Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Таныгин Максим Олегович
Должность: Заведующий кафедрой
Дата подписания: 10.11.2026 11:45:06
Уникальный программный ключ:
c581cd75563a552725439b81ebe71cb37bca10f0

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
_____ М.О. Таныгин
(подпись)
«30» 06 2026г.

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

Методы и средства защиты компьютерной информации
*(наименование дисциплины)*

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

Курск – 2026

## 1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

### *1.1 ВОПРОСЫ И ЗАДАНИЯ В ТЕСТОВОЙ ФОРМЕ*

*Раздел 1. Основные понятия и анализ угроз информационной безопасности*

Вопросы в закрытой форме.

1.1. Что понимается под угрозой информационной безопасности? Выберите один ответ:

а) Недостаток системы, позволяющий нарушить одно или несколько условий безопасности

б) Потенциальная возможность нарушения одного или нескольких условий безопасности информационной системы

в) Попытка реализации несанкционированного доступа к информации

г) Состояние защищённости информационной системы, при котором обеспечивается её нормальное функционирование

1.2. Какое свойство информации нарушается при несанкционированном изменении, искажении или уничтожении данных? Выберите один ответ:

а) Конфиденциальность

б) Доступность

в) Целостность

г) Достоверность

1.3. Какое из перечисленных воздействий на вычислительную сеть является примером пассивной угрозы? Выберите один ответ:

а) Изменение конфигурации сети

б) Нарушение работоспособности узла сети

в) Прослушивание канала связи в сети

г) Передача сообщений от имени другого объекта

1.4. Какие из перечисленных угроз относятся к угрозам нарушения доступности информации? Выберите несколько ответов:

а) Блокирование доступа пользователей к данным

б) Отказ в обслуживании (Denial of Service)

в) Несанкционированное копирование файлов

г) Выход узла сети из строя, в результате чего доступ к ресурсам становится невозможным

д) Прослушивание канала связи

е) Перехват информации без её модификации

ж) Ограничение доступа к информационному ресурсу

з) Несанкционированное изменение данных

Вопросы в открытой форме.

1.5. Заполните пропуск:

Попытка реализации угрозы называется _____, а тот, кто предпринимает такую попытку, – злоумышленником.

1.6. Заполните пропуск:

В соответствии с классификацией удалённых угроз по цели воздействия выделяют три основных класса угроз: нарушение конфиденциальности информации (класс 2.1), нарушение целостности информации (класс 2.2) и нарушение _____ информации (класс 2.3).

Вопросы на установление последовательности.

1.7. Установите правильную последовательность этапов, характеризующих жизненный цикл угрозы информационной безопасности (от появления возможности до её устранения):

а) Возникновение уязвимости в информационной системе

б) Появление возможности воспользоваться уязвимостью

в) Реализация угрозы (атака)

г) Ликвидация возможности использования уязвимости

1.8. Установите правильную последовательность действий при анализе угроз информационной безопасности (от первоначального этапа к заключительному):

а) Идентификация угроз

б) Определение перечня и характеристик актуальных угроз

в) Оценка уровня и вероятности возникновения угроз

г) Формирование требований по защите информации

Вопросы на установление соответствия.

1.9. Установите соответствие между типом угрозы и её определением.

| Тип угрозы | Определение |
|---|---|
| 1. Угроза конфиденциальности | а) Несанкционированное изменение, искажение или уничтожение информации |
| 2. Угроза целостности | б) Нарушение работоспособности объекта, доступ к которому должен быть обеспечен |
| 3. Угроза доступности | в) Нарушение свойства информации быть известной только определённым субъектам |
| | г) Угроза, связанная с несанкционированным копированием информации без её модификации |
| | д) Угроза, заключающаяся в отказе в обслуживании законных пользователей |

1.10. Установите соответствие между классификационным признаком угроз и его содержанием.

| Классификационный признак | Содержание |
|---|---|
| 1. По характеру воздействия | а) Наружные и внутренние |
| 2. По местонахождению источника | б) Пассивные и активные |
| 3. По нарушаемому свойству информации | в) Конфиденциальность, целостность, доступность |
| | г) Преднамеренные и непреднамеренные |

*Раздел 2. Проблемы информационной безопасности сетей*

Вопросы в закрытой форме.

2.1. Какой уровень модели OSI отвечает за маршрутизацию пакетов в сети? Выберите один ответ:

а) Физический

б) Канальный

в) Сетевой

г) Транспортный

2.2. Какой вид атаки заключается в перехвате и анализе сетевого трафика без его изменения? Выберите один ответ:

а) Спуфинг

б) Сниффинг

в) DoS-атака
г) Фишинг

2.3. Что такое фишинг? Выберите один ответ:
а) Атака на беспроводную сеть с целью подбора пароля
б) Вид мошенничества, целью которого является получение конфиденциальных данных пользователя путём поддельных сообщений
в) Нарушение доступности сервера путём перегрузки запросами
г) Перехват сессии между клиентом и сервером

2.4. Какие из перечисленных угроз характерны для беспроводных сетей? Выберите несколько ответов:
а) Несанкционированное подключение к точке доступа
б) Прослушивание трафика (сниффинг)
в) Атака типа "человек посередине"
г) Подмена MAC-адреса
д) Атака на WEP-шифрование
е) Отказ в обслуживании (DoS)
ж) Внедрение вредоносного кода через веб-страницы
з) Фишинг по электронной почте

Вопросы в открытой форме.
2.5. Заполните пропуск:
В модели OSI на уровне _____ происходит преобразование форматов данных (кодирование, сжатие, шифрование).

2.6. Ответьте на вопрос:
Сколько уровней содержит модель OSI? _____.

Вопросы на установление последовательности.
2.7. Установите правильную последовательность уровней модели OSI сверху вниз (от прикладного к физическому):
а) Прикладной
б) Представления
в) Сеансовый
г) Транспортный
д) Сетевой
е) Канальный
ж) Физический

2.8. Установите правильную последовательность этапов типичной сетевой атаки:
а) Разведка (сбор информации о цели)
б) Проникновение в систему
в) Получение привилегий (эскалация)
г) Внедрение вредоносного ПО
д) Установка бэкдора для сохранения доступа

Вопросы на установление соответствия.
2.9. Установите соответствие между уровнями модели OSI и их протоколами. В правом столбце есть лишние варианты.

| Уровень OSI | Протокол |
|---|---|
| 1. Сетевой уровень | а) IP |
| 2. Транспортный уровень | б) TCP |

| | |
|---|---|
| 3. Прикладной уровень | в) HTTP |
| | г) Ethernet |
| | д) FTP |

2.10. Установите соответствие между типом сетевой атаки и её описанием. В правом столбце есть лишние варианты.

| Тип атаки | Описание |
|---|---|
| 1. Сниффинг | а) Подмена сетевого адреса отправителя |
| 2. Спуфинг | б) Перехват и анализ трафика |
| 3. DoS-атака | в) Нарушение доступности ресурса путём перегрузки |
| | г) Внедрение вредоносного кода на сервер |
| | д) Перехват сессии |

*Раздел 3. Политика безопасности*

Вопросы в закрытой форме.

3.1. Что понимается под политикой безопасности организации? Выберите один ответ:

а) Набор правил, процедур и практик, регулирующих защиту информации

б) Только система парольной защиты

в) Комплекс криптографических средств

г) Совокупность технических средств фильтрации трафика

3.2. Какой уровень политики безопасности определяет стратегические цели и общие принципы защиты информации? Выберите один ответ:

а) Верхний уровень

б) Средний уровень

в) Нижний уровень

г) Операционный уровень

3.3. К какому компоненту архитектуры безопасности сети относится контроль доступа на основе ролей и учётных записей? Выберите один ответ:

а) Физическая безопасность

б) Логическая безопасность

в) Защита ресурсов

г) Аудит и оповещение

3.4. Какие из перечисленных политик относятся к специализированным политикам безопасности? Выберите несколько ответов:

а) Политика управления доступом

б) Политика использования интернета

в) Политика паролей

г) Политика защиты от вирусов

д) Политика резервного копирования

е) Политика конфиденциальности персональных данных

ж) Политика физической защиты

з) Политика реагирования на инциденты

Вопросы в открытой форме.

3.5. Заполните пропуск:

Процедуры безопасности описывают _____ действия, которые должны быть выполнены для реализации политики безопасности.

3.6. Ответьте на вопрос:

Сколько уровней политики безопасности обычно выделяют в организации? _____.

Вопросы на установление последовательности.

3.7. Установите правильную последовательность этапов разработки политики безопасности организации (от начального к заключительному):

а) Анализ рисков и оценка активов

б) Разработка проектов политик

в) Согласование и утверждение политик

г) Внедрение политик в практику

д) Контроль исполнения и актуализация

3.8. Установите правильную последовательность компонентов архитектуры безопасности сети в порядке их перечисления в стандартной модели (от физического к организационному):

а) Физическая безопасность

б) Логическая безопасность

в) Защита ресурсов

г) Определение административных полномочий

д) Аудит и оповещение

Вопросы на установление соответствия.

3.9. Установите соответствие между уровнем политики безопасности и его характеристикой.

| Уровень политики | Характеристика |
|---|---|
| 1. Верхний уровень | а) Определяет стратегические цели и общие принципы защиты |
| 2. Средний уровень | б) Разрабатывает тактические решения и стандарты |
| 3. Нижний уровень | в) Устанавливает конкретные правила и инструкции для операционной деятельности |
| | г) Описывает процедуры реагирования на инциденты |
| | д) Содержит шаблоны документов |

3.10. Установите соответствие между компонентом архитектуры безопасности сети и его описанием.

| Компонент | Описание |
|---|---|
| 1. Физическая безопасность | а) Обеспечение контроля доступа в помещения и защита оборудования от физических воздействий |
| 2. Логическая безопасность | б) Управление доступом к данным и системам на основе идентификации и аутентификации |
| 3. Защита ресурсов | в) Применение антивирусных средств, межсетевых экранов и систем обнаружения вторжений |
| 4. Аудит и оповещение | г) Регистрация событий безопасности и информирование администратора о нарушениях |
| | д) Определение прав и обязанностей персонала |
| | е) Планирование непрерывности бизнеса |

*Раздел 4. Криптографическая защита информации*

Вопросы в закрытой форме.

4.1. Как называется наука о методах обеспечения конфиденциальности и целостности информации с помощью математических преобразований? Выберите один

ответ:

а) Криптография
б) Криптоанализ
в) Стеганография
г) Кодирование

4.2. В каком типе криптосистем для шифрования и расшифрования используются разные, но математически связанные ключи? Выберите один ответ:

а) Симметричные криптосистемы
б) Асимметричные криптосистемы
в) Блочные шифры
г) Потоковые шифры

4.3. Какой из перечисленных алгоритмов является блочным симметричным шифром, принятым в качестве стандарта в США? Выберите один ответ:

а) RSA
б) AES
в) SHA-256
г) Эль-Гамаль

4.4. Какие из перечисленных алгоритмов относятся к симметричным криптосистемам? Выберите несколько ответов:

а) AES
б) DES
в) RSA
г) ГОСТ 28147-89
д) RC4
е) Эль-Гамаль
ж) SHA-256
з) MD5

Вопросы в открытой форме.

4.5. Заполните пропуск:

Электронная цифровая подпись предназначена для подтверждения подлинности и _____ электронного документа, а также для обеспечения неотказуемости от авторства.

4.6. Ответьте на вопрос:

Какой алгоритм хэширования имеет длину выхода 256 бит и входит в состав стандарта SHA-2? _____.

Вопросы на установление последовательности.

4.7. Установите правильную последовательность этапов шифрования сообщения в асимметричной системе RSA (от получения открытого ключа до отправки зашифрованного текста):

а) Получение открытого ключа отправителем
б) Шифрование сообщения открытым ключом получателя
в) Передача зашифрованного текста по каналу связи
г) Расшифрование получателем с использованием закрытого ключа

4.8. Установите правильную последовательность исторического развития шифров (от наиболее простых к современным):

а) Шифр простой замены

б) Шифр Виженера (полиалфавитный)
в) Блочные шифры (DES, AES)
г) Асимметричные криптосистемы (RSA)

Вопросы на установление соответствия.

4.9. Установите соответствие между криптографическим термином и его определением.

| Термин | Определение |
|---|---|
| 1. Шифрование | а) Преобразование открытого текста в зашифрованный вид с использованием ключа |
| 2. Расшифрование | б) Восстановление исходного текста из зашифрованного с использованием ключа |
| 3. Хэширование | в) Преобразование данных произвольной длины в строку фиксированной длины |
| 4. Электронная цифровая подпись | г) Цифровой аналог собственноручной подписи, обеспечивающий целостность и подлинность |
| | д) Способ скрытия факта передачи информации |

4.10. Установите соответствие между алгоритмом и его типом (симметричный, асимметричный, хэш-функция).

| Алгоритм | Тип |
|---|---|
| 1. AES | а) Симметричный шифр |
| 2. RSA | б) Асимметричный шифр |
| 3. SHA-256 | в) Хэш-функция |
| | г) Потоковый шифр |
| | д) Блочный шифр |

*Раздел 5. Технологии аутентификации*

Вопросы в закрытой форме.

5.1. Что понимается под аутентификацией в информационной безопасности? Выберите один ответ:

а) Процесс проверки подлинности пользователя или устройства
б) Процесс предоставления прав доступа к ресурсам
в) Процесс регистрации действий пользователя в системе
г) Процесс шифрования данных при передаче

5.2. Какая технология аутентификации основана на использовании симметричного ключа и генерации одноразовых паролей по времени или счётчику? Выберите один ответ:

а) Аутентификация по многоразовому паролю
б) Строгая аутентификация (OTP на основе симметричных алгоритмов)
в) Биометрическая аутентификация
г) Аутентификация по PIN-коду

5.3. Какое из перечисленных средств относится к аппаратно-программным системам идентификации и аутентификации? Выберите один ответ:

а) Программный генератор паролей
б) USB-токен (криптотокен)
в) Файл с хэшами паролей
г) Сервер удалённого доступа

5.4. Какие из перечисленных методов относятся к биометрической аутентификации? Выберите несколько ответов:

а) Аутентификация по отпечатку пальца

б) Аутентификация по радужной оболочке глаза
в) Аутентификация по голосу
г) Аутентификация по динамике подписи
д) Аутентификация по паролю
е) Аутентификация по PIN-коду
ж) Аутентификация по сертификату
з) Аутентификация по аппаратному токену

Вопросы в открытой форме.

5.5. Заполните пропуск:

Процесс проверки полномочий пользователя на доступ к ресурсам после успешной аутентификации называется _____.

5.6. Ответьте на вопрос:

Сколько основных факторов аутентификации принято выделять в классической модели? _____.

Вопросы на установление последовательности.

5.7. Установите правильную последовательность этапов при входе пользователя в систему (от начала к предоставлению доступа):

а) Ввод идентификатора (логина)
б) Ввод пароля (или иного аутентификатора)
в) Проверка аутентификации (сравнение с эталоном)
г) Проверка авторизации (права доступа)
д) Предоставление доступа к ресурсам

5.8. Установите правильную последовательность развития методов аутентификации от наиболее простых (наименее защищённых) к более сложным и защищённым:

а) Многоразовый пароль
б) Одноразовый пароль (на основе временных или событийных синхронизаторов)
в) Биометрическая аутентификация
г) Аппаратно-программные системы (токены, смарт-карты)

Вопросы на установление соответствия.

5.9. Установите соответствие между фактором аутентификации и примером его реализации.

| Фактор аутентификации | Пример |
|---|---|
| 1. Знание (то, что знает пользователь) | а) Пароль |
| 2. Владение (то, что имеет пользователь) | б) Аппаратный токен |
| 3. Свойство (то, чем является пользователь) | в) Отпечаток пальца |
| | г) PIN-код |
| | д) Смарт-карта |

5.10. Установите соответствие между методом аутентификации и его описанием.

| Метод аутентификации | Описание |
|---|---|
| 1. Многоразовый пароль | а) Один и тот же пароль используется многократно до смены |
| 2. Одноразовый пароль (OTP) | б) Пароль действителен только для одной сессии и генерируется алгоритмически |
| 3. Биометрическая аутентификация | в) Аутентификация на основе уникальных физиологических или поведенческих |

| | |
|---|---|
| | характеристик |
| | г) Проверка подлинности по аппаратному ключу |
| | д) Использование PIN-кода как дополнительного фактора |

*Раздел 6. Технологии межсетевых экранов*

Вопросы в закрытой форме.

6.1. Что представляет собой межсетевой экран? Выберите один ответ:

а) Программное или аппаратное средство, осуществляющее фильтрацию сетевого трафика

б) Система обнаружения вторжений

в) Антивирусное средство

г) Средство шифрования данных

6.2. На каком уровне модели OSI работает пакетный фильтр (базовый межсетевой экран)? Выберите один ответ:

а) Физический

б) Канальный

в) Сетевой

г) Транспортный

6.3. Какая дополнительная функция межсетевого экрана позволяет скрыть внутреннюю структуру сети и использовать частные IP-адреса? Выберите один ответ:

а) Трансляция сетевых адресов (NAT)

б) Аутентификация пользователей

в) Регистрация событий

г) Выполнение функций посредничества (прокси)

6.4. Какие из перечисленных функций выполняет межсетевой экран? Выберите несколько ответов:

а) Фильтрация трафика

б) Трансляция сетевых адресов (NAT)

в) Проксирование (посредничество)

г) Идентификация и аутентификация пользователей

д) Регистрация и анализ событий

е) Антивирусная проверка трафика

ж) Балансировка нагрузки

з) Шифрование данных на лету

Вопросы в открытой форме.

6.5. Заполните пропуск:

Политика, определяющая правила пропуска сетевого трафика через межсетевой экран, называется политикой _____.

6.6. Ответьте на вопрос:

Сколько сетевых интерфейсов требуется для подключения межсетевого экрана по схеме с демилитаризованной зоной? _____.

Вопросы на установление последовательности.

6.7. Установите правильную последовательность этапов обработки сетевого пакета межсетевым экраном (от приёма до передачи):

а) Приём пакета

б) Проверка правил фильтрации

в) Принятие решения (пропустить, отбросить, отклонить)
г) Регистрация события (логирование)
д) Передача пакета на выходной интерфейс (если разрешено)

6.8. Установите правильную последовательность уровней модели OSI, на которых могут функционировать межсетевые экраны, в порядке возрастания номера уровня (от самого низкого к самому высокому):
а) Сетевой
б) Транспортный
в) Сеансовый
г) Прикладной

Вопросы на установление соответствия.
6.9. Установите соответствие между функцией межсетевого экрана и её описанием.

| Функция | Описание |
|---|---|
| 1. Фильтрация трафика | а) Анализ заголовков пакетов и принятие решения о пропуске на основе правил |
| 2. Трансляция адресов (NAT) | б) Замена внутренних IP-адресов на внешний адрес и обратно |
| 3. Проксирование | в) Выполнение посредничества между клиентом и сервером, возможно с кешированием |
| 4. Регистрация событий | г) Ведение журнала событий для аудита |
| | д) Шифрование данных |
| | е) Проверка подлинности пользователей |

6.10. Установите соответствие между схемой подключения межсетевого экрана и её характеристикой.

| Схема подключения | Характеристика |
|---|---|
| 1. Шлюз | а) Один межсетевой экран с двумя сетевыми интерфейсами |
| 2. Экран с демилитаризованной зоной | б) Один межсетевой экран с тремя сетевыми интерфейсами |
| 3. Двухбарьерная схема | в) Два межсетевых экрана с демилитаризованной зоной между ними |
| | г) Один межсетевой экран с одним интерфейсом |
| | д) Межсетевой экран с функцией прокси |

*Раздел 7. Технологии защиты от вирусов*
Вопросы в закрытой форме.
7.1. Какой тип вируса заражает загрузочный сектор диска? Выберите один ответ:
а) Загрузочный вирус
б) Файловый вирус
в) Макровирус
г) Вирус-сценарий

7.2. Какой метод обнаружения вирусов основан на сравнении кода программы с известными образцами (сигнатурами)? Выберите один ответ:
а) Сигнатурный метод
б) Эвристический метод
в) Поведенческий метод
г) Метод белых списков

7.3. Какая вредоносная программа маскируется под полезное ПО и предоставляет злоумышленнику удалённый доступ к системе? Выберите один ответ:

а) Червь

б) Троянская программа

в) Макровирус

г) Файловый вирус

7.4. Какие из перечисленных видов относятся к компьютерным вирусам по среде обитания? Выберите несколько ответов:

а) Файловые

б) Загрузочные

в) Макровирусы

г) Вирусы-сценарии

д) Сетевые черви

е) Троянские программы

ж) Руткиты

з) Шифровальщики-вымогатели

Вопросы в открытой форме.

7.5. Заполните пропуск:

Метод обнаружения вирусов, основанный на сравнении кода программы с известными образцами, называется _____ обнаружением.

7.6. Ответьте на вопрос:

Сколько основных каналов распространения вредоносных программ обычно выделяют в классификации? _____.

Вопросы на установление последовательности.

7.7. Установите правильную последовательность этапов жизненного цикла вируса:

а) Маскировка

б) Активизация

в) Внедрение

г) Размножение

7.8. Установите правильную последовательность этапов построения системы антивирусной защиты корпоративной сети (от начального к заключительному):

а) Анализ рисков

б) Выбор антивирусных решений

в) Развертывание

г) Настройка политик

д) Мониторинг

Вопросы на установление соответствия.

7.9. Установите соответствие между видом вируса и его характеристикой.

| Вид вируса | Характеристика |
|---|---|
| 1. Загрузочный | а) Заражает загрузочный сектор диска |
| 2. Файловый | б) Заражает исполняемые файлы |
| 3. Макровирус | в) Заражает документы с поддержкой макросов |
| 4. Вирус-сценарий | г) Использует скрипты (JavaScript, VBS) |
| | д) Распространяется через сетевые протоколы |

7.10. Установите соответствие между методом обнаружения и его описанием.

| Метод обнаружения | Описание |
|---|---|
| 1. Сигнатурный | а) Сравнение кода с базой известных сигнатур |
| 2. Эвристический | б) Анализ структуры кода на подозрительные признаки |
| 3. Поведенческий | в) Мониторинг действий программы в процессе выполнения |
| 4. Метод белых списков | г) Разрешение только утверждённых программ |
| | д) Использование эмуляции для проверки |

*Раздел 8. Требования к системам защиты информации*

Вопросы в закрытой форме.

8.1. Что определяет класс защищённости автоматизированной системы? Выберите один ответ:

а) Степень доверия к системе со стороны государства

б) Уровень гарантированной защищённости от несанкционированного доступа

в) Количество установленных средств защиты

г) Сложность парольной политики

8.2. Какое требование предъявляется к защите информации при работе с системами управления базами данных? Выберите один ответ:

а) Обязательное шифрование всех полей таблиц

б) Разграничение доступа на уровне записей и полей

в) Использование только облачных СУБД

г) Отказ от использования транзакций

8.3. Какой показатель характеризует способность системы противостоять попыткам несанкционированного доступа в течение заданного времени? Выберите один ответ:

а) Стойкость защиты

б) Вероятность преодоления защиты

в) Время непрерывной работы

г) Пропускная способность каналов

8.4. Какие меры защиты информации являются обязательными при обработке персональных данных согласно законодательству РФ? Выберите несколько ответов:

а) Разграничение доступа пользователей

б) Регистрация событий безопасности

в) Применение средств криптографической защиты

г) Назначение ответственного за обработку персональных данных

д) Регулярный аудит безопасности

е) Установка антивирусного ПО

ж) Резервное копирование баз данных

з) Обучение персонала мерам защиты

Вопросы в открытой форме.

8.5. Заполните пропуск:

В РФ классы защищённости автоматизированных систем от несанкционированного доступа установлены в _____ документе Гостехкомиссии.

8.6. Ответьте на вопрос:

Сколько классов защищённости автоматизированных систем от несанкционированного доступа установлено в действующей классификации? _____.

Вопросы на установление последовательности.

8.7. Установите правильную последовательность этапов оценки защищённости автоматизированной системы:

а) Анализ исходных требований

б) Разработка модели угроз

в) Выбор и обоснование мер защиты

г) Проверка эффективности принятых мер

д) Оформление результатов (аттестация)

8.8. Установите правильную последовательность уровней доступа к информации в автоматизированной системе по степени уменьшения прав (от наивысших к наименьшим):

а) Администратор системы

б) Привилегированный пользователь

в) Пользователь с частичными правами

г) Гость (минимальный доступ)

Вопросы на установление соответствия.

8.9. Установите соответствие между объектом защиты и типовым требованием к его защите.

| Объект защиты | Требование |
|---|---|
| 1. Автоматизированная система | а) Обеспечение разграничения доступа на уровне сессий и ролей |
| 2. Локальная вычислительная сеть | б) Защита каналов передачи данных и сегментация сети |
| 3. Рабочее место пользователя | в) Установка персонального межсетевого экрана и антивируса |
| 4. Система управления базами данных | г) Контроль доступа к записям и полям таблиц |
| | д) Резервное копирование всей системы |

8.10. Установите соответствие между показателем защищённости и его определением.

| Показатель | Определение |
|---|---|
| 1. Стойкость защиты | а) Минимальное время, в течение которого система успешно противостоит атакам |
| 2. Вероятность преодоления | б) Вероятность того, что злоумышленник преодолеет защиту за заданное время |
| 3. Время защиты | в) Максимальное время непрерывной работы системы без сбоев |
| | г) Количество зафиксированных попыток вторжения |
| | д) Степень сложности паролей |

*Раздел 9. Основы правового обеспечения защиты информации*

Вопросы в закрытой форме.

9.1. Что является объектом правового регулирования информационного права? Выберите один ответ:

а) Информация и информационные отношения

б) Имущество

в) Личные неимущественные права

г) Результаты интеллектуальной деятельности

9.2. Какой федеральный закон регулирует отношения, связанные с защитой государственной тайны? Выберите один ответ:

а) ФЗ "О государственной тайне"
б) ФЗ "Об информации, информационных технологиях и о защите информации"
в) ФЗ "О персональных данных"
г) ФЗ "Об электронной подписи"

9.3. Что из перечисленного является элементом правового регулирования деятельности организаций в области информационной безопасности? Выберите один ответ:
а) Лицензирование деятельности по защите информации
б) Установка антивирусного ПО
в) Проведение аудита безопасности
г) Разработка политики безопасности

9.4. Какие федеральные законы являются базовыми в системе законодательства об информационной безопасности Российской Федерации? Выберите несколько ответов:
а) ФЗ "Об информации, информационных технологиях и о защите информации"
б) ФЗ "О государственной тайне"
в) ФЗ "О персональных данных"
г) ФЗ "Об электронной подписи"
д) ФЗ "О связи"
е) ФЗ "О рекламе"
ж) ФЗ "О защите прав потребителей"
з) ФЗ "О банках и банковской деятельности"

Вопросы в открытой форме.
9.5. Заполните пропуск:
Правовая защита интеллектуальной собственности в Российской Федерации регламентируется частью _____ Гражданского кодекса РФ.

9.6. Заполните пропуск:
Государственная политика в области обеспечения информационной безопасности определяется _____.

Вопросы на установление последовательности.
9.7. Установите правильную последовательность этапов формирования государственной системы правового обеспечения информационной безопасности (от начального к текущему):
а) Принятие Конституции РФ
б) Принятие базовых федеральных законов
в) Создание системы органов государственного управления в области ИБ
г) Разработка Доктрины информационной безопасности

9.8. Установите иерархию нормативных правовых актов в области информационной безопасности по убыванию юридической силы (сверху вниз):
а) Конституция РФ
б) Федеральные законы
в) Указы Президента
г) Постановления Правительства

Вопросы на установление соответствия.
9.9. Установите соответствие между законом и его предметом регулирования.

| Закон | Предмет регулирования |
|---|---|
| 1. ФЗ "О государственной тайне" | а) Регулирование отношений при |

| | |
|---|---|
| | обработке персональных данных |
| 2. ФЗ "О персональных данных" | б) Регулирование защиты сведений, составляющих государственную тайну |
| 3. ФЗ "Об электронной подписи" | в) Регулирование использования электронной подписи |
| 4. ФЗ "Об информации, информационных технологиях и о защите информации" | г) Регулирование отношений в сфере информации и информационных технологий |
| | д) Регулирование авторских прав |

9.10. Установите соответствие между видом интеллектуальной собственности и его объектом.

| Вид права | Объект |
|---|---|
| 1. Авторское право | а) Произведения науки, литературы и искусства |
| 2. Патентное право | б) Изобретения, полезные модели, промышленные образцы |
| 3. Смежные права | в) Исполнения, фонограммы, передачи |
| 4. Ноу-хау (секрет производства) | г) Коммерческая тайна (секрет производства) |
| | д) Товарные знаки |

***Шкала оценивания тестов №1-4*** *(очная форма)*: 4 балльная.

Тест №1 включает вопросы из 1 и 2 разделов, тест №2 – вопросы из 3-5 разделов, тест №3 – вопросы из 6 и 7 разделов, тест №4 – вопросы из 8 и 9 разделов.

***Критерии оценивания*** *(очная форма)**:***

Тест состоит из 10 вопросов (по 3 вопроса в открытой и закрытой формах, по 2 вопроса на установление соответствия и на установление последовательности). Процент правильных ответов переводится в баллы БРС и 5-балльной шкалу следующим образом:

- **85-100% – 4 балла** соответствует оценке **«отлично»**;
- **70-84% – 3 балла** – оценке **«хорошо»;**
- **50-69% – 2 балла** – оценке **«удовлетворительно»;**
- **0-49% – 1 балл** – оценке «**неудовлетворительно».**

***Шкала оценивания тестов №1-2*** *(заочная форма)*: 4 балльная.

Тест №1 включает вопросы из 1-5 разделов, тест №2 – вопросы из 6-9 разделов.

***Критерии оценивания*** *(заочная форма)**:***

Тест состоит из 20 вопросов (по 6 вопроса в открытой и закрытой формах, по 4 вопроса на установление соответствия и на установление последовательности). Процент правильных ответов переводится в баллы БРС и 5-балльной шкалу следующим образом:

- **85-100% – 7-8 баллов** соответствует оценке **«отлично»**;
- **70-84% – 6 баллов** – оценке **«хорошо»;**
- **50-69% – 4-5 баллов** – оценке **«удовлетворительно»;**
- **0-49% – 1-3 балла** – оценке «**неудовлетворительно».**

## *1.2 ВОПРОСЫ И ЗАДАНИЯ ДЛЯ ЗАЩИТЫ ЛАБОРАТОРНЫХ РАБОТ*

*Раздел 4. Криптографическая защита информации*

Лабораторная работа №1 «Разработка криптографической программы «Алгоритм RSA»

1.1. В чём заключается алгоритм RSA?

1.2. Для чего и почему используют комбинированные криптоалгоритмы?

1.3. В чём заключаются достоинства и недостатки асимметричных алгоритмов?

1.4. В чём заключаются достоинства и недостатки симметричных алгоритмов?

1.5. Какие параметры блочных шифров влияют на его криптостойкость?

1.6. Каким образом происходит преобразование текстового сообщения в числовое представление m в алгоритме RSA, и какое условие должно соблюдаться для числа m относительно модуля N?

1.7. Какова роль функции Эйлера φ(N) в алгоритме RSA, и каким образом вычисляется секретная экспонента d на основе открытой экспоненты e и значения φ(N)? Опишите математическую связь между ними.

1.8. Почему в алгоритме RSA нельзя шифровать сообщение, числовое значение которого превышает модуль N, и как эта проблема решается на практике при работе с длинными текстами?

1.9. В чем заключается уязвимость алгоритма RSA, связанная с выбором малых значений открытой экспоненты E (например, 3), и какие меры предосторожности рекомендуются для повышения криптостойкости?

1.10. Для чего при практической реализации RSA часто используют комбинированные схемы шифрования (гибридные криптосистемы), где RSA применяется только для шифрования сеансового ключа симметричного алгоритма, а не всего сообщения?

Лабораторная работа №2 «Разработка криптографической программы «Шифр Виженера»

2.1. Заданы две подстановки Вижинера с периодами $d_1$=56 и $d_2$=33, применяемые последовательно. Каков будет общий период такого шифра?

2.2. Каким способом осуществляется подавление телефонных закладок в устройстве, описанном в файле DEV3.doc.?

2.3. Какова зона подавления, которое обеспечивает устройство, описанном в файле DEV31.doc.?

2.4. Какой текст называется открытым?

2.5. Какой текст называется закрытым?

2.6. В чём заключается основное отличие шифра Виженера от моноалфавитных шифров (например, от шифра Цезаря)? За счёт какого механизма достигается многоалфавитность?

2.7. Опишите процедуру использования ключевого слова при шифровании текста методом Виженера. Как поступают, если длина ключа меньше длины открытого сообщения? Приведите пример циклического повторения ключа.

2.8. Запишите математические формулы для шифрования $C_i = (P_i + K_i) \bmod 32$ и расшифрования $P_i = (C_i – K_i + 31) \bmod 32$ применительно к русскому алфавиту (32 буквы). Поясните, почему в формуле расшифрования добавляется 31, а не просто вычитание по модулю.

2.9. Какие исторические личности внесли вклад в создание шифра Виженера (Альберти, Трисемус, Беллазо, Виженер)? Почему шифр получил имя именно Блеза Виженера, хотя он не был первым автором этого метода?

2.10. Почему в XIX–XX веках шифр Виженера считался невзламываемым и получил репутацию «неподдающегося взлому»? Каким образом (и кем) впоследствии была показана его уязвимость?

*Раздел 6. Технологии межсетевых экранов*

Лабораторная работа №3 «Настройка межсетевого экрана в ОС Windows»

3.1. Дайте определение межсетевого экрана?

3.2. В чем заключается механизм межсетевого экранирования?

3.3. В чем отличия программных и программно-аппаратных МЭ?

3.4. От каких угроз не может защитить МЭ?

3.5. Если на ПК будет установлено два МЭ, будут ли они конфликтовать?

3.6. С какими трудностями встретится пользователь при наличии двух МЭ на ПК?

3.7. Какие достоинства и недостатки есть при наличии установленного программного МЭ на ПК?

3.8. Какие сетевые профили (доменный, частный, общедоступный) предлагает брандмауэр Windows и какова их роль в обеспечении безопасности?

3.9. В чём заключается различие между настройкой правил для входящих и исходящих подключений в брандмауэре Windows, и какой из этих типов трафика по умолчанию блокируется, а какой разрешается?

3.10. Для чего в брандмауэре Windows используется ведение журнала безопасности (логирование) и какая информация записывается в файл журнала?

*Раздел 8. Требования к системам защиты информации*

Лабораторная работа №4 «Шифрование с помощью программы TrueCrypt»

4.1. Для какой цели используются группы в программе TrueCrypt?

4.2. Какие поля по умолчанию используются в записях? Можно ли добавить дополнительные поля в записях?

4.3. Какие типы паролей можно создавать с помощью генератора паролей? Дайте их краткую характеристику.

4.4. Объясните, что такое пасскарта в программе TrueCrypt?

4.5. В каком виде хранятся пароли в программе TrueCrypt по умолчанию?

4.6. Какие три варианта создания новых томов для хранения секретных данных поддерживает программа TrueCrypt?

4.7. Какие алгоритмы шифрования поддерживает программа TrueCrypt?

4.8. Что означает флажок «–не сохранять историю‖» в программе TrueCrypt?

4.9. Если мы используем файл в качестве тома, каково может быть имя и расширение файла?

4.10. Если мы используем файл в качестве тома, по какой причине рекомендуется создать новый файл, а не использовать уже имеющийся файл?

***Шкала оценивания защиты лабораторных работ*** *(очная форма):* 8 балльная.

***Критерии оценивания:***

8 баллов (или оценка «отлично») выставляется обучающемуся, если работа правильно выполнена, и доля правильных ответов на «защите» составила более 85% заданий.

7 баллов (или оценка «хорошо») выставляется обучающемуся, если работа правильно выполнена, и доля правильных ответов на «защите» составила 75-84% заданий.

6 баллов (или оценка «хорошо») выставляется обучающемуся, если работа правильно выполнена, и доля правильных ответов на «защите» составила 65-74% заданий.

5 баллов (или оценка «удовлетворительно») выставляется обучающемуся, если работа правильно выполнена, и доля правильных ответов на «защите» составила 55-64% заданий.

4 балла (или оценка «удовлетворительно») выставляется обучающемуся, если работа правильно выполнена, и доля правильных ответов на «защите» составила 50-54% заданий.

0-3 балла (или оценка «неудовлетворительно») выставляется обучающемуся, если работа выполнена не полностью или доля правильных ответов на «защите» составила менее 50% заданий.

***Шкала оценивания защиты лабораторных работ*** *(заочная форма):* 10 балльная.

***Критерии оценивания:***

10 баллов (или оценка «отлично») выставляется обучающемуся, если работа правильно выполнена, и доля правильных ответов на «защите» составила более 90% заданий.

9 баллов (или оценка «отлично») выставляется обучающемуся, если работа правильно выполнена, и доля правильных ответов на «защите» составила 85-90% заданий.

8 баллов (или оценка «хорошо») выставляется обучающемуся, если работа правильно выполнена, и доля правильных ответов на «защите» составила 79-84% заданий.

7 баллов (или оценка «хорошо») выставляется обучающемуся, если работа правильно выполнена, и доля правильных ответов на «защите» составила 70-77% заданий.

6 баллов (или оценка «удовлетворительно») выставляется обучающемуся, если работа правильно выполнена, и доля правильных ответов на «защите» составила 60-69% заданий.

5 баллов (или оценка «удовлетворительно выставляется обучающемуся, если работа правильно выполнена, и доля правильных ответов на «защите» составила 55-59% заданий.

0-4 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если работа выполнена не полностью или доля правильных ответов на «защите» составила менее 50% заданий.

## 2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

### *2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ*

1 Вопросы в закрытой форме.

1.1. Законы, нормативные акты, стандарты относятся к каким мерам защиты субъектов информационных отношений? Выберите один ответ:

а) административным

б) законодательным

в) процедурным

1.2. Качество передачи сигналов передачи данных оценивается по ….. . Выберите один ответ:

а) искажениям формы сигналов

б) отсутствию искажения в принятой информации

в) числу ошибок в принятой информации, т.е. верности передачи

1.3. Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления – это ….. . Выберите один ответ:

а) данные

б) информация

в) знания

1.4. Угроза безопасности – это ….. . Выберите один ответ:

а) совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации

б) нарушение целостности информации

в) комплекс мероприятий, проводимых для взлома информации

1.5. Что из нижеперечисленного не относится к параметрам системы защиты информации? Выберите один ответ:

а) входы и выходы системы

б) процессы внутри системы, занимающиеся преобразованием информации

в) цели и задачи

1.6. Что из нижеперечисленного относится к важным свойствам информации? Выберите один ответ:

а) полезность

б) доступность

в) новизна

1.7. Конфиденциальность информации – это ….. . Выберите один ответ:

а) действия, проводимые с целью закрытия доступа к информации субъектов, не имеющих на это право

б) состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право

в) состояние информации, при котором доступ к ней субъектами, не имеющими на это права, осуществляется лишь в некоторых случаях

1.8. Состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно, называется ….. . Выберите один ответ:

а) допустимость

б) доступность
в) целостность

1.9. Что представляет собой предотвращение пассивных атак для передаваемых или хранимых данных? Выберите один ответ:
а) конфиденциальность
б) контроль доступа
в) аутентификация

1.10. Принцип Кирхгофа утверждает, что ….. . Выберите один ответ:
а) секретность ключа определена секретностью открытого сообщения
б) секретность информации определена скоростью передачи данных
в) секретность закрытого сообщения определяется секретностью ключа

1.11. ЭЦП – это ….. . Выберите один ответ:
а) электронно-цифровой преобразователь
б) электронно-цифровая подпись
в) электронно-цифровой процессор

1.12. Какие из перечисленных средств относятся к основным средствам защиты данных? Выберите несколько ответов:
а) резервное копирование наиболее ценных данных
б) аппаратные средства
в) программные средства

1.13. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? Выберите один ответ:
а) сотрудники
б) хакеры
в) атакующие
г) контрагенты (лица, работающие по договору)

1.14. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое действие следует предпринять руководству? Выберите один ответ:
а) снизить уровень безопасности этой информации для обеспечения ее доступности
б) требовать подписания специального разрешения каждый раз при доступе
в) улучшить контроль за безопасностью этой информации
г) снизить уровень классификации этой информации

1.15. Что самое главное должно продумать руководство при классификации данных? Выберите один ответ:
а) типы сотрудников, контрагентов и клиентов, которые будут иметь доступ
б) необходимый уровень доступности, целостности и конфиденциальности
в) оценить уровень риска и отменить контрмеры
г) управление доступом, которое должно защищать данные

1.16. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков? Выберите один ответ:
а) никогда, для обеспечения хорошей безопасности нужно учитывать и снижать все риски
б) когда риски не могут быть приняты во внимание по политическим соображениям

в) когда необходимые защитные меры слишком сложны

г) когда стоимость контрмер превышает ценность актива и потенциальные потери

1.17. Эффективная программа безопасности требует сбалансированного применения ….. . Выберите один ответ:

а) технических и нетехнических методов

б) контрмер и защитных механизмов

в) физической безопасности и технических средств защиты

г) процедур безопасности и шифрования

1.18. Если используются автоматизированные инструменты для анализа рисков, почему всё равно требуется много времени для проведения анализа? Выберите один ответ:

а) много информации нужно собрать и ввести в программу

б) руководство должно одобрить создание группы

в) анализ рисков не может быть автоматизирован по своей природе

г) множество людей должно одобрить данные

1.19. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности? Выберите один ответ:

а) список стандартов, процедур и политик для разработки программы безопасности

б) текущая версия ISO 17799

в) структура, разработанная для снижения внутреннего мошенничества

г) открытый стандарт, определяющий цели контроля

1.20. Из каких четырёх доменов состоит CobiT? Выберите один ответ:

а) Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

б) Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

в) Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка

г) Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

1.21. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO? Выберите один ответ:

а) COSO – подход к управлению рисками, относящийся к контрольным объектам и бизнес-процессам

б) COSO относится к стратегическому уровню, а CobiT – к операционному

в) COSO учитывает корпоративную культуру и разработку политик

г) COSO – система отказоустойчивости

1.22. Что лучше всего описывает цель расчета ALE (Annualized Loss Expectancy)? Выберите один ответ:

а) количественно оценить уровень безопасности среды

б) оценить потенциальные потери от угрозы в год

в) количественно оценить затраты и выгоды

г) оценить возможные потери для каждой контрмеры

1.23. К конфиденциальной информации относятся документы, содержащие ….. . Выберите один ответ:

а) государственную тайну

б) законодательные акты
в) ноу-хау
г) сведения о золотом запасе страны

1.24. Запрещено относить к информации ограниченного доступа ….. . Выберите один ответ:
а) информацию о чрезвычайных ситуациях
б) информацию о деятельности органов государственной власти
в) документы открытых архивов и библиотек
г) всё перечисленное в остальных пунктах

1.25. Что не относится к конфиденциальной информации? Выберите один ответ:
а) коммерческая тайна
б) персональные данные о гражданах
в) государственная тайна
г) ноу-хау

1.26. Для успешной реализации концепции комплексной защиты при построении автоматизированной системы ….. . Выберите один ответ:
а) необходимо создать несколько последовательных зон безопасности
б) следует установить некоторый приемлемый уровень безопасности без попыток создать абсолютную защиту
в) должны быть разработаны и регулярно использоваться все необходимые механизмы гарантированного обеспечения требуемого уровня защищённости
г) требуется предварительное ранжирование угроз по степени важности

1.27. Исходным пунктом проектирования систем защиты информации является ….. . Выберите один ответ:
а) формирование требований к защите информации
б) определение значений важнейших параметров защищаемой информации
в) построение математической модели системы защиты
г) разработка процедур оперативного реагирования на непредвиденные ситуации

1.28. Для долгосрочного управления комплексной системой защиты характерно ….. . Выберите один ответ:
а) использование только средств защиты, которые включены в состав системы и находятся в работоспособном состоянии
б) большое внимание развитию и совершенствованию концепции защиты
в) преобладание процедур оперативного реагирования над иными процедурами управления
г) отсутствие изменений в архитектуре средств защиты и автоматизированной системы

1.29. Непрерывное слежение за функционированием механизмов защиты относится к показателям ….. . Выберите один ответ:
а) планирования управления защитой
б) календарно-планового руководства защитой информации
в) обеспечения повседневной деятельности средств защиты
г) оперативно-диспетчерского управления

1.30. Организация и обеспечение выполнения плановых мероприятий по защите информации является целью ….. . Выберите один ответ:
а) планирования управления защитой

б) календарно-планового руководства защитой информации
в) обеспечения повседневной деятельности средств защиты
г) оперативно-диспетчерского управления

1.31. Какой метод анализа рисков пытается определить, где вероятнее всего произойдёт сбой? Выберите один ответ:
а) анализ связующего дерева
б) AS/NZS
в) NIST
г) анализ сбоев и дефектов

1.32. Что было разработано, чтобы помочь странам построить законодательство по защите персональных данных похожим образом? Выберите один ответ:
а) Безопасная OECD
б) ISOIEC
в) OECD

1.33. Метод шифрования, при котором символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, называется ….. . Выберите один ответ:
а) гаммирования
б) подстановки
в) кодирования
г) перестановки
д) аналитических преобразований

1.34. Защита информации от утечки – это деятельность по предотвращению ….. . Выберите один ответ:
а) получения защищаемой информации заинтересованным субъектом с нарушением установленных прав или правил доступа
б) воздействия с нарушением установленных прав на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа
в) воздействия на защищаемую информацию ошибок пользователя, сбоя технических и программных средств, природных явлений
г) неконтролируемого распространения защищаемой информации от её разглашения, несанкционированного доступа и получения злоумышленниками
д) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей

1.35. Искусственные угрозы безопасности информации вызваны ….. . Выберите один ответ:
а) деятельностью человека
б) ошибками при проектировании АСОИ или разработке ПО
в) воздействиями объективных физических процессов или стихийных природных явлений
г) корыстными устремлениями злоумышленников
д) ошибками при действиях персонала

1.36. К основным непреднамеренным искусственным угрозам АСОИ относится ….. Выберите один ответ:
а) физическое разрушение системы путём взрыва, поджога и т.п.
б) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи

в) изменение режимов работы устройств или программ, саботаж персонала, постановка мощных активных помех

г) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств

д) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению ресурсов

1.37. Антивирус, который запоминает исходное состояние программ, каталогов и системных областей диска, а затем сравнивает текущее состояние с исходным, называется ….. . Выберите один ответ:

а) детектор

б) доктор

в) сканер

г) ревизор

д) сторож

1.38. Антивирус, представляющий собой небольшую резидентную программу для обнаружения подозрительных действий, характерных для вирусов, называется ….. . Выберите один ответ:

а) детектор

б) доктор

в) сканер

г) ревизор

д) сторож

1.39. Активный перехват информации – это перехват, который ….. . Выберите один ответ:

а) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации

б) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники

в) неправомерно использует технологические отходы информационного процесса

г) осуществляется путём использования оптической техники

д) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера

1.40. Перехват, заключающийся в установке подслушивающего устройства в аппаратуру средств обработки информации, называется ….. . Выберите один ответ:

а) активный перехват

б) пассивный перехват

в) аудиоперехват

г) видеоперехват

д) просмотр мусора

1.41. Перехват, основанный на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники, называется ….. . Выберите один ответ:

а) активный перехват

б) пассивный перехват

в) аудиоперехват

г) видеоперехват

1.42. Перехват, осуществляемый с использованием оптической техники, называется ….. . Выберите один ответ:

а) активный перехват

б) пассивный перехват

в) аудиоперехват

г) видеоперехват

д) просмотр мусора

1.43. К внутренним нарушителям информационной безопасности относятся ….. . Выберите несколько ответов:

а) клиенты

б) пользователи системы

в) посетители

г) любые лица, находящиеся внутри контролируемой территории

д) представители организаций, взаимодействующих по вопросам жизнедеятельности

е) персонал, обслуживающий технические средства

ж) сотрудники отделов разработки и сопровождения ПО

з) технический персонал, обслуживающий здание

1.44. Организационная структура службы информационной безопасности определяется ….. . Выберите один ответ:

а) требованиями законодательства

б) требованиями государственных и международных стандартов

в) потребностями в защите информационных ресурсов и возможностями в соответствии с оценками руководителей

1.45. В состав службы информационной безопасности предприятия могут быть включены ….. . Выберите один ответ:

а) отдел нормативной документации

б) отдел технической поддержки пользователей

в) отдел внутреннего аудита информационной безопасности

г) отдел персонала

1.46. Отбор персонала при назначении на должности, связанные с обработкой конфиденциальной информации, включает в себя ….. . Выберите несколько ответов:

а) психологическую оценку

б) проверку знания внутренних регламентов работы с информацией

в) оценку навыков использования средств обнаружения вторжений

1.47. В методологии работы с персоналом фигурируют такие понятия, как ….. . Выберите один ответ:

а) социальная инженерия, человеческий фактор, человеко-машинная система

б) моделирование, анализ

в) контроль, система обработки данных

1.48. К задачам обучения и информационной работы с персоналом предприятия относится ….. . Выберите несколько ответов:

а) недопущение утечек информации с использованием уязвимостей в сетях и ПО

б) ознакомление с требованиями законодательства и локальных регламентов

в) противодействие методам социальной инженерии

1.49. Приёмы социотехники основаны на ….. . Выберите один ответ:

а) особенностях человеческой психологии

б) недостатках организационных структур

в) недостатках программных и аппаратных средств защиты информации

1.50. Обучение персонала, ответственного за обработку информации, включает в себя ….. . Выберите несколько ответов:

а) изучение автоматизированных систем обнаружения вторжений

б) изучение приёмов и методов защиты информации, необходимых для выполнения должностных обязанностей

в) ознакомление с возможными мерами ответственности в случае нарушения требований информационной безопасности

1.51. Основным противодействием методам социальной инженерии является ….. . Выберите один ответ:

а) повышение надёжности криптографических алгоритмов

б) информационная работа с персоналом предприятия

в) страхование информационных ресурсов

1.52. Социальная инженерия – это ….. . Выберите один ответ:

а) метод нарушения информационной безопасности

б) метод защиты от нарушений информационной безопасности

в) метод осуществления общественных связей

1.53. Нарушения информационной безопасности с использованием социотехники предполагают ….. . Выберите один ответ:

а) социологическое обследование персонала предприятия

б) использование недостатков в организационной структуре предприятия

в) обман сотрудников предприятия

1.54. Регламент реагирования на инциденты должен предусматривать ….. . Выберите один ответ:

а) регламент круглосуточного дежурства технического персонала

б) распределение функций персонала в процессе реагирования на инциденты

в) соглашение с поставщиками ИТ-платформ о срочной поставке компонент, вышедших из строя

1.55. Обнаружение вторжений осуществляется на основе ….. . Выберите один ответ:

а) косвенных признаков, сигнатур и сообщений пользователей

б) внутренних признаков и сообщений администратора

в) внешних признаков

1.56. К косвенным признакам, по которым могут быть выявлены нарушения информационной безопасности, относятся ….. . Выберите несколько ответов:

а) опубликование конфиденциальной информации в открытых источниках

б) использование баз данных и учётных записей в нехарактерное время

в) резкое повышение нагрузки на информационные системы предприятия

1.57. На персонал, отвечающий за обнаружение вторжений, оказывает влияние такой негативный психологический фактор, как ….. . Выберите один ответ:

а) круглосуточный режим дежурства

б) необходимость постоянно изучать новые методы анализа вирусов

в) частые ложные сообщения пользователей о предполагаемом заражении вирусами

1.58. Высокий уровень полномочий необходим для локализации длящихся нарушений в связи с тем, что ….. . Выберите один ответ:

а) локализация требует дорогостоящих услуг сторонних аналитиков

б) может потребоваться временное оперативное отключение важных информационных систем предприятия

в) необходимо проинформировать о нарушениях большое число пользователей

1.59. Ущерб от нарушения информационной безопасности включает в себя ….. . Выберите несколько ответов:

а) уменьшение рыночной капитализации

б) упущенную выгоду

в) штрафные санкции за разглашение конфиденциальной информации

1.60. Расследование нападений, совершённых из корпоративной сети, по сравнению с нападением из внешней сети, является ….. . Выберите один ответ:

а) более лёгким

б) более сложным

в) аналогичным по сложности

1.61. Выявление вторжения в процессе его совершения по сравнению с выявлением уже завершённого нарушения ….. . Выберите один ответ:

а) упрощает выявление нарушителя

б) усложняет выявление нарушителя

в) никак не влияет на сложность выявления нарушителя

1.62. Анализ действий нарушителя необходим для ….. . Выберите один ответ:

а) проверки правильности настроек систем защиты информации

б) установления сведений, известных нарушителю до нападения

в) установления круга контактов, которые могли быть у нарушителя до нападения

1.63. Кто является основным ответственным за определение уровня классификации информации? Выберите один ответ:

а) руководитель среднего звена

б) высшее руководство

в) владелец

г) пользователь

1.64. Кто в конечном счёте несёт ответственность за гарантии того, что данные классифицированы и защищены? Выберите один ответ:

а) владельцы данных

б) пользователи

в) администраторы

г) руководство

1.65. Что такое процедура? Выберите один ответ:

а) правила использования программного и аппаратного обеспечения

б) пошаговая инструкция по выполнению задачи

в) руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

г) обязательные действия

1.66. Какой фактор наиболее важен для уверенности в успешном обеспечении безопасности в компании? Выберите один ответ:

а) поддержка высшего руководства

б) эффективные защитные меры и методы их внедрения

в) актуальные и адекватные политики и процедуры безопасности

г) проведение тренингов по безопасности для всех сотрудников

1.67. Что такое политики безопасности? Выберите один ответ:

а) пошаговые инструкции по выполнению задач безопасности

б) общие руководящие требования по достижению определённого уровня безопасности

в) широкие, высокоуровневые заявления руководства

г) детализированные документы по обработке инцидентов безопасности

1.68. Какая техника является самой важной при выборе конкретных защитных мер? Выберите один ответ:

а) анализ рисков

б) анализ затрат и выгоды

в) результаты ALE

г) выявление уязвимостей и угроз, являющихся причиной риска

1.69. Тактическое планирование – это ….. . Выберите один ответ:

а) среднесрочное планирование

б) долгосрочное планирование

в) ежедневное планирование

г) планирование на 6 месяцев

1.70. Что является определением воздействия (exposure) на безопасность? Выберите один ответ:

а) нечто, приводящее к ущербу от угрозы

б) любая потенциальная опасность для информации или систем

в) любой недостаток или отсутствие информационной безопасности

г) потенциальные потери от угрозы

1.71. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют ….. . Выберите один ответ:

а) внедрение управления механизмами безопасности

б) классификацию данных после внедрения механизмов

в) уровень доверия, обеспечиваемый механизмом безопасности

г) соотношение затрат и выгод

1.72. Какое утверждение правильно отражает разницу в целях безопасности для коммерческой и военной организации? Выберите один ответ:

а) только военные имеют настоящую безопасность

б) коммерческая компания обычно больше заботится о целостности и доступности, а военные – о конфиденциальности

в) военным требуется больший уровень безопасности, т.к. их риски существенно выше

г) коммерческая компания больше заботится о доступности и конфиденциальности, а военные – о целостности

1.73. Как рассчитать остаточный риск? Выберите один ответ:

а) угрозы × риски × ценность актива

б) (угрозы × ценность актива × уязвимости) × риски
в) SLE × частоту ALE
г) (угрозы × уязвимости × ценность актива) × недостаток контроля

1.74. Что из перечисленного не является целью проведения анализа рисков? Выберите один ответ:
а) делегирование полномочий
б) количественная оценка воздействия потенциальных угроз
в) выявление рисков
г) определение баланса между воздействием риска и стоимостью контрмер

1.75. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности? Выберите один ответ:
а) поддержка
б) выполнение анализа рисков
в) определение цели и границ
г) делегирование полномочий

1.76. Почему при проведении анализа информационных рисков следует привлекать специалистов из различных подразделений компании? Выберите один ответ:
а) чтобы убедиться, что проводится справедливая оценка
б) это не требуется, для анализа достаточно небольшой группы независимых специалистов
в) поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях
г) поскольку люди в различных подразделениях сами являются причиной рисков, они должны быть ответственны за их оценку

1.77. Что является наилучшим описанием количественного анализа рисков? Выберите один ответ:
а) анализ, основанный на сценариях, для выявления различных угроз
б) метод для точной оценки потенциальных потерь, вероятности и рисков
в) метод, сопоставляющий денежное значение с каждым компонентом оценки рисков
г) метод, основанный на суждениях и интуиции

1.78. Почему количественный анализ рисков в чистом виде не достижим? Выберите один ответ:
а) он достижим и используется
б) он присваивает уровни критичности, которые сложно перевести в денежный вид
в) это связано с точностью количественных элементов
г) количественные измерения должны применяться к качественным элементам

1.79. Какой законодательный термин относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств? Выберите один ответ:
а) стандарты
б) должный процесс (due process)
в) должная забота (due care)
г) снижение обязательств

1.80. Наиболее распространённые средства воздействия на сеть офиса – это ….. . Выберите один ответ:

а) слабый трафик, информационный обман, вирусы в интернет

б) вирусы в сети, логические мины (закладки), информационный перехват

в) компьютерные сбои, изменение администрирования, топологии

1.81. Утечкой информации в системе называется ситуация, характеризуемая ….. . Выберите один ответ:

а) потерей данных в системе

б) изменением формы информации

в) изменением содержания информации

1.82. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности, являются ….. . Выберите несколько ответов:

а) целостность

б) доступность

в) актуальность

1.83. Угроза информационной системе (компьютерной сети) – это ….. . Выберите один ответ:

а) вероятное событие

б) детерминированное (всегда определённое) событие

в) событие, происходящее периодически

1.84. Информация, которую следует защищать по нормативам, правилам сети, системы, называется ….. . Выберите один ответ:

а) регламентированной

б) правовой

в) защищаемой

1.85. Разновидностями угроз безопасности (сети, системы) являются ….. . Выберите один ответ:

а) программные, технические, организационные, технологические

б) серверные, клиентские, спутниковые, наземные

в) личные, корпоративные, социальные, национальные

1.86. Окончательно, ответственность за защищённость данных в компьютерной сети несёт ….. . Выберите один ответ:

а) владелец сети

б) администратор сети

в) пользователь сети

1.87. Политика безопасности в системе (сети) – это комплекс ….. . Выберите один ответ:

а) руководств, требований обеспечения необходимого уровня безопасности

б) инструкций, алгоритмов поведения пользователя в сети

в) норм информационного права, соблюдаемых в сети

1.88. Наиболее важным при реализации защитных мер политики безопасности является ….. . Выберите один ответ:

а) аудит, анализ затрат на проведение защитных мер

б) аудит, анализ безопасности

в) аудит, анализ уязвимостей и риск-ситуаций

1.89. Основная масса угроз информационной безопасности приходится на ….. . Выберите один ответ:

а) троянские программы

б) шпионские программы

в) черви

1.90. Какой вид идентификации и аутентификации получил наибольшее распространение? Выберите один ответ:

а) системы PKI

б) постоянные пароли

в) одноразовые пароли

1.91. Какие угрозы безопасности информации являются преднамеренными? Выберите один ответ:

а) ошибки персонала

б) открытие электронного письма, содержащего вирус

в) несанкционированный доступ

1.92. Какие из перечисленных угроз относятся к угрозам нарушения доступности информации? Выберите несколько ответов:

а) Блокирование доступа пользователей к данным

б) Отказ в обслуживании (Denial of Service)

в) Несанкционированное копирование файлов

г) Выход узла сети из строя, в результате чего доступ к ресурсам становится невозможным

д) Прослушивание канала связи

е) Перехват информации без её модификации

ж) Ограничение доступа к информационному ресурсу

з) Несанкционированное изменение данных

1.93. Какие из перечисленных угроз характерны для беспроводных сетей? Выберите несколько ответов:

а) Несанкционированное подключение к точке доступа

б) Прослушивание трафика (сниффинг)

в) Атака типа "человек посередине"

г) Подмена MAC-адреса

д) Атака на WEP-шифрование

е) Отказ в обслуживании (DoS)

ж) Внедрение вредоносного кода через веб-страницы

з) Фишинг по электронной почте

1.94. Какие из перечисленных политик относятся к специализированным политикам безопасности? Выберите несколько ответов:

а) Политика управления доступом

б) Политика использования интернета

в) Политика паролей

г) Политика защиты от вирусов

д) Политика резервного копирования

е) Политика конфиденциальности персональных данных

ж) Политика физической защиты

з) Политика реагирования на инциденты

1.95. Какие из перечисленных алгоритмов относятся к симметричным криптосистемам? Выберите несколько ответов:

а) AES
б) DES
в) RSA
г) ГОСТ 28147-89
д) RC4
е) Эль-Гамаль
ж) SHA-256
з) MD5

1.96. Какие из перечисленных методов относятся к биометрической аутентификации? Выберите несколько ответов:

а) Аутентификация по отпечатку пальца
б) Аутентификация по радужной оболочке глаза
в) Аутентификация по голосу
г) Аутентификация по динамике подписи
д) Аутентификация по паролю
е) Аутентификация по PIN-коду
ж) Аутентификация по сертификату
з) Аутентификация по аппаратному токену

1.97. Какие из перечисленных функций выполняет межсетевой экран? Выберите несколько ответов:

а) Фильтрация трафика
б) Трансляция сетевых адресов (NAT)
в) Проксирование (посредничество)
г) Идентификация и аутентификация пользователей
д) Регистрация и анализ событий
е) Антивирусная проверка трафика
ж) Балансировка нагрузки
з) Шифрование данных на лету

1.98. Какие из перечисленных видов относятся к компьютерным вирусам по среде обитания? Выберите несколько ответов:

а) Файловые
б) Загрузочные
в) Макровирусы
г) Вирусы-сценарии
д) Сетевые черви
е) Троянские программы
ж) Руткиты
з) Шифровальщики-вымогатели

1.99. Какие меры защиты информации являются обязательными при обработке персональных данных согласно законодательству РФ? Выберите несколько ответов:

а) Разграничение доступа пользователей
б) Регистрация событий безопасности
в) Применение средств криптографической защиты
г) Назначение ответственного за обработку персональных данных
д) Регулярный аудит безопасности
е) Установка антивирусного ПО
ж) Резервное копирование баз данных

з) Обучение персонала мерам защиты

1.100. Какие федеральные законы являются базовыми в системе законодательства об информационной безопасности Российской Федерации? Выберите несколько ответов:

а) ФЗ "Об информации, информационных технологиях и о защите информации"

б) ФЗ "О государственной тайне"

в) ФЗ "О персональных данных"

г) ФЗ "Об электронной подписи"

д) ФЗ "О связи"

е) ФЗ "О рекламе"

ж) ФЗ "О защите прав потребителей"

з) ФЗ "О банках и банковской деятельности"

2 Вопросы в открытой форме.

2.1. Заполните пропуск:

Свойство информации, означающее её доступность только для авторизованных лиц, называется _____.

2.2. Заполните пропуск:

Информация, имеющая коммерческую ценность и защищаемая от разглашения, относится к _____.

2.3. Заполните пропуск:

Состояние информации, при котором она не подвергалась несанкционированным изменениям, называется _____.

2.4. Заполните пропуск:

Устройство, предназначенное для фильтрации сетевого трафика, называется _____.

2.5. Заполните пропуск:

Функция межсетевого экрана, заключающаяся в замене внутренних IP-адресов на внешний адрес, называется _____.

2.6. Заполните пропуск:

Алгоритм шифрования, использующий один ключ для шифрования и расшифрования, называется _____.

2.7. Заполните пропуск:

Алгоритм шифрования, использующий пару ключей, называется _____.

2.8. Заполните пропуск:

Процесс проверки подлинности пользователя называется _____.

2.9. Заполните пропуск:

Метод аутентификации, основанный на уникальных физиологических характеристиках человека, называется _____.

2.10. Заполните пропуск:

Вид компьютерного вируса, заражающего исполняемые файлы, называется _____.

2.11. Заполните пропуск:

Вид компьютерного вируса, заражающего загрузочный сектор диска, называется _____.

2.12. Заполните пропуск:

Метод обнаружения вирусов, анализирующий структуру кода на подозрительные признаки, называется _____.

2.13. Заполните пропуск:

Протокол стека TCP/IP, отвечающий за надёжную доставку данных между приложениями, называется _____.

2.14. Заполните пропуск:

Атака, заключающаяся в подмене сетевого адреса отправителя, называется _____.

2.15. Заполните пропуск:

Атака, целью которой является нарушение доступности ресурса путём перегрузки, называется _____.

2.16. Заполните пропуск:

Документ, определяющий правила и процедуры защиты информации в организации, называется _____.

2.17. Заполните пропуск:

Подсистема системы защиты информации, отвечающая за регистрацию и анализ событий, называется _____.

2.18. Заполните пропуск:

Средство обнаружения вторжений, работающее в реальном времени, называется _____.

2.19. Заполните пропуск:

Метод шифрования, при котором каждый символ заменяется другим по определённому правилу, называется _____.

2.20. Заполните пропуск:

Метод шифрования, при котором символы переставляются согласно ключу, называется _____.

2.21. Заполните пропуск:

Угроза, при которой злоумышленник только наблюдает за передачей данных, называется _____.

2.22. Заполните пропуск:

Величина, характеризующая ожидаемый годовой ущерб от реализации угрозы, называется _____.

2.23. Заполните пропуск:

Длина ключа в алгоритме AES-256 составляет _____ бит.

2.24. Заполните пропуск:

Длина блока в алгоритме AES составляет _____ байт.

2.25. Заполните пропуск:

Количество раундов в алгоритме AES-128 равно _____.

2.26. Заполните пропуск:

Попытка реализации угрозы называется _____, а тот, кто предпринимает такую попытку, – злоумышленником.

2.27. Заполните пропуск:

В соответствии с классификацией удалённых угроз по цели воздействия выделяют три основных класса угроз: нарушение конфиденциальности информации (класс 2.1), нарушение целостности информации (класс 2.2) и нарушение _____ информации (класс 2.3).

2.28. Заполните пропуск:

Процедуры безопасности описывают _____ действия, которые должны быть выполнены для реализации политики безопасности.

2.29. Ответьте на вопрос:

Сколько уровней политики безопасности обычно выделяют в организации? _____.

2.30. Заполните пропуск:

Электронная цифровая подпись предназначена для подтверждения подлинности и _____ электронного документа, а также для обеспечения неотказуемости от авторства.

2.31. Ответьте на вопрос:

Какой алгоритм хэширования имеет длину выхода 256 бит и входит в состав стандарта SHA-2? _____.

2.32. Заполните пропуск:

Процесс проверки полномочий пользователя на доступ к ресурсам после успешной аутентификации называется _____.

2.33. Ответьте на вопрос:

Сколько основных факторов аутентификации принято выделять в классической модели? _____.

2.34. Заполните пропуск:

Политика, определяющая правила пропуска сетевого трафика через межсетевой экран, называется политикой _____.

2.35. Ответьте на вопрос:

Сколько сетевых интерфейсов требуется для подключения межсетевого экрана по схеме с демилитаризованной зоной? _____.

2.36. Заполните пропуск:

Метод обнаружения вирусов, основанный на сравнении кода программы с известными образцами, называется _____ обнаружением.

2.37. Ответьте на вопрос:

Сколько основных каналов распространения вредоносных программ обычно выделяют в классификации? _____.

2.38. Заполните пропуск:

В РФ классы защищённости автоматизированных систем от несанкционированного доступа установлены в _____ документе Гостехкомиссии.

2.39. Ответьте на вопрос:

Сколько классов защищённости автоматизированных систем от несанкционированного доступа установлено в действующей классификации? _____.

2.40. Заполните пропуск:

Правовая защита интеллектуальной собственности в Российской Федерации регламентируется частью _____ Гражданского кодекса РФ.

2.41. Заполните пропуск:

Государственная политика в области обеспечения информационной безопасности определяется _____.

2.42. Ответьте на вопрос:

Какой протокол используется для безопасного удалённого управления сервером? _____.

2.43. Заполните пропуск:

Вредоносная программа, распространяющаяся по сети и не требующая заражения других файлов, называется _____.

2.44. Ответьте на вопрос:

Какой стандарт ISO определяет требования к системе менеджмента информационной безопасности? _____.

2.45. Заполните пропуск:

Процесс восстановления исходного текста из зашифрованного с использованием ключа называется _____.

2.46. Ответьте на вопрос:

Какова длина ключа (в битах) в алгоритме ГОСТ 28147-89? _____.

2.47. Заполните пропуск:

На сетевом уровне модели OSI для маршрутизации используется протокол _____.

2.48. Ответьте на вопрос:

Как называется злоумышленная программа, собирающая информацию о пользователе без его ведома? _____.

2.49. Заполните пропуск:

Процесс предоставления прав доступа к ресурсам после успешной аутентификации называется _____.

2.50. Ответьте на вопрос:

Сколько уровней в стеке протоколов TCP/IP? _____.

3. Вопросы на установление последовательности.

3.1. Установите правильную последовательность этапов работы по обеспечению режима информационной безопасности.

а) Выявление максимально полного множества потенциальных угроз, способов и

каналов их осуществления

б) Определение и выработка политики информационной безопасности

в) Определение совокупности целей создания системы ИБ и сферы ее функционирования

г) Выявление уязвимостей, проведение оценки рисков, формирование методик управления рисками

3.2. Установите правильную последовательность этапов защиты от угроз безопасности.

а) Предоставление персоналу защищенного удаленного доступа к информационным ресурсам

б) Обеспечение безопасного доступа к открытым ресурсам внешних сетей и Интернет

в) Защита внешних каналов передачи информации

г) Разработка политики информационной безопасности

д) Анализ угроз безопасности

3.3. Установите правильную последовательность этапов стадии исполнения компьютерных вирусов.

а) Выполнение деструктивных функций

б) Передача управления программе-носителю вируса

в) Поиск жертвы

г) Заражение найденной жертвы

д) Загрузка вируса в память

3.4. Установите правильную последовательность этапов построения системы антивирусной защиты сети.

а) Реализация плана антивирусной безопасности

б) Проведение анализа объекта защиты и определение основных принципов обеспечения антивирусной безопасности

в) Разработка политики антивирусной безопасности

г) Разработка плана обеспечения антивирусной безопасности

3.5. Установите правильную последовательность приоритетных этапов защиты информации.

а) Защита информации от несанкционированного доступа

б) Защита информации в системах связи

в) Защита юридической значимости электронных документов

г) Защита конфиденциальной информации от утечки по каналам побочных электромагнитных излучений и наводок

д) Защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ

е) Защита от несанкционированного копирования и распространения программ и ценной компьютерной информации

3.6. Установите правильную последовательность этапов построения программы обеспечения безопасности.

а) Проведение разъяснительных мероприятий и обучения персонала

б) Регулярный контроль пошаговой реализации плана безопасности

в) Установление уровня безопасности

г) Формирование политики безопасности организации

д) Определение ценности технологических и информационных активов организации

3.7. Установите правильную последовательность действий этапа анализа рисков.

а) Оценка вероятности реализации угрозы на практике

б) Оценка рисков технологических и информационных активов

в) Идентификация и оценка стоимости технологических и информационных активов

г) Анализ угроз, для которых активы являются целевым объектом

3.8. Установите правильную последовательность процессов для обнаружения и выдачи сигнала тревоги.

а) Одно системное событие не является достаточным для утверждения об опасности

б) Если результат превышает пороговую величину, выдается сигнал тревоги

в) Совокупность событий сравнивается с пороговой величиной

г) Каждое нарушение безопасности генерирует системное событие

3.9. Установите правильную последовательность параметров для группировки данных на сервере сбора информации об атаке.

а) Дата, время

б) Протокол

в) Порт получателя

г) Номер агента

д) IP-адрес атакующего

е) Тип атаки

3.10. Установите правильную последовательность стандартов информационной безопасности в порядке возрастания даты их разработки.

а) ISO 27001:2005

б) ISO/IEC 17799

в) ISO/IEC 15408

г) Критерии оценки доверенных компьютерных систем

3.11. Установите правильную последовательность этапов процесса управления рисками информационной безопасности.

а) Классификация рисков, выбор методологии оценки и проведение оценки

б) Анализ угроз и их последствий, определение слабостей в защите

в) Выбор, реализация и проверка защитных мер

г) Оценка остаточного риска

д) Идентификация активов и ценности ресурсов

е) Выбор анализируемых объектов и степени детальности

3.12. Установите правильную последовательность этапов проведения аудита информационной безопасности.

а) Разработка рекомендаций по повышению уровня защиты

б) Анализ полученных данных

в) Сбор исходных данных

г) Разработка регламента проведения аудита

3.13. Установите правильную последовательность объектов защиты по степени важности (от высшей к низшей).

а) Коммерческая тайна (ценность определяется собственником)

б) Персональные данные (ограниченный доступ по федеральным законам)

в) Государственная тайна (высший уровень защиты)

3.14. Установите правильную последовательность этапов процесса комплекса превентивных мер.

а) Подача и рассмотрение заявки

б) Предварительное ознакомление специалистов с аттестуемыми объектами

в) Разработка программы и методики испытаний

г) Запрос и получение необходимой технической документации

д) Проведение испытаний

е) Оформление, регистрация и выдача аттестата (сертификата соответствия)

3.15. Установите правильную последовательность алгоритма испытаний.

а) Анализ информационных потоков, системы в целом и отдельных объектов

б) Оценка правильности классификации и выбора средств защиты

в) Проверка сертификатов на ПО и оборудование

г) Проведение аттестационных испытаний и оформление протоколов

д) Оформление заключения по результатам проверок

3.16. Установите правильную последовательность этапов проведения моделирования угроз.

а) Определение негативных последствий от угроз

б) Определение объектов воздействия угроз

в) Оценка возможности реализации угроз и их актуальности

3.17. Установите правильную последовательность этапов реализации механизмов безопасности в ОС в порядке их внедрения.

а) Создание кольцевой системы защиты процессора

б) Реализация аутентификации пользователя

в) Реализация многозадачности

г) Создание виртуальных контейнеров для запуска приложений

3.18. Установите правильную последовательность этапов создания системы защиты персональных данных.

а) Опытная и промышленная эксплуатация

б) Проектный этап

в) Аттестация или декларирование

г) Предпроектный этап

3.19. Установите правильную последовательность этапов разработки профиля защиты.

а) Анализ среды применения ИТ-продукта с точки зрения безопасности

б) Выбор профиля-прототипа

в) Синтез требований

3.20. Установите правильную последовательность этапов реагирования на инциденты информационной безопасности.

а) Обнаружение инцидента

б) Сдерживание и локализация

в) Искоренение (удаление причины)

г) Восстановление систем

д) Анализ и извлечение уроков

3.21. Установите правильную последовательность исторического развития шифров (от наиболее простых к современным):

а) Шифр простой замены

б) Шифр Виженера (полиалфавитный)
в) Блочные шифры (DES, AES)
г) Асимметричные криптосистемы (RSA)

3.22. Установите правильную последовательность уровней модели OSI, на которых могут функционировать межсетевые экраны, в порядке возрастания номера уровня (от самого низкого к самому высокому):
а) Сетевой
б) Транспортный
в) Сеансовый
г) Прикладной

3.23. Установите правильную последовательность этапов жизненного цикла вируса:
а) Маскировка
б) Активизация
в) Внедрение
г) Размножение

3.24. Установите правильную последовательность уровней доступа к информации в автоматизированной системе по степени уменьшения прав (от наивысших к наименьшим):
а) Администратор системы
б) Привилегированный пользователь
в) Пользователь с частичными правами
г) Гость (минимальный доступ)

3.25. Установите иерархию нормативных правовых актов в области информационной безопасности по убыванию юридической силы (сверху вниз):
а) Конституция РФ
б) Федеральные законы
в) Указы Президента
г) Постановления Правительства

4 Вопросы на установление соответствия.
4.1. Установите соответствие между этапом аудита информационной безопасности и его содержанием.

| Этап | Содержание |
|---|---|
| 1. Выявление критически важной информации | а) Определение документов и данных, утечка которых наносит максимальный ущерб |
| 2. Выявление слабых мест в защите | б) Анализ уязвимостей и недостатков существующей системы защиты |
| 3. Оценка возможностей защиты | в) Определение эффективности мер защиты и выбор необходимых контрмер |
| | г) Проведение обучения персонала по безопасности |
| | д) Разработка политики безопасности |

4.2. Установите соответствие между аспектом информационной безопасности и его содержанием.

| Аспект | Содержание |
|---|---|
| 1. Конфиденциальность | а) Предотвращение несанкционированного доступа к информации |
| 2. Целостность | б) Защита от несанкционированных изменений и |

| | |
|---|---|
| | уничтожения |
| 3. Доступность | в) Обеспечение своевременного доступа авторизованных пользователей |
| | г) Обеспечение актуальности информации |
| | д) Гарантирование юридической значимости данных |

4.3. Установите соответствие между видом угрозы и её проявлением.

| Угроза | Проявление |
|---|---|
| 1. Аппаратная угроза | а) Нарушение работоспособности оборудования |
| 2. Угроза утечки информации | б) Несанкционированный доступ и потеря данных |
| 3. Нестабильность программного обеспечения | в) Некорректная работа приложений и сбои |
| | г) Физическое разрушение системы |
| | д) Перехват трафика по сети |

4.4. Установите соответствие между средством защиты информации и его назначением.

| Средство | Назначение |
|---|---|
| 1. Антивирусная программа | а) Обнаружение и удаление компьютерных вирусов |
| 2. CloudAV | б) Облачное решение для обнаружения вредоносного кода |
| 3. DLP-решения | в) Защита от утечек конфиденциальной информации |
| 4. Криптографическое преобразование | г) Преобразование данных в неявный вид с помощью шифрования |
| | д) Средство для анализа сетевого трафика |
| | е) Система обнаружения вторжений |

4.5. Установите соответствие между понятием в области защиты информации и его определением.

| Понятие | Определение |
|---|---|
| 1. Защита информации | а) Деятельность по предотвращению утечки и несанкционированных воздействий |
| 2. Объект защиты | б) Информация, носитель или информационный процесс, подлежащие защите |
| 3. Цель защиты информации | в) Желаемый результат – предотвращение ущерба |
| 4. Эффективность защиты | г) Степень соответствия результатов поставленной цели |
| | д) Совокупность организационных мер |
| | е) Процесс управления рисками |

4.6. Установите соответствие между видом защиты и её содержанием.

| Вид защиты | Содержание |
|---|---|
| 1. Защита от утечки | а) Предотвращение неконтролируемого распространения информации |
| 2. Защита от разглашения | б) Предотвращение несанкционированного доведения информации до посторонних |
| 3. Защита от несанкционированного доступа (НСД) | в) Предотвращение получения информации нарушителем |
| 4. Система защиты информации | г) Совокупность органов, исполнителей и средств защиты |
| | д) Правовое обеспечение защиты |
| | е) Организационные меры |

4.7. Установите соответствие между правовым термином и его значением.

| Термин | Значение |
|---|---|
| 1. Доступ к информации | а) Возможность ознакомления с информацией |
| 2. Оперативность доступа | б) Способность информации быть доступной в нужный момент |
| 3. Собственник информации | в) Субъект, реализующий полномочия владения, пользования, распоряжения |
| 4. Владелец информации | г) Субъект, осуществляющий владение и пользование в пределах прав |
| | д) Администратор системы |
| | е) Пользователь |

4.8. Установите соответствие между элементом системы защиты и его характеристикой.

| Элемент | Характеристика |
|---|---|
| 1. Способ защиты | а) Порядок и правила применения средств защиты |
| 2. Средство защиты | б) Техническое, программное средство для защиты |
| 3. Комплекс средств защиты | в) Совокупность средств защиты, контроля и управления |
| 4. Техника защиты | г) Технические средства защиты |
| | д) Организационные меры |
| | е) Правовые нормы |

4.9. Установите соответствие между видом гарантированности защиты и её описанием.

| Вид гарантированности | Описание |
|---|---|
| 1. Операционная гарантированность | а) Охватывает весь жизненный цикл системы |
| 2. Технологическая гарантированность | б) Относится к архитектурным и реализационным аспектам |
| 3. Доверенная вычислительная база | в) Совокупность защитных механизмов системы |
| | г) Уровень доверия к системе |
| | д) Сертификация системы |

4.10. Установите соответствие между методом управления доступом и его характеристикой.

| Метод | Характеристика |
|---|---|
| 1. Произвольное управление доступом | а) Метод, основанный на личности субъекта |
| 2. Безопасность повторного использования объектов | б) Защита от извлечения информации из остаточной памяти |
| 3. Метки безопасности | в) Свойства объектов и субъектов доступа |
| 4. Принудительное (мандатное) управление доступом | г) Метод, основанный на сопоставлении меток безопасности |
| | д) Ролевое управление доступом |
| | е) Разграничение по времени |

4.11. Установите соответствие между понятием в области аутентификации и его определением.

| Понятие | Определение |
|---|---|
| 1. Ядро безопасности | а) Совокупность компонентов, реализующих функции защиты |
| 2. Аутентификация | б) Проверка подлинности пользователя или устройства |
| 3. Идентификация | в) Присвоение уникальных меток субъектам |

| | |
|---|---|
| 4. Адекватность защиты | г) Показатель эффективности и надежности защиты |
| | д) Авторизация |
| | е) Регистрация событий |

4.12. Установите соответствие между видом обеспечения информационной системы и его содержанием.

| Вид обеспечения | Содержание |
|---|---|
| 1. Математическое и программное обеспечение | а) Математические методы, модели, алгоритмы и программы |
| 2. Организационное обеспечение | б) Методы и средства, регламентирующие взаимодействие персонала |
| 3. Правовое обеспечение | в) Правовые нормы, определяющие создание и функционирование ИС |
| | г) Техническое обеспечение |
| | д) Информационное обеспечение |

4.13. Установите соответствие между этапом жизненного цикла ИС и его определением.

| Этап | Определение |
|---|---|
| 1. Сопровождение | а) Обеспечение штатной эксплуатации системы |
| 2. Функционирование | б) Штатный процесс эксплуатации в соответствии с целями и задачами |
| 3. Внедрение | в) Установка и ввод системы в действие |
| 4. Тестирование | г) Проверка соответствия системы заданным показателям |
| | д) Разработка |
| | е) Проектирование |

4.14. Установите соответствие между принципом построения системы защиты и его сущностью.

| Принцип | Сущность |
|---|---|
| 1. Принцип интеграции | а) Установление связей между компонентами для обеспечения целостности |
| 2. Принцип системности | б) Рассмотрение всех сторон объекта в связи с другими процессами |
| 3. Принцип комплексности | в) Однократный ввод данных и их многократное использование |
| | г) Принцип эшелонированной защиты |
| | д) Принцип минимальных привилегий |

4.15. Установите соответствие между категорией персональных данных и её содержанием.

| Категория | Содержание |
|---|---|
| 1. Специальные категории ПДн | а) Информация о расовой, национальной принадлежности, религии, здоровье |
| 2. Биометрические ПДн | б) Биологические и физиологические особенности личности |
| 3. Общедоступные ПДн | в) Сведения, доступ к которым предоставлен самим субъектом |
| 4. Иные категории ПДн | г) Данные субъектов, не являющихся работниками организации |
| | д) Коммерческая тайна |
| | е) Служебная тайна |

4.16. Установите соответствие между уровнем политики безопасности и его характеристикой.

| Уровень | Характеристика |
|---|---|
| 1. Верхний уровень | а) Определяет стратегические цели и общие принципы защиты |
| 2. Средний уровень | б) Разрабатывает тактические стандарты и решения |
| 3. Нижний уровень | в) Устанавливает конкретные правила и инструкции для операционной деятельности |
| | г) Описывает процедуры реагирования на инциденты |
| | д) Содержит шаблоны документов |

4.17. Установите соответствие между типом криптосистемы и её особенностью.

| Тип | Особенность |
|---|---|
| 1. Симметричная криптосистема | а) Использует один ключ для шифрования и расшифрования |
| 2. Асимметричная криптосистема | б) Использует пару ключей (открытый и закрытый) |
| 3. Хэш-функция | в) Преобразует данные произвольной длины в строку фиксированного размера |
| | г) Использует потоковое шифрование |
| | д) Применяется только для аутентификации |

4.18. Установите соответствие между фактором аутентификации и примером его реализации.

| Фактор | Пример |
|---|---|
| 1. Знание (то, что знает пользователь) | а) Пароль или PIN-код |
| 2. Владение (то, что имеет пользователь) | б) Аппаратный токен или смарт-карта |
| 3. Свойство (то, чем является пользователь) | в) Отпечаток пальца или радужная оболочка |
| | г) Голосовая биометрия |
| | д) Электронная подпись |

4.19. Установите соответствие между функцией межсетевого экрана и её описанием.

| Функция | Описание |
|---|---|
| 1. Фильтрация трафика | а) Анализ заголовков пакетов и принятие решения о пропуске на основе правил |
| 2. Трансляция сетевых адресов (NAT) | б) Замена внутренних IP-адресов на внешний и обратно |
| 3. Проксирование (посредничество) | в) Выполнение посредничества между клиентом и сервером |
| | г) Шифрование данных |
| | д) Балансировка нагрузки |

4.20. Установите соответствие между показателем защищённости и его определением.

| Показатель | Определение |
|---|---|
| 1. Стойкость защиты | а) Минимальное время, в течение которого система успешно противостоит атакам |
| 2. Вероятность преодоления | б) Вероятность того, что злоумышленник преодолеет защиту за заданное время |
| 3. Время защиты | в) Максимальное время непрерывной работы системы без сбоев |

| | |
|---|---|
| | г) Количество зафиксированных попыток вторжения |
| | д) Степень сложности паролей |

4.21. Установите соответствие между методом аутентификации и его описанием.

| Метод аутентификации | Описание |
|---|---|
| 1. Многоразовый пароль | а) Один и тот же пароль используется многократно до смены |
| 2. Одноразовый пароль (OTP) | б) Пароль действителен только для одной сессии и генерируется алгоритмически |
| 3. Биометрическая аутентификация | в) Аутентификация на основе уникальных физиологических или поведенческих характеристик |
| | г) Проверка подлинности по аппаратному ключу |
| | д) Использование PIN-кода как дополнительного фактора |

4.22. Установите соответствие между схемой подключения межсетевого экрана и её характеристикой.

| Схема подключения | Характеристика |
|---|---|
| 1. Шлюз | а) Один межсетевой экран с двумя сетевыми интерфейсами |
| 2. Экран с демилитаризованной зоной | б) Один межсетевой экран с тремя сетевыми интерфейсами |
| 3. Двухбарьерная схема | в) Два межсетевых экрана с демилитаризованной зоной между ними |
| | г) Один межсетевой экран с одним интерфейсом |
| | д) Межсетевой экран с функцией прокси |

4.23. Установите соответствие между методом обнаружения и его описанием.

| Метод обнаружения | Описание |
|---|---|
| 1. Сигнатурный | а) Сравнение кода с базой известных сигнатур |
| 2. Эвристический | б) Анализ структуры кода на подозрительные признаки |
| 3. Поведенческий | в) Мониторинг действий программы в процессе выполнения |
| 4. Метод белых списков | г) Разрешение только утверждённых программ |
| | д) Использование эмуляции для проверки |

4.24. Установите соответствие между показателем защищённости и его определением.

| Показатель | Определение |
|---|---|
| 1. Стойкость защиты | а) Минимальное время, в течение которого система успешно противостоит атакам |
| 2. Вероятность преодоления | б) Вероятность того, что злоумышленник преодолеет защиту за заданное время |
| 3. Время защиты | в) Максимальное время непрерывной работы системы без сбоев |
| | г) Количество зафиксированных попыток вторжения |
| | д) Степень сложности паролей |

4.25. Установите соответствие между видом интеллектуальной собственности и его объектом.

| Вид права | Объект |
|---|---|
| 1. Авторское право | а) Произведения науки, литературы и искусства |
| 2. Патентное право | б) Изобретения, полезные модели, промышленные образцы |
| 3. Смежные права | в) Исполнения, фонограммы, передачи |
| 4. Ноу-хау (секрет производства) | г) Коммерческая тайна (секрет производства) |
| | д) Товарные знаки |

***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 заочной форме – 60 баллов (установлено положением П 02.016).

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

Соответствие 100-балльной и дихотомической шкал

| *Сумма баллов по 100-балльной шкале* | *Оценка по дихотомической шкале* |
|---|---|
| 100-50 | зачтено |
| 49 и менее | незачтено |

**Критерии оценивания результатов тестирования** (очная форма)**:**

Каждый тестовый вопрос в закрытой форме оценивается по дихотомической шкале: выполнено – **1 балл**, не выполнено – **0 баллов**. Каждый тестовый вопрос (задание) в открытой форме, на установление соответствия и на установление последовательности оценивается по дихотомической шкале: выполнено – **2 балла**, не выполнено – **0 баллов**.

**Критерии оценивания результатов тестирования** (заочная форма)**:**

Каждый вопрос (задание) в тестовой форме оценивается по дихотомической шкале: выполнено – **3 балла**, не выполнено – **0 баллов**.

## *2.2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ*

*Компетентностно-ориентированная задача № 1*

Зашифровать строку «Стремитесь не к успеху, а к ценностям, которые он дает», используя шифрование с помощью таблицы Виженера.

*Компетентностно-ориентированная задача № 2*

Зашифровать строку «Лучшая месть – огромный успех», используя шифр RSA.

*Компетентностно-ориентированная задача № 3*

Зашифровать строку «Упади семь раз и восемь раз поднимись.», используя алгоритм шифрования Эль-Гамаля.

*Компетентностно-ориентированная задача № 4*

Настройте политику паролей в локальной групповой политике Windows (минимальная длина, сложность, срок действия) в соответствии с рекомендациями базовой политики безопасности организации.

*Компетентностно-ориентированная задача № 5*

Разработайте фрагмент политики безопасности для отдела кадров, регламентирующий порядок работы с персональными данными сотрудников и ответственность за их разглашение.

*Компетентностно-ориентированная задача № 6*

Зашифровать строку «Я не жертва обстоятельств, я - результат моих решений.», используя алгоритм шифрования Деффи-Хеллмана.

*Компетентностно-ориентированная задача № 7*

Зашифровать строку «Надо любить жизнь больше, чем смысл жизни», используя шифрование с помощью таблицы Виженера.

*Компетентностно-ориентированная задача № 8*

Настройте брандмауэр Windows для блокировки всех входящих подключений, кроме разрешённых для порта 443 (HTTPS) и порта 3389 (RDP) только с доверенного IP-адреса.

*Компетентностно-ориентированная задача № 9*

Зашифровать строку «Лучшая месть – огромный успех», используя шифр RSA.

*Компетентностно-ориентированная задача № 10*

Зашифровать строку «Если нет ветра, беритесь за вёсла.», используя алгоритм шифрования Эль-Гамаля.

*Компетентностно-ориентированная задача № 11*

Зашифровать строку «Я не провалил тест. Я просто нашел сто способов написать его неправильно.», используя алгоритм шифрования Деффи-Хеллмана.

*Компетентностно-ориентированная задача № 12*

Опишите схему подключения межсетевого экрана типа «скрининг-роутер» для защиты корпоративной сети и перечислите правила фильтрации для предотвращения DoS-атак.

*Компетентностно-ориентированная задача № 13*

Проведите анализ уязвимостей беспроводной сети стандарта 802.11 с использованием WPA2-PSK и предложите меры по усилению безопасности (смена пароля, включение WPA3, настройка MAC-фильтрации).

*Компетентностно-ориентированная задача № 14*

Включите шифрование твердотельного накопителя используя операционную систему Windows 10.

*Компетентностно-ориентированная задача № 15*

Воспользовавшись операционной системой Linux произведите сканирование локальной сети на поиск подозрительных устройств.

*Компетентностно-ориентированная задача № 16*

Зашифровать строку «Научитесь говорить “Я не знаю”, и это уже будет прогресс.», используя шифр RSA.

*Компетентностно-ориентированная задача № 17*

Создайте электронную цифровую подпись (ЭЦП) для текстового документа с помощью утилиты OpenSSL и проверьте её подлинность, используя открытый ключ сертификата.

*Компетентностно-ориентированная задача № 18*

Настройте двухфакторную аутентификацию для входа в операционную систему с использованием смарт-карты и PIN-кода (или программного токена) в среде Windows.

*Компетентностно-ориентированная задача № 19*

Зашифровать строку «Жизнь - это то, что с тобой происходит, пока ты строишь планы.», используя шифрование с помощью таблицы Виженера.

*Компетентностно-ориентированная задача № 20*

Зашифровать строку «Мы становимся тем, о чем мы думаем.», используя алгоритм шифрования Эль-Гамаля.

*Компетентностно-ориентированная задача № 21*

Опишите модель поведения нарушителя для административного корпуса завода ООО «СтройМаш».

*Компетентностно-ориентированная задача № 22*

Зашифровать строку «Стоит только поверить, что вы можете – и вы уже на полпути к цели.», используя шифр RSA.

*Компетентностно-ориентированная задача № 23*

Составьте перечень нормативно-правовых актов Российской Федерации, регулирующих защиту информации, и укажите, какие из них применимы для организации, работающей с персональными данными граждан РФ.

*Компетентностно-ориентированная задача № 24*

Разработайте план мероприятий по защите информации при взаимодействии корпоративной сети с сетью Интернет (включая использование VPN, шифрование трафика, применение антивирусов и МЭ).

*Компетентностно-ориентированная задача № 25*

Выполните резервное копирование заголовка тома TrueCrypt (или аналогичного контейнера) и восстановите его в случае повреждения, используя встроенные средства программы.

*Компетентностно-ориентированная задача № 26*

Зашифровать строку «Я не провалил тест. Я просто нашел сто способов написать его неправильно.», используя алгоритм шифрования Деффи-Хеллмана.

*Компетентностно-ориентированная задача № 27*

Не имея непосредственного доступа к персональному компьютеру, совершите удаленный запуск приложений на нём.

*Компетентностно-ориентированная задача № 28*

Зашифровать строку «Неудача – это просто возможность начать снова, но уже более мудро.» используя шифрование с помощью таблицы Виженера.

*Компетентностно-ориентированная задача № 29*

Произведите установку антивирусного программного обеспечения на персональный компьютер.

*Компетентностно-ориентированная задача № 30*

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 заочной форме – 60 баллов (установлено положением П 02.016).

Максимальное количество баллов за решение компетентностно-ориентированной задачи по очной форме – 10 баллов, по заочной форме – 15 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 дихотомический шкале следующим образом:

Соответствие 100-балльной и дихотомической шкал

| *Сумма баллов по 100-балльной шкале* | *Оценка по дихотомической шкале* |
|---|---|
| 100-50 | зачтено |
| 49 и менее | незачтено |

***Критерии оценивания решения компетентностно-ориентированной задачи***

**10-9 баллов** (очная форма)**, 15-12 баллов** (заочная форма) выставляется обучающемуся, если решение задачи демонстрирует глубокое понимание обучающимся предложенной проблемы и разностороннее ее рассмотрение; 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.

**8-7 балла** (очная форма)**, 11-8 баллов** (заочная форма) 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).

**6-4 балла** (очная форма)**, 7-4 баллов** (заочная форма) 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.

**0-3 баллов** (очная форма)**, 0-3 баллов** (заочная форма) 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.