователей
3. Бизнес-ориентированные, коммерческие системы

17 Основными рисками информационной безопасности являются:

1. Искажение, уменьшение объема, перекодировка информации
2. Техническое вмешательство, выведение из строя оборудования сети
3. Потеря, искажение, утечка информации

18 К основным принципам обеспечения информационной безопасности относится:

1. Экономической эффективности системы безопасности
2. Многоплатформенной реализации системы
3. Усиления защищенности всех звеньев системы

19 Основными субъектами информационной безопасности являются:

1. Руководители, менеджеры, администраторы компаний
2. Органы права, государства, бизнеса
3. Сетевые базы данных, фаерволлы

20 К основным функциям системы безопасности можно отнести все перечисленное:

1. Установление регламента, аудит системы, выявление рисков
2. Установка новых офисных приложений, смена хостинг-компании
3. Внедрение аутентификации, проверки контактных данных пользователей

Тема 5

21 В организации проводятся проверки «чистый стол», целью которых является выявление нарушений требований по хранению ключевых

носителей и конфиденциальных документов. К какому уровню обеспечения ИБ они относятся?

1. Законодательный
2. Административный
3. Процедурный
4. Научно-технический

22 Как называется бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена:

1. Угроза
2. Утечка
3. Уязвимость
4. Атака

23 Как называется пространство, в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств?

1. Ограниченная зона
2. Пограничная зона
3. Контролируемая зона
4. Зона 1

24 Как называется технический канал утечки информации, при котором производится съем информации с линии связи контактного подключения аппаратуры злоумышленника?

1. Электромагнитный
2. Электрический
3. Индукционный

Тема 6

25 Каким термином обозначается анализ регистрационной информации системы защиты?

1. Мониторинг
2. Аудит
3. Аккредитация
4. Сертификация

26 Как называется технический канал утечки информации, при котором производится бесконтактный съем информации с кабельных линий связи?

1. Электромагнитный
2. Электрический
3. Индукционный

27 В каких технических каналах утечки акустической информации основным средством съема информации является микрофон?

1. Воздушные

2. Вибрационные
3. Электроакустические
4. Параметрические

Тема 7

28 К какой из составляющих интегрального комплекса физической защиты информационной инфраструктуры относятся охранные датчики, датчики напряжения питания и датчики защиты аппаратуры?

1. Система опознавания
2. Механическая система защиты
3. Система оповещения
4. Оборонительная система защиты

29 К какой из составляющих интегрального комплекса физической защиты информационной инфраструктуры относятся камеры видеонаблюдения?

1. Система опознавания
2. Механическая система защиты
3. Система оповещения
4. Оборонительная система защиты

30 К какой из составляющих интегрального комплекса физической защиты информационной инфраструктуры относятся решетки и ставни на окнах?

1. Система опознавания
2. Механическая система защиты
3. Система оповещения
4. Оборонительная система защиты

31 К какой из составляющих интегрального комплекса физической защиты информационной инфраструктуры относятся считыватели карт на входе и выходе?

1. Система опознавания
2. Механическая система защиты
3. Система управления доступом
4. Оборонительная система защиты

32 К какой из составляющих интегрального комплекса физической защиты информационной инфраструктуры относятся громкоговорители и сирены?

1. Система опознавания
2. Механическая система защиты
3. Система управления доступом
4. Оборонительная система защиты

Тема 8

33 Недостатком какого метода обнаружения вирусов является большое количество ложных срабатываний антивирусных средств?

1. Сканирование
2. Эвристический анализ
3. Обнаружение изменений
4. Использование резидентных сторожей

34 Недостатком какого метода является невозможность обнаружения вируса в файлах, которые поступают в систему уже зараженными?

1. Сканирование
2. Эвристический анализ
3. Обнаружение изменений
4. Использование резидентных сторожей

35 Для какого метода обнаружения вирусов необходимо регулярное обновление сведений о новых вирусах?

1. Сканирование
2. Эвристический анализ
3. Обнаружение изменений
4. Использование резидентных сторожей

36 Какой метод обнаружения вирусов базируется на применении программ-ревизоров, которые следят за изменениями файлов и дисковых секторов на компьютере?

1. Сканирование
2. Эвристический анализ
3. Обнаружение изменений
4. Использование резидентных сторожей

37 Какие типы систем обнаружения вторжения существуют?

1. Сетевые
2. Узловые
3. Распределенные
4. Локальные

Критерии оценки:

2 балла по шкале БРС выставляется обучающемуся, если даны правильные ответы на 2 вопроса из 2;

1 балл по шкале БРС выставляется обучающемуся, если дан правильный ответ на 1 вопрос из 2;

0 баллов по шкале БРС выставляется обучающемуся, если дан правильный ответы на 0 вопросов из 2.

1.3 КОНТРОЛЬНЫЕ ВОПРОСЫ К ЛАБОРАТОРНЫМ РАБОТАМ

Контрольные вопросы для защиты лабораторной работы №1.

1. Какой состав и организационная структура системы обеспечения информационной безопасности?
2. В чем заключается стандарт ISO 17799?
3. Гарантии безопасности компьютерных систем в системе общих критериев.
4. Классификация защищенности компьютерной системы по требованиям безопасности информации в системе общих критериев.
5. Основные угрозы безопасности информации в компьютерных системах.
6. Государственная политика в области безопасности компьютерных систем.
7. Проектирование доступа к данным. Инфологические и даталогические модели.
8. Руководящий документ "Классификация автоматизированных систем."

Контрольные вопросы для защиты практической работы №2.

1. Система обнаружения компьютерных атак, дайте определение.
2. Виды программ технического обслуживания (стандартные программы).
3. Значение технического обслуживания.
4. Причины отказа в гарантийном обслуживании.
5. Программы технического обслуживания.
6. Разовые мероприятия.
7. Расширенные программы технического обслуживания.
8. Регламентные мероприятия.
9. Как обслуживаются высококритичные системы.

Контрольные вопросы для защиты практической работы №3.

1. Анализ схемы на наличие слабостей и поиск вариантов усиления с минимальным модифицированием.
2. Опишите сравнительный анализ основных методов защиты от копирования.
3. Опишите, как GFI LANguard защищает против червей.
4. Что является результатом анализа требований?
5. Охарактеризуйте защитные оболочки и перечень преград, применяемые в учебной компьютерной лаборатории.
6. Каким образом классифицируются каналы утечки информации?

7. Какие основные методы контроля доступа используются в известных вам информационных системах? В чем их достоинства и недостатки?

8. Что такое скрытые каналы утечки информации и как их обнаружить?

Контрольные вопросы для защиты практической работы №4.

1. Определение и классификация систем обнаружения вторжений.
2. Какие методы используются для обнаружения модифицированного кода?
3. Что в себя включает понятие защита программного обеспечения?
4. Сетевые системы обнаружения вторжений.
5. Узловые системы обнаружения вторжений
6. Сравнение систем обнаружения вторжений.
7. Назовите 4 типа установки я СОВ OSSEC.
8. Какие системы СОВ вы изучили?

Контрольные вопросы для защиты практической работы №5.

1. Как классифицируются системы обнаружения вторжений?
2. Какие задачи выполняют СОВ?
3. Что вы знаете об узловых СОВ?
4. Назовите основные требования СОВ.
5. Что вы знаете о сетевых СОВ?
6. Назовите функции СОВ OSSEC.
7. Назовите отличия пассивных СОВ от активных СОВ.
8. Что включает архитектура системы обнаружения вторжений?

Критерии оценки:

3 балла (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

2 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

1 балл (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы,

но недостаточно четко дает определение основных 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 он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1. Какая система обеспечивает защиту от вредоносного кода во время загрузки файлов пользователями?

    1) idp
    2) av
    3) wcf
    4) ips

2. Какой механизм фильтрации интернет-трафика в межсетевых экранах netdefend помогает защитить пользователей от потенциально опасного контента веб-страниц – объектов activex, java-скриптов и т.п.?

    1) работа с активным содержимым
    2) статическая фильтрация
    3) динамическая фильтрация

3. Какой протокол в составе ipsec обеспечивает проверку целостности защищаемой части пакета, но при этом не гарантирует конфиденциальность?

    1) ah
    2) esp
    3) ike

4. Какие протоколы обмена позволят защититься от атаки «анализ сетевого трафика»?

    1) telnet
    2) ssl
    3) ssh
    4) tls
    5) ftp
    6) http

5. Для чего применяется экранирование помещений и дополнительное заземление объектов защиты?

    1) для увеличения уровня побочных электромагнитных излучений

2) для уменьшения уровня побочных электромагнитных излучений
3) для обеспечения бесперебойного питания объектов защиты
4) для исключения внедрения злоумышленников во внутренние сегменты сети

6. Какое требование к системе защиты информации предполагает организацию единого управления по обеспечению защиты информации?

1) адекватность
2) непрерывность
3) централизованность
4) универсальность

7. Какое требование к системе защиты информации предполагает то, что методы защиты должны обеспечивать возможность перекрытия канала утечки информации, независимо от его вида и места появления?

1) адекватность
2) непрерывность
3) централизованность
4) универсальность

8. Как называется логическая группа устройств, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам?

1) виртуальная частная сеть
2) виртуальная локальная сеть
3) защищенная магистральная сеть
4) виртуальная канальная сеть

9. Какое название получила технология, позволяющая обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети с применением средств криптографии?

1) виртуальная частная сеть
2) виртуальная локальная сеть
3) защищенная магистральная сеть
4) виртуальная канальная сеть

10. Назовите основную причину низкой надежности парольной защиты:

1) человеческий фактор

2) неразвитое программное обеспечение
3) большое количество "черных ходов" в программном обеспечении

11. Наиболее общий способ проникновения в систему:

1) слабые пароли
2) дефекты программирования
3) переполнение буфера

12. Какой из перечисленных паролей наиболее надежен?

1) директор
2) й2ц3у4к5
3) безопасность
4) ао4тг7й6

13. Наиболее надежный способ аутентификации:

1) парольная защита
2) смарт-карты
3) биометрические методы

14. Какие методы используют хакеры при проведении социального инжиниринга?

1) умение вести телефонную беседу
2) подбор паролей методом перебора
3) скрытое сканирование портов

15. Если логин сотрудника компании ivanovvv, то использование какого пароля не допустимо?

1) ivanovvv
2) й2ц3у4к5
3) безопасность
4) ао4тг7й6

16. Лучший способ борьбы с социальным инжинирингом:

1) обеспечение физической защиты и контроля доступа
2) информирование служащих
3) использование сертифицированного программного обеспечения

17. Получение несанкционированного доступа к информации или к системе без применения технических средств называется:

1) социальный инжиниринг
2) скрытое сканирование
3) получение информации из открытых источников

18. Какие методы используют хакеры при проведении социального инжиниринга?

1) умение вести телефонную беседу
2) использование источников открытой информации
3) открытый грабеж
4) подбор паролей методом перебора
5) скрытое сканирование портов

19. Какую из возможных угроз для безопасности системы труднее всего обнаружить?

1) слабые пароли
2) ошибки конфигурации
3) переполнение буфера

20. Переполнение буфера опасно тем, что:

1) позволяет хакерам выполнить практически любую команду в системе, являющейся целью атаки
2) его не возможно обнаружить в результате исследования исходного кода программы
3) ограничивает доступ к удаленной системе

21. Какие из этих описаний характеризует централизованные dos-атаки?

1) это злонамеренные действия, выполняемые для запрещения легальному пользователю доступа к системе, сети, приложению или информации
2) для осуществления атаки система-отправитель посылает огромное количество tcp syn-пакетов (пакетов с синхронизирующими символами) к системе-получателю, игнорируя ack-пакеты, добиваясь переполнения буфера очереди соединений
3) в осуществлении атаки участвует большое количество систем, которыми управляет одна главная система и один хакер. Выход системы из строя достигается путем огромного объема передаваемых данных

22.Какие из этих описаний характеризует распределенные dos-атаки?

1) это злонамеренные действия, выполняемые для запрещения легальному пользователю доступа к системе, сети, приложению или информации
2) для осуществления атаки система-отправитель посылает огромное количество tcp syn-пакетов (пакетов с синхронизирующими символами) к системе-получателю, игнорируя ack-пакеты, добиваясь переполнения буфера очереди соединений
3) в осуществлении атаки участвует большое количество систем, которыми управляет одна главная система и один хакер. Выход системы из строя достигается путем огромного объема передаваемых данных

23.Выберите верное утверждение:

1) прослушивание (снифинг) работают только в сетях с разделяемой пропускной способностью с сетевыми концентраторами – хабами; использование коммутаторов обеспечивает достаточно надежную защиту от прослушивания
2) прослушивание (снифинг) хорошо работают в сетях с разделяемой пропускной способностью с сетевыми концентраторами – хабами; использование коммутаторов снижает эффективность снифинга
3) прослушивание (снифинг) работают только в сетях с коммутируемой средой, использующей коммутаторы; использование концентраторов исключает возможность снифинга

24.Для прослушивания трафика в коммутируемой среде хакер должен:

1) "убедить" коммутатор в том, что трафик, представляющий интерес, должен быть направлен к сниферу
2) заставить коммутатор отправлять весь трафик ко всем портам
3) организовать на коммутатор dos-атаку

25.Хакеры используют для перенаправления трафика:

1) arp-спуфинг
2) дублирование mac-адресов
3) имитация доменного имени
4) подмену ip-адреса

26. Для выполнения каких атак хакер должен установить приложения на локальном компьютере?

    1) arp-спуфинг
    2) mac-флудинг
    3) подмена ip-адреса

27. Какие из перечисленных служб наиболее уязвимы для атаки с изменением ip-адреса?

    1) веб-службы
    2) электронная почта
    3) rlogin
    4) rsh

28. Хакеры используют для перенаправления трафика:

    1) arp-спуфинг
    2) дублирование mac-адресов
    3) подмену ip-адреса

29. Какой тип атаки был использован кевином митником для проникновения в центр суперкомпьютеров в сан-диего?

    1) имитация ip-адреса
    2) перенаправление трафика
    3) переполнение буфера

30. Какие типы программ относятся к вредоносным?

    1) вирусы
    2) троянские кони
    3) черви
    4) системные службы
    5) операционные системы

31. Троянский конь – это:

    1) программный код, внедряющийся в исполняемый код других программ и активизирующийся при их запуске
    2) законченная и независимая программа, которая разработана для выполнения вредоносных действий под видом полезной и интересной программы:

3) это самораспространяющаяся и самовоспроизводящаяся программа, которая «переползает» от системы к системе без всякой помощи со стороны жертвы

32.Компьютерный червь – это:

1) программный код, внедряющийся в исполняемый код других программ и активизирующийся при их запуске
2) законченная и независимая программа, которая разработана для выполнения вредоносных действий под видом полезной и интересной программы:
3) это самораспространяющаяся и самовоспроизводящаяся программа, которая «переползает» от системы к системе без всякой помощи со стороны жертвы

33. Какая часть предварительного исследования является наиболее опасной для хакера при подготовке направленной атаки?

1) развернутая отправка пинг-пакетов
2) скрытое сканирование портов
3) сканирование уязвимых мест

34.Примером компьютерного вируса является:

1) michelangelo
2) макровирус мелисса
3) iloveyou
4) slapper

35.Примером "троянского коня" является:

1) michelangelo
2) макровирус мелисса
3) iloveyou
4) slapper

36.Примером компьютерного червя является:

1) michelangelo
2) макровирус мелисса
3) iloveyou
4) slapper

37.Как называется канал типа «точка-точка» в vpn-соединении?

1) шлюз
2) транк
3) туннель
4) мост

38. Для какой цели применяются виртуальные частные сети?

1) для снижения нагрузки на сеть
2) для обеспечения информационной безопасности
3) для обеспечения отказоустойчивости
4) для уменьшения количества передаваемого служебного трафика

39. На каком уровне модели osi создают туннели протоколы l2tp и pptp?

1) канальный
2) транспортный
3) сетевой
4) прикладной

40. На каком уровне модели osi создается управляющее vpn-туннелем соединение при работе с протоколом pptp?

1) канальный
2) транспортный
3) сетевой
4) прикладной

41. Как называется протокол инкапсуляции сетевых пакетов, обеспечивающий туннелирование трафика через сети без шифрования?

1) pptp
2) gre
3) l2tp
4) ipsec

42. Какой протокол следует применить для туннелирования ipv6-трафика через сеть ipv4 без шифрования?

1) pptp
2) gre
3) l2tp
4) ipsec

43. Какое основное отличие протокола l2tp перед pptp?

1) не шифрует информационные данные
2) позволяет создавать vpn-соединения
3) позволяет создавать туннель не только в сетях ip, но и в сетях atm, x.25 и frame relay
4) позволяет шифровать информационный пакет полностью

44. Необходимо построить vpn-канал через открытую ip-сеть к netbeui-сети. Какие протоколы можно использовать?

1) pptp
2) l2tp
3) ipsec

45. Какой заголовок добавляется к пакету при передаче по туннелю l2tp после udp-заголовка?

1) l2tp
2) ppp
3) ip
4) pptp

46. Компьютер-получатель получил данные по туннелю l2tp. Какой заголовок он обрабатывает вначале?

1) l2tp
2) ppp
3) ip
4) pptp

47. Какие данные в составе кадра l2tp использует компьютер-получатель для идентификации туннеля?

1) l2tp-заголовок
2) ppp-заголовок
3) ip-заголовок
4) pptp-заголовок

48. Выберите верное утверждение в отношении vlan.

1) передача кадров между разными vlan осуществляется на основе mac-адреса
2) передача кадров между разными vlan невозможна
3) передача кадров между разными vlan возможна только на основании индивидуального mac-адреса

4) передача кадров между разными vlan на основании mac-адреса невозможна

49. Как называется стандарт для виртуальных локальных сетей?

1) ieee 802.11
2) ieee 802.11i
3) ieee 802.1q
4) 802.1ad

50. Как называется стандарт, который позволяет пробрасывать vlan внутри другого vlan’а?

1) ieee 802.11
2) ieee 802.11i
3) ieee 802.1q
4) 802.1ad

51. Выберите верные утверждения в отношении vlan и netdefendos.

1) vlan id может назначаться только одному порту
2) vlan id может назначаться разным портам
3) если на одном коммутаторе разным портам присвоены разные значения vlan id, трафик подключенных vlan не будет изолирован
4) если на одном коммутаторе разным портам присвоены разные значения vlan id, трафик подключенных vlan будет изолирован

52. Какое название получила технология, позволяющая обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети с применением средств криптографии?

1) виртуальная частная сеть
2) виртуальная локальная сеть
3) защищенная магистральная сеть
4) виртуальная канальная сеть

53. Как называется канал типа «точка-точка» в vpn-соединении?

1) шлюз
2) транк
3) туннель
4) мост

54. Для какой цели применяются виртуальные частные сети?

1) для снижения нагрузки на сеть
2) для обеспечения информационной безопасности
3) для обеспечения отказоустойчивости
4) для уменьшения количества передаваемого служебного трафика

55. На каком уровне модели osi создают туннели протоколы l2tp и pptp?

1) канальный
2) транспортный
3) сетевой
4) прикладной

56. На каком уровне модели osi создается управляющее vpn-туннелем соединение при работе с протоколом pptp?

1) канальный
2) транспортный
3) сетевой
4) прикладной

57. Как называется протокол инкапсуляции сетевых пакетов, обеспечивающий туннелирование трафика через сети без шифрования?

1) pptp
2) gre
3) l2tp
4) ipsec

58. Какой протокол следует применить для туннелирования ipv6-трафика через сеть ipv4 без шифрования?

1) pptp
2) gre
3) l2tp
4) ipsec

59. Какое основное отличие протокола l2tp перед pptp?

1) не шифрует информационные данные
2) позволяет создавать vpn-соединения
3) позволяет создавать туннель не только в сетях ip, но и в сетях atm, x.25 и frame relay
4) позволяет шифровать информационный пакет полностью

60. Необходимо построить vpn-канал через открытую ip-сеть к netbeui-сети. Какие протоколы можно использовать?

    1) pptp
    2) l2tp
    3) ipsec

61. Какой заголовок добавляется к пакету при передаче по туннелю l2tp после udp-заголовка?

    1) l2tp
    2) ppp
    3) ip
    4) pptp

62. Компьютер-получатель получил данные по туннелю l2tp. Какой заголовок он обрабатывает вначале?

    1) l2tp
    2) ppp
    3) ip
    4) pptp

63. Какие данные в составе кадра l2tp использует компьютер-получатель для идентификации туннеля?

    1) l2tp-заголовок
    2) ppp-заголовок
    3) ip-заголовок
    4) pptp-заголовок

64. Какой протокол в составе ipsec обеспечивает проверку целостности защищаемой части пакета, но при этом не гарантирует конфиденциальность?

    1) ah
    2) esp
    3) ike

65. Какой протокол в составе ipsec обеспечивает конфиденциальность и целостность передаваемых данных?

    1) ah
    2) esp
    3) ike

66. Какой протокол обеспечивает средства аутентификации между двумя конечными точками vpn?

    1) ah
    2) esp
    3) ike

67. В чем отличие транспортного режима работы протоколов ah и esp от режима туннелирования?

    1) в транспортном режиме шифруется поле данных, содержащее протоколы tcp/udp, в туннельном –весь ip-пакет
    2) в транспортном режиме шифруются только данные прикладного уровня, а туннельном –весь ip-пакет
    3) в транспортном режиме шифруется весь ip-пакет, в туннельном – поле данных, содержащее протоколы tcp/udp
    4) в транспортном режиме работает ah, в туннельном – esp.

68. Какой режим работы протоколов ah и esp используется при организации безопасной передачи данных через интернет между шлюзами для объединения разных частей виртуальной частной сети?

    1) транспортный
    2) туннельный

69. В каком режиме работы протоколов ah и esp шифруется весь пакет, в том числе заголовок сетевого уровня?

    1) транспортный
    2) туннельный

70. Что такое icv?

    1) идентификатор протокола
    2) контрольная сумма
    3) идентификатор виртуальной частной сети
    4) время жизни

71. Для чего используется контрольная сумма пакета?

    1) для сжатия пакета
    2) для маршрутизации пакета
    3) для начала процесса расшифровки
    4) для аутентификации

72. Для чего используется вектор инициализации?

1) для сжатия пакета
2) для маршрутизации пакета
3) для начала процесса расшифровки
4) для аутентификации

73. В каком режиме установки vpn-соединения есть возможность согласования всех параметров конфигурации устройств отправителя и получателя?

1) main mode
2) aggressive mode

74. Выберите верные утверждения в отношении phase one и phase two.

1) phase two lifetime короче, чем phase one
2) phase one lifetime короче, чем phase two
3) для обоих узлов необходимо задать одинаковые параметры phase two и phase one соответственно
4) у обоих узлов должно быть разное значение phase one

75. Что должно произойти при истечении времени, установленного в качестве ipsec Sa lifetime?

1) прекращение обмена по данному vpn-каналу
2) взаимная переидентификация участниками обмена
3) смена ключа шифрования
4) смена алгоритма шифрования

76. Для чего применяется параметр dpd expire time в межсетевых экранах d-link?

1) для того чтобы задать время, по истечении которого происходит взаимная переидентификация узлов в vpn-туннеле
2) для того чтобы исключить существование vpn «туннелей-призраков»
3) для того чтобы задать время, по истечении которого меняется ключ шифрования vpn-туннеля
4) для того чтобы задать время, по истечении которого меняется алгоритм шифрования vpn-туннеля

77. Для чего был создан протокол nat traversal?

1) для того чтобы согласовывать алгоритм шифрования в vpn-туннеле
2) для того чтобы nat-шлюзы могли обрабатывать ipsec-трафик
3) для выработки ключа шифрования в vpn-туннеле
4) для возможности добавления esp-заголовка в состав передаваемого пакета данных

78. Какой дополнительный заголовок добавляет протокол nat traversal к пакетам ipsec?

1) tcp
2) udp
3) ppp
4) esp

79. Для чего центр сертификации ca подписывает сертификаты открытых ключей?

1) чтобы контролировать их целостность
2) чтобы обеспечить конфиденциальность
3) чтобы инкапсулировать их в протоколы канального уровня
4) чтобы подтвердить их подлинность

80. Для чего сертификат центра сертификации ca добавляется в поле root certificates в межсетевых экранах d-link?

1) чтобы межсетевой экран подписывал клиентские сертификаты сертификатом ca
2) чтобы межсетевой экран не пропускал данные от клиентов, сертификаты которых подписаны данным ca
3) чтобы межсетевой экран знал, каким сертификатам он может доверять
4) чтобы создавать самоподписанные сертификаты

81. Как называется логическая группа устройств, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам?

1) виртуальная частная сеть
2) виртуальная локальная сеть
3) защищенная магистральная сеть
4) виртуальная канальная сеть

82. Выберите верное утверждение в отношении vlan.

1) трафик устройств, находящихся в разных vlan’ах, полностью изолирован от других узлов сети на канальном уровне, только если они подключены к разным коммутаторам
2) трафик устройств, находящихся в разных vlan’ах, полностью изолирован от других узлов сети на канальном уровне, даже если они подключены к одному коммутатору
3) трафик устройств, находящихся в разных vlan’ах, полностью изолирован от других узлов сети на канальном уровне, только если они подключены в разным маршрутизаторам
4) трафик устройств, находящихся в разных vlan’ах, не изолирован от других устройств сети

83. Какой дополнительный параметр при настройке vpn в межсетевых экранах необходимо использовать для дополнительного шифрования при обмене ключами во второй фазе?

1) nat traversal
2) режим ike
3) группа ключей dh ike
4) совершенная прямая секретность (pfs)

84. Какой протокол в составе ipsec обеспечивает проверку целостности защищаемой части пакета, но при этом не гарантирует конфиденциальность?

1) ah
2) esp
3) ike

85. Какой протокол в составе ipsec обеспечивает конфиденциальность и целостность передаваемых данных?
1) ah
2) esp
3) ike

86. Какой протокол обеспечивает средства аутентификации между двумя конечными точками vpn?
1) ah
2) esp
3) ike

87. В чем отличие транспортного режима работы протоколов ah и esp от режима туннелирования?

1) в транспортном режиме шифруется поле данных, содержащее протоколы tcp/udp, в туннельном –весь ip-пакет
2) в транспортном режиме шифруются только данные прикладного уровня, а туннельном –весь ip-пакет
3) в транспортном режиме шифруется весь ip-пакет, в туннельном – поле данных, содержащее протоколы tcp/udp
4) в транспортном режиме работает ah, в туннельном – esp.

88. Какой режим работы протоколов ah и esp используется при организации безопасной передачи данных через интернет между шлюзами для объединения разных частей виртуальной частной сети?

1) транспортный
2) туннельный

89. В каком режиме работы протоколов ah и esp шифруется весь пакет, в том числе заголовок сетевого уровня?

1) транспортный
2) туннельный

90. Что такое icv?

1) идентификатор протокола
2) контрольная сумма
3) идентификатор виртуальной частной сети
4) время жизни

91. Для чего используется контрольная сумма пакета?

1) для сжатия пакета
2) для маршрутизации пакета
3) для начала процесса расшифровки
4) для аутентификации

92. Для чего используется вектор инициализации?

1) для сжатия пакета
2) для маршрутизации пакета
3) для начала процесса расшифровки
4) для аутентификации

93. В каком режиме установки vpn-соединения есть возможность согласования всех параметров конфигурации устройств отправителя и получателя?

1) main mode
2) aggressive mode

94. Выберите верные утверждения в отношении phase one и phase two.

1) phase two lifetime короче, чем phase one
2) phase one lifetime короче, чем phase two
3) для обоих узлов необходимо задать одинаковые параметры phase two и phase one соответственно
4) у обоих узлов должно быть разное значение phase one

95. Что должно произойти при истечении времени, установленного в качестве ipsec
Sa lifetime?

1) прекращение обмена по данному vpn-каналу
2) взаимная переидентификация участниками обмена
3) смена ключа шифрования
4) смена алгоритма шифрования

96. Для чего применяется параметр dpd expire time в межсетевых экранах d-link?

1) Для того чтобы задать время, по истечении которого происходит взаимная переидентификация узлов в vpn-туннеле
2) Для того чтобы исключить существование vpn «туннелей-призраков»
3) Для того чтобы задать время, по истечении которого меняется ключ шифрования vpn-туннеля
4) Для того чтобы задать время, по истечении которого меняется алгоритм шифрования vpn-туннеля

97. Для чего был создан протокол nat traversal?

1) Для того чтобы согласовывать алгоритм шифрования в vpn-туннеле
2) Для того чтобы nat-шлюзы могли обрабатывать ipsec-трафик
3) Для выработки ключа шифрования в vpn-туннеле
4) Для возможности добавления esp-заголовка в состав передаваемого пакета данных

98. Какой дополнительный заголовок добавляет протокол nat traversal к пакетам ipsec?

1) tcp
2) udp
3) ppp
4) esp

99. Для чего центр сертификации CA подписывает сертификаты открытых ключей?

1) Чтобы контролировать их целостность.
2) Чтобы обеспечить конфиденциальность.
3) Чтобы инкапсулировать их в протоколы канального уровня.
4) Чтобы подтвердить их подлинность.

100. Основными источниками угроз информационной безопасности являются все указанное в списке:

1) Хищение жестких дисков, подключение к сети, инсайдерство.
2) Перехват данных, хищение данных, изменение архитектуры системы.
3) Хищение данных, подкуп системных администраторов, нарушение регламента работы.

Задания в открытой форме

1) … - характеристика средств системы, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню и глубине в зависимости от класса защищенности

2) … - это активный компонент защиты, включающий в себя анализ возможных угроз и рисков, выбор мер противодействия и методологию их применения.

3) Под термином … понимается системный процесс получения и оценки объективных данных о текущем состоянии обеспечения безопасности информации.

4) … — анализ реализованных мер защиты информации, который позволит определить степень соответствия требованиям основных нормативно-правовых актов, а также оценить реальный уровень защищенности организации от возможных угроз.

5) … критерии предъявляются к возможностям мер и средств защиты информации, определяющим желательный режим работы ИС. Включают в себя требования: организационные, эксплуатационные и к безопасности ИТ.

6) … критерии предъявляются к действиям разработчика системы, документам для оценивания и работе самой организации. Включают требования доверия к мерам к СЗИ в информационных системах, а также к их разработке и эксплуатации.

7) … — положения политик безопасности, затрагивающих ОО и учитывающих его особенности;

8) … — меры физической защиты, персонал и его специфика;

9) … — назначение ОО, предполагаемые области его применения.

10) … — типовой набор требований для некоторой категории ОО.

11) … — документ, содержащий требования безопасности для конкретной разработки, выполнение которых обеспечивает достижение поставленных целей безопасности.

12) … – любой контейнер, предназначенный для хранения информации, подверженный угрозам информационной безопасности (сервер, рабочая станция, переносной компьютер).

13) … – действие, которое потенциально может привести к нарушению безопасности

14) … – это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы.

15) …– ущерб, который понесет компания от потери ресурса

16) … – степень влияния реализации угрозы на ресурс, т.е. как сильно реализация угрозы повлияет на работу ресурса.

17) В концепции обеспечения информационной безопасности предприятия определяются…

18) Формирование защиты в ИС основывается на …

19) Тестирование по методу «…» предполагает отсутствие у тестирующей стороны каких-либо специальных знаний о конфигурации и внутренней структуре объекта испытаний.

20) Метод «…» предполагает составление программы тестирования на основании знаний о структуре и конфигурации объекта испытаний.

21) … — процесс, включающий анализ конфигураций объекта оценки и риск-ориентированную симуляцию действий злоумышленника.

Задание на установление правильной последовательности

1. Расположите этапы построения экспертной системы в правильной последовательности:
   1) Формализация,
   2) Выполнение,
   3) Тестирование
   4) Опытная экспертиза
   5) Идентификация,
   6) Концептуализация,

2. Установите этапы аудита безопасности:
   1) Инициирование процедуры аудита;
   2) Сбор информации аудита;
   3) Анализ данных аудита;
   4) Выработку рекомендаций;
   5) подготовку аудиторского отчета.

3. Установите этапы СЗИ:
   1) Требования и критерии систем защиты информации.
   2) Внедрение СЗИ.
   3) Аттестация СЗИ.
   4) Разработка СЗИ.

4. Установите этапы анализа защищенности:
   1) Анализ полученных данных и уязвимостей.
   2) Выработка рекомендаций.
   3) Подготовка отчетных документов.
   4) Инициирование и планирование Определение области и границ аудита.
   5) Обследование, документирование и сбор информации.

5. Установите этапы внедрения межсетевого экрана:
    1) Планирование
    2) Тестирование
    3) Развертывание
    4) Управление
    5) Конфигурирование

6. Установите этапы развития информационных технологий:
    1) «электрическая» технология.
    2) «электронная» технология.
    3) «компьютерная» технология.
    4) «ручная» технология.
    5) «механическая» технология.

7. Расположите этапы развития информационных технологий в соответствии с проблемами, стоящими на пути информатизации общества.
    1) Максимальное удовлетворение потребностей пользователя и создание соответствующего интерфейса работы в компьютерной среде.
    2) Обработка больших объемов данных в условиях ограниченных возможностей аппаратных средств.
    3) Отставание программного обеспечения от уровня развития аппаратных средств.
    4) Выработка соглашений и установление стандартов, протоколов для компьютерной связи; организация доступа к стратегической информации; организация защиты и безопасности информации.

8. Процесс разработки в среде ООП включает в себя следующие этапы:
    1) Сопровождение
    2) Модификация
    3) Программирование
    4) Анализ
    5) Проектирование

9. 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.

10. Выберите правильную последовательность этапов защиты информации, информационных технологий и автоматизированных систем от атак:

1) Анализ рисков для активов организации, включающий в себя выявление ценных активов и оценку возможных последствий реализации атак с использованием скрытых каналов
2) Реализация защитных мер по противодействию скрытых каналов
3) Организация контроля за противодействием скрытых каналов.
4) Выявление скрытых каналов и оценка их опасности для активов организации

11. Выберите правильную последовательность этапов жизненного цикла информационного сервиса:
    1) Сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию.
    2) На данном этапе выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение.
    3) На данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно закупка.
    4) На данном этапе сервис не только работает и администрируется, но и подвергается модификациям.

12. Установите этапы существования оборудования ИБ:
    1) Установка.
    2) Эксплуатация.
    3) Выведение из эксплуатации.
    4) Инициация.
    5) Закупка.

13. 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.

14. 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;
5) Выберите правильную последовательность этапов работы по обеспечению режима ИБ:

15. Установите последовательность этапов работы по обеспечению информационной безопасности:
    1) Определение требований к системе защиты информации;
    2) Выбор контрмер, обеспечивающих режим иб, и средств защиты;
    3) Разработка, внедрение и организация использования выбранных мер, способов и средств защиты;
    4) Осуществление текущего контроля целостности информационных ресурсов и средств защиты и плановый аудит системы управления информационной безопасностью.

16. Выберите правильную последовательность этапов процесса управления рисками:
    1) Идентификация активов и ценности ресурсов, нуждающихся в защите;
    2) Анализ угроз и их последствий, определение слабостей в защите;
    3) Классификация рисков, выбор методологии оценки рисков и проведение оценки;
    4) Выбор, реализация и проверка защитных мер;
    5) Оценка остаточного риска;
    6) Выбор анализируемых объектов и степени детальности их рассмотрения;

17. Выберите правильную последовательность этапов обеспечения информационной:
    1) Оценка стоимости;
    2) Реализация политики;
    3) Квалифицированная подготовка специалистов;
    4) Аудит;
    5) Разработка политики безопасности;

18. Выберите последовательность уровней безопасности информации:
    1) Административный уровень
    2) Процедурный уровень
    3) Программно-технический уровень
    4) Законодательный уровень

19. Выберите правильную последовательность этапов оценки угроз безопасности информации:

1) Определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;
2) Инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;
3) Определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;
4) Оценка способов реализации (возникновения) угроз безопасности информации;
5) Оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;
6) Оценка сценариев реализации угроз безопасности информации в системах и сетях.

20. Выберите правильную последовательность этапов построения политики безопасности:
    1) Выбор и установка средств защиты;
    2) Организация обслуживания по вопросам информационной безопасности;
    3) Создание системы периодического контроля информационной безопасности
    4) Обследование информационной системы на предмет установления организационной и информационной структуры и угроз безопасности информации;
    5) Подготовка персонала работе со средствами защиты;

Задание на установление соответствия

1. Установить соответствие основных видов систем обнаружения вторжений:

1) Сетевые (NIDS)	a) Для проверки специализированных прикладных протоколов.
2) Основанные на прикладных протоколах СОВ (APIDS)	b) Анализируют журналы приложений, состояние хостов, системные вызовы.
3) Узловые или Host-Based (HIDS)	c) Для проверки сетевого трафика с коммутатора.

2. Установить соответствие:

1) Планирование	a) Отладка программы в соответствии с индивидуальными запросами конкретного предприятия базируется на контроле конфиденциальных сведений в соответствии с признаками особенной документации, принятой в компании
2) Реализация	b) Заключается в точном определении программы защиты данных. Ответ на простой, казалось бы, вопрос: «Что будем защищать?»
3) Корректировка	c) Проанализировав информацию, собранную на этапе тестовой эксплуатации DLP-решения, приступают к перенастройке ресурса.

3. Установить соответствие методов предотвращения утечки информации:

1) Dlp-система (data leak prevention)	a) Отслеживает пересылку и распечатку файлов, внезапные всплески интернет-общения, посещение нехарактерных для работы сайтов и т. Д.
2) Тренинг	b) Сотрудники имеют полный доступ к информации на компьютерах работников, а в случае разглашения коммерческой тайны будут требовать возмещения убытков. Эти меры являются мощным сдерживающим психологическим фактором.
3) Трудовой договор.	c) Сотрудникам рассылают письма с вирусами, просят по телефону выдать конфиденциальные сведения и т. П. В результате теста выясняется, как персонал реагирует на такие действия, и разрабатываются меры защиты.

4. Установить соответствие видов угроз:

1) Аппаратная	a) Когда возможен несанкционированный доступ к

	данным и их потеря.
2) Вероятность утечки	b) Когда существует вероятность нарушения работоспособности оборудования.
3) Нестабильность ПО	c) Когда есть вероятность некорректной работы программного обеспечения.

5. Установить соответствие:

1) Угроза целостности	a) Это вероятный ущерб, который зависит от защищенности системы.
2) Угроза доступности	b) Это стоимость потерь, которые понесет компания в случае реализации угрозы конфиденциальности, целостности или доступности по каждому виду ценной информации.
3) Ущерб	c) Это угроза нарушения работоспособности системы при доступе к информации.
4) Риск	d) Это угроза изменения информации.

6. Установить соответствие:

4) Системность целевая	a) Подразумевает единство организации всех работ по защите информации и их управления.
5) Системность пространственная	b) Защищенность информации рассматривается как составная часть общего понятия качества информации.
6) Системность временная	c) Защищенность основанная на принципе непрерывности функционирования системы защиты
7) Системность организационная	d) Защищенность рассматривается как увязка вопросов защиты информации

7. Установить соответствие:

1) Основные	a) Мероприятия по обеспечению

организационные и организационно-технические мероприятия по созданию и поддержанию функционирования системы защиты включают:	достаточного уровня физической защиты всех компонентов АСОД (противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности средств вычислительной техники, носителей информации и т.п.).
2) Разовые мероприятия включают:	b) Распределение реквизитов разграничения доступа (пароли, ключи шифрования и т.д.).
3) Периодически проводимые мероприятия включают:	c) Общесистемные мероприятия по созданию научно-технических и методологических основ защиты АСОД.
4) Постоянно проводимые мероприятия включают:	d) Мероприятия проводимые и повторяемые только при полном пересмотре принятых решений.

8. Установить соответствие технических каналов утечки информации:

1) Прямой акустический (окна, двери, щели, проемы)	a) Электронные спетоскопы, установленные в смежном помещении
2) Акусто-вибрационный (через ограждающие кострукции)	b) Направленные микрофоны, установленные за границей КЗ
3) Акусто-электрический (через соединительные линии ВТСС)	c) Специальные низкочастотные усилители, подсоединенные к соединительным линиям ВТСС, обладающие «микрофонным» эффектом
4) Акусто-электромагнитный (параметрический)	d) Защищенность рассматривается как увязка вопросов защиты информации

9. Установить соответствие технических каналов утечки информации:

1) Прямой акустический (окна, двери, щели, проемы)	a) Электронные устройства перехвата речевой информации с датчиками контактного типа, установленными на инженерно-технических коммуникациях
2) Акусто-вибрационный (через ограждающие кострукции)	b) Специализированные высокочувствительные микрофоны, установленные в воздуховодах или смежных помещениях
3) Акусто-электрический (через соединительные линии ВТСС)	c) Аппаратура высокочастотного облучения, установленная за пределами КЗ
4) Акусто-электромагнитный (параметрический)	d) Аппаратура «высокочастотного навязывания», подключенная к соединительным линиям ВТСС

10. Установить соответствие технических каналов утечки информации:

1) Прямой акустический (окна, двери, щели, проемы)	a) Электронные устройства перехвата речевой информации с датчиками микрофонного типа при условии неконтролируемого доступа к ним посторонних лиц
2) Акусто-оптический (через оконные стекла)	b) Лазерные акустические локационные системы, находящиеся за пределами КЗ
3) Акусто-электрический (через соединительные линии ВТСС)	c) Специальные низкочастотные усилители, подсоединенные к соединительным линиям ВТСС, обладающие «микрофонным» эффектом
4) Акусто-электромагнитный (параметрический)	d) Прослушивание разговоров, ведущихся в помещении без применения технических средств посторонними лицами

11. Установить соответствие нарушителей по уровням знания АСОД:

1) 1 уровень	a) Обладает высоким уровнем знаний и опытом работы с техническими средствами системы и ее обслуживания.

2) 2 уровень	b) Знает функциональные особенности АСОД, основные закономерности формирования в нестандартных массивах данных и потоков запросов к ним. Умеет пользоваться штатными средствами.
3) 3 уровень	4) Знает структуру, функции и механизмы действия средств защиты, их слабые и сильные стороны.
5) 4 уровень	6) Обладает уровнем знаний в области программирования и вычислительных технологий, проектирования и эксплуатации АСОД.

12. Установить соответствие нарушителей по уровням возможностей (используемым методам и вопросам):

1) 1 уровень	a) Применяющие пассивные средства (технические средства перехвата без модификации компонентов системы).
2) 2 уровень	b) Применяющие только агентурные методы получения сведений
3) 3 уровень	c) Использующие только штатные средства и недостатки системы защиты, их сильные и слабые стороны.
4) 4 уровень	d) Применяющие методы и действия активного воздействия (модификация и подключение дополнительных технических устройств).

13. Установить соответствие оценки рисков в зависимости от факторов:

1) Высокий риск	a) Предполагается, что без снижения таких рисков обращение к информационной системе предприятия может оказать отрицательное влияние на бизнес;
2) Существенный риск	b) Здесь требуется эффективная стратегия управления рисками, которая позволит уменьшить или полностью исключить отрицательные последствия нападения;
3) Умеренный риск	c) Усилия по управлению рисками в данном случае не будут играть важной

	роли.
4) Незначительный риск	d) В отношении рисков, попавших в эту область, достаточно применить основные процедуры управления рисками;

14. Установить соответствие:

1) Правовая защита	a) Это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, которая исключает или ослабляет нанесение каких-либо убытков предприятию;
2) Организационная защита	b) Это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, которые обеспечивают защиту информации на правовой основе;
3) Инженерно-техническая защита	c) Это использование разнообразных технических средств, которые препятствуют нанесению убытков предприятию.

15. Установить соответствие:

1) OLE-automation или просто Automation	a) Технология, организующая доступ к данным разных компьютеров с учетом балансировки нагрузки сети.
2) ActiveX	b) Технология, обеспечивающая безопасность и стабильную работу распределенных приложений при больших объемах передаваемых данных.
3) MIDAS	c) Технология предназначена для создания программного обеспечения как сосредоточенного на одном компьютере, так и распределенного в сети.
4) MTS (Microsoft Transaction Server)	d) Технология создания программируемых приложений, обеспечивающая программируемый доступ к внутренним службам этих приложений

16. Установить соответствие средств информационной защиты:

1) SIEM-системы	a) Виртуально-частная сеть определяет использование собственной частной сети внутри общедоступной. Поэтому ваше приложение, работающее по VPN, будет надежно защищено.
2) CloudAV	b) Они собирают информацию о возможных угрозах из различных источников: файервол, антивирус, межсетевой экран и др., потом проводят анализ и могут среагировать на вероятность возникновения потенциальной угрозы, предупредив о ней заранее.
3) Брандмаузер и фаервол	c) Это специальная система шифрования вашей информации. Шифровка происходит таким образом, что для того, чтобы расшифровать нужную информацию, необходимо обладать специальным шифром.
4) Криптографическое преобразование	d) Это специализированные средства, которые контролируют выход во всемирную паутину, при необходимости фильтруют или блокируют сетевой трафик.

17. Установить соответствие средств информационной защиты:

1) Программы-антивирусы	a) Это специальные технологии, которые предотвращают потерю конфиденциальной информации. Как правило, данная технология используется большими предприятиями, так как требует больших финансовых и трудоресурсных затрат.
2) VPN	b) Борются с самыми распространенными вирусами, также способны восстанавливать поврежденные файлы.

3) DLP-решения	c) Это облачные решения для обеспечения антивирусной защиты вашего ресурса.

18. Установить соответствие каналов утечки:

1) Несанкционированное копирование, уничтожение или подделка информации	a) Ошибки персонала и пользователей
2) Перебои электропитания	b) Из-за некорректной работы программ
3) Случайное уничтожение или изменение данных	c) Потери информации, связанная с несанкционированным доступом
4) Потеря или изменение данных при ошибках по	d) Сбои оборудования, при котором теряется информация

19. Установить соответствие:

1) Программно-аппаратные (технические) методы	a) Для обеспечения безопасности используются приемы «перестраховки», с помощью которых исключается возможность ошибочного или несанкционированного проникновения в информационную систему
2) Физическая защита	b) Для осуществления информационной защиты используются специальные компьютерные технологии. С их помощью можно скрыть важные данные, не допустить утечки во время пересылки через интернет
3) Морально-этические методы	c) Профилактические действия, в основном, воспитательного характера
4) Технологические приемы	d) Мероприятия направлены на снижение риска потери данных и выявление лиц, пытающихся проникнуть на охраняемую территорию или в информационную систему

20. Установить соответствие степеней происхождения угрозы информационной безопасности:

1) Естественная	a) Данные угрозы, в свою очередь, делятся на 2 подкатегории: преднамеренная подкатегория — это действия хакеров, конкурентов, недобросовестных сотрудников и т. д., непреднамеренная — действия происходят из-за людей по их неосторожности.
2) Искусственная	b) Это те угрозы, которые не зависят от деятельности человека: землетрясения, ураганы, смерчи, дожди, молнии и т. д.
3) Внутренняя	c) Все угрозы, которые происходят вне системы.
4) Внешняя	d) Угроза исходит изнутри самой системы.

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. Для некоторой системы характерно наличие беспроводного канала связи (Wi-fi), соединяющей компьютеры, находящиеся в аттестованных помещениях. Распространение сети проходит через неаттестованное помещение. Предложите перечень мероприятий, направленных на сохранение класса защиты данной информационной системы.
2. Предложите перечень мероприятий, направленных на улучшение класса защиты информационной системы вашего университета.
3. Определите, чем опасно для организации наличие беспроводного канала связи, соединяющей компьютеры, находящиеся в неаттестованных помещениях.
4. Определите, чем опасно для организации наличие беспроводного канала связи, соединяющей компьютеры, находящиеся в аттестованных помещениях.
5. Зашифровать строку «Стремитесь не к успеху, а к ценностям, которые он дает», используя шифрование с помощью таблицы Виженера
6. Опишите модель поведения нарушителя для административного корпуса завода ООО «СтройМаш».
7. Зашифровать строку «Лучшая месть – огромный успех», используя шифр RSA
8. Зашифровать строку «Лучшая месть – огромный успех», используя шифр RSA
9. Зашифровать строку «Если нет ветра, беритесь за вёсла.», используя алгоритм шифрования Эль-Гамаля
10. Зашифровать строку «Я не провалил тест. Я просто нашел сто способов написать его неправильно.», используя алгоритм шифрования Деффи-Хеллмана
11. Включите шифрование твердотельного накопителя используя операционную систему Windows 10

12. Воспользовавшись операционной системой Linux произведите сканирование локальной сети на поиск подозрительных устройств
13. Зашифровать строку «Научитесь говорить “Я не знаю”, и это уже будет прогресс.», используя шифр RSA
14. Зашифровать строку «Жизнь - это то, что с тобой происходит, пока ты строишь планы.», используя шифрование с помощью таблицы Виженера
15. Зашифровать строку «Мы становимся тем, о чем мы думаем.», используя алгоритм шифрования Эль-Гамаля
16. Произведите установку антивирусного программного обеспечения на персональный компьютер
17. Зашифровать строку «Стоит только поверить, что вы можете – и вы уже на полпути к цели.», используя шифр RSA
18. Зашифровать строку «Я не провалил тест. Я просто нашел сто способов написать его неправильно.», используя алгоритм шифрования Деффи-Хеллмана
19. Не имея непосредственного доступа к персональному компьютеру, совершите удаленный запуск приложений на нём
20. Зашифровать строку «Неудача – это просто возможность начать снова, но уже более мудро.» используя шифрование с помощью таблицы Виженера

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.