МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

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

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

Управление информационной безопасностью
(наименование учебной дисциплины)

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

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

Тема 1. Основные понятия технологии программирования.

Какие угрозы должны быть устранены и в какой мере?

1. Какие ресурсы системы должны быть защищаемы и в какой степени?
2. С помощью каких средств должна быть реализована защита?
3. Какова должна быть полная стоимость реализации защиты и затраты на эксплуатацию с учетом потенциальных угроз?
4. Проблема информационной безопасности общества.
5. Составляющие информационной безопасности.
6. Система формирования информационной безопасности
7. Что предполагает динамическая целостность информации?
8. Что предполагает статическая целостность информации?
9. Понятие конфиденциальности в ИБ.
10. Какие существуют уровни формирования информационной безопасности?

Тема 2. Проблемы информационной безопасности сетей

1. Какие механизмы обеспечения безопасности существуют?
2. Какие проблемы информационной безопасности вы знаете?
3. Правильно построенная архитектура решает некоторые проблемы ИБ сетей?
4. Компрометация информации является угрозой?
5. На какие типы делят угрозы ИБ сетей?
6. Раскрытие конфиденциальной информации является угрозой?
7. Несанкционированный обмен информацией подразумевает угрозу?
8. Опишите умышленные угрозы.
9. Расскажите о пассивных угрозах.
10. Несанкционированное использование ресурсов сети увеличивает риски ИБ сетей?

Тема 3. Политика безопасности

1. Какие системы вовлекаются в политику безопасности?
2. Роль информации и информационных систем Компании.
3. Основные подразделения, работающие в области защиты информации.
4. Что такое категорирование сотрудников?
5. Расскажите классификацию информации в организациях.

6. Что такое «внутренние сетевые подключения»?
7. Что такое «маркирование информации»?
8. Что такое «изменения в топологии сети»?
9. Опишите порядок работы с электронной почтой.
10. Нужна ли в организации политика учетных записей?
11. Какие требования выдвигаются к партнерам (третьим сторонам)?

Тема 4. Криптографическая защита информации.

1. Какие средства криптографической защиты информации вы знаете?
2. Что такое Шифрование?
3. Назовите 3 цели шифрования.
4. Конфиденциальность как цель шифрования.
5. Неизменность как цель шифрования.
6. Подтверждение источника как цель шифрования.
7. Опишите процесс передачи данных от одного человека к другому с использованием метода шифрования.
8. Какие алгоритмы шифрования вы знаете?
9. На какие категории делятся алгоритмы?
10. Хэш-функции как средство защиты информации.
11. Что такое ключ в шифровании?

Тема 5. Технологии аутентификации.

1. Определения аутентификация, идентификация, авторизация, Классификация с точки зрения применяемых технологий.
2. Парольная аутентификация, плюсы и минусы.
3. Двухфакторная и многофакторная аутентификация, электронные ключи Rutoken, eToken.
4. Смарт-карты, описание, классификация по способу обмена со считывающим устройством, сферы применения.
5. Локальная аутентификация Windows, схема работы.
6. Распределенные COA (distributed IDS), принцип работы, основные подсистемы.
7. Системы Security Information and Event Management (SIEM), назначение, основные задачи.
8. Основные источники данных для SIEM.
9. Схема работы протокола NTLMv2 с контроллером домена.
10. Протокол аутентификации Kerberos, принцип работы, основные понятия.
11. Протокол аутентификации RADIUS, описание, роли, используемые в RADIUS, и их назначение.

Тема 6. Технологии межсетевых экранов.

1. Позволит ли межсетевой экран нового поколения повысить прозрачность и понимание трафика приложений в сети?
2. Можно ли сделать политику управления трафиком более гибкой, добавив дополнительные варианты действий, кроме разрешения и запрета?
3. Методы обхода межсетевого экрана.
4. Как классифицируются межсетевые экраны?
5. Какие существуют требования к МЭ?
6. Основные возможности и схемы развертывания межсетевого экрана.
7. Достоинства и недостатки межсетевого экрана.
8. Построение правил фильтрации.
9. Дополнительные функции межсетевых экранов. Функция DMZ. Функция Zone-Defense. Transparent mode.
10. Методы сетевой трансляции адресов (NAT).
11. Какие бывают шлюзы уровня приложений.
12. Программные и аппаратные МЭ. Задачи межсетевых экранов.

Тема 7. Технологии защиты от вирусов.

1. Основные методы предотвращения и обнаружения вторжений.
2. Характеристика системы обнаружения вторжений (СОВ).
3. Назначение и возможности средств обнаружения вторжений на хосты, протоколы и сетевые службы.
4. Место и роль средств обнаружения вторжений в общей системе обеспечения сетевой безопасности.
5. Классификация СОВ.
6. Выявление атак на основе сигнатур атак и выявления аномалий.
7. Аудит прикладных служб.
8. Средства обнаружения уязвимостей сетевых служб.
9. Системы виртуальных ловушек (Honey Pot и Padded Cell).
10. Основные способы противодействия вторжениям.

Тема 8. Требования к системам защиты информации.

1. Перечислите требования, предъявляемые к системам защиты информации.
2. Основные методы защиты от атак на сетевую инфраструктуру.
3. Перечислите основные методы и средства обеспечения защиты информации.
4. Что включают в себя организационные средства обеспечения защиты информации?
5. Что включают в себя правовые средства обеспечения защиты информации?
6. Характеристика технических мер защиты от сетевых атак.

7. Что включают в себя инженерно-технические средства защиты информации?

8. Дайте определение термина «информационная война».

9. Что включают в себя программно-аппаратные средства защиты информации?

10. Руководящий документ «Классификация автоматизированных систем.

Тема 9. Основы правового обеспечения защиты информации.

1. Стандарт PCI DSS, назначение, область применения, основные требования. ФСТЭК России, описание, основные функции.

2. Сформулируйте основные понятия в области государственной тайны.

3. Назовите основные составляющие государственной тайны.

4. Какие сведения не подлежат отнесению к государственной тайне и засекречиванию?

5. Назовите органы защиты государственной тайны.

6. Назовите основные нормативные руководящие документы, касающиеся государственной тайны.

7. Какие существуют нормативно-справочные документы и нормативно правовые акты в области защиты информации?

8. Охарактеризуйте правовые документы в сфере обеспечения информационной безопасности.

9. Назовите цели информационной безопасности государства.

10. Дайте характеристику основным задачам обеспечения информационной безопасности государства.

11. Сформулируйте принципы правового регулирования отношений, возникающих в сфере информации, информационных технологий и защиты информации.

12. Какой перечень действий предусматривает государственное регулирование в сфере применения информационных технологий?

Критерии оценки:

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

0,5 балла выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ К ЛАБОРАТОРНЫМ РАБОТАМ

Контрольные вопросы к лабораторной работе №1

1. Что такое политика информационной безопасности?
2. Какие организационные меры защиты существуют?
3. Назначение организационных мер?
4. Какие из них наиболее эффективны? Почему?
5. Перечислите основные нормативные документы, регламентирующие
6. Информационная безопасность в России – её классификация.
7. Какой состав и организационная структура системы обеспечения информационной безопасности?
8. В чем заключается стандарт ISO 17799?
9. Опишите методику анализа рисков.

Контрольные вопросы к лабораторной работе №2

1. Где необходима электронная подпись документов?
2. Какие могут быть альтернативные наборы вариантов решения?
3. Какой перечень документов, по которым готовился?
4. Атаки на реализации сетевых протоколов, отдельные узлы и службы.
5. Стадии проведения сетевой атаки.
6. Основные механизмы проведения сетевых атак на различных уровнях.
7. Федеральные законы РФ в сфере ИБ. Описание, основные положения.
8. Модели ISO/OSI.
9. Проблемы обеспечения конфиденциальности, целостности и доступности информации на различных уровнях модели ISO/OSI.

Контрольные вопросы к лабораторной работе №3

1. Какие функции выполняет СЗИ предприятия для решения задач защиты информации?

2. Как строится структура полномасштабной системы обеспечения
3. безопасности и защиты информации предприятия?
4. Какова специфика организации и выполнения охранных функций?
5. Каковы суть и содержание нормативной основы организации ЗСИ?
6. Какие факторы влияют на формирование организационно-правового
7. обеспечения защиты информации?
8. Какова структура организационно-правовой основы защиты информации?
9. Опишите организационно-правовые мероприятия по защите конфиденциальной информации.

Критерии оценки:

4-5 баллов (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

2-3 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

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

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

1.3 КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРАКТИЧЕСКИМ РАБОТАМ

Контрольные вопросы к практической работе №1

1. Какие части документа относятся к вопросам защиты информации?
2. Что такое CISQ?
3. Что показывают комментарии к данному документу?
4. Как менялся текст нормативного акта с момента его создания по настоящее время?
5. Анализ методик и технологий управления рисками.
6. Раскройте качественные методики управления рисками.
7. Какие количественные методики управления рисками вы знаете?
8. Опишите метод CRAMM.
9. Раскройте важность и сложность проблемы информационной безопасности.
10. Задачи комитета технической безопасности ETSI.

Контрольные вопросы к практической работе №2

1. В чем заключается сложность функционального построения системы защиты объекта информатизации? Приведите примеры.
2. Приведите формулу для вычисления величины Ротки), прокомментируйте ее.
3. Приведите примеры многозвенной системы защиты объекта информатизации.
4. Прокомментируйте выражение для определения прочности многозвенной защиты при противостоянии одному нарушителю.
5. Прокомментируйте выражение для определения прочности многозвенной защиты при противостоянии нескольким нарушителю.
6. Какие выводы можно сделать, если прочность слабейшего звена защиты удовлетворяет предъявленным требованиям оболочки защиты в целом?
7. Какие меры повышения прочности защиты можно порекомендовать, если звено защиты не удовлетворяет предъявленным требованиям?
8. Каким образом система будет способствовать целям бизнеса?
9. Требует ли разработка системы технологии, которая до этого не использовалась в организации?
10. Что должен включать отчет по результатам оценки CASE-средств?
11. Какие этапы оценки вы знаете?
12. Опишите рамки информационной безопасности NIST (NIST CSF).

Контрольные вопросы к практической работе №3

1. Сколько поколения CASE-средств существует? Опишите их.
2. Какие требования предъявляются к CASE-средствам?
3. Какие направления развития CASE-средств используются наиболее интенсивно?
4. По каким критериям оценивается CASE-средство для UML?
5. Как делятся CASE-средства по функциональному назначению?
6. Опишите архитектуру CASE-средств.
7. Опишите виды классификации CASE-средств.
8. Охарактеризуйте критерии выбора CASE-средств.
9. Какие текущие проблемы существуют в организации и как новая система поможет их решить?
10. Опишите этапы программы оценки соответствия ИБ.

Контрольные вопросы к практической работе №4

1. Как проводится сертификация средств защиты информации?
2. Что показывают характеристики данного средства защиты?
3. Какой регулятор контролирует данную область информационной безопасности?
4. Проекты международных стандартов по облачным вычислениям.
5. Опишите стандарты и руководства США.
6. Общая картина введенных в действие и ожидаемых в ближайшее время стандартов и руководств в области облачных вычислений.
7. Российская стандартизация облачных вычислений и ее проблемы и пути решения.
8. Что произойдет с организацией, если система не будет введена в эксплуатацию?
9. Какая основная информация содержится в сертификате?

Критерии оценки:

5-6 баллов (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

3-4 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе;

допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

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

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

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 ТЕМЫ КУРСОВЫХ РАБОТ

1. Современные DDoS-атаки как угроза для бизнеса в Интернете: методы и средства защиты.
2. Особенности оценки экономической эффективности системы защиты информации в организации .
3. Проектирование защищенной информационной системы для предприятий нефтегазовой отрасли.
4. Проектирование защищенной информационной системы для органов местного самоуправления.
5. Проектирование защищенной информационной системы для предприятий банковской сферы.
6. Проектирование защищенной информационной системы для муниципальных предприятий.
7. Проектирование защищенной информационной системы для машиностроительной отрасли.

8. Технические методы разграничения доступа в компьютерных системах и их правовая регламентация.
9. Проектирование защищенной информационной системы для энергетической отрасли.
10. Проектирование защищенной информационной системы для военизированной отрасли.
11. Проектирование защищенной информационной системы для строительной отрасли.
12. Проектирование защищенной информационной системы для металлургической отрасли.
13. Проектирование защищенной информационной системы для жилищно-коммунального хозяйства.
14. Разработка модели угроз образовательного учреждения.
15. Разработка модели угроз образовательного учреждения.
16. Разработка модели угроз медицинского учреждения.
17. Разработка модели угроз муниципального учреждения.
18. Разработка модели угроз коммерческой организации.
19. Разработка модели угроз банка.
20. Аудит безопасности информационной системы с использованием теста на проникновение.
21. Структурирование массива событий и инцидентов информационной безопасности с использованием специализированного ПО.
22. Правовые аспекты применения усиленной неквалифицированной электронной подписи.
23. Правовые основы деятельности Роскомнадзора в контроле Интернета
24. Регулирование деятельности с применением криптографии в России.
25. Технические методы разграничения доступа в компьютерных системах и их правовая регламентация.
26. Где и как нужно и можно применять шифрование информации
27. Место DLP-систем в современной структуре обеспечения ИБ АИС.

28. Современные тенденции развития отечественных средств электронной подписи.
29. Система шифрования (RSA).
30. Система шифрования (скремблер).
31. Верификатор решения задач.
32. Система тестирования.
33. Проблемы ИБ инфраструктуры ЦОД большой территориально распределенной АИС.
34. Анализ подходов к ролевому управлению доступом.
35. Современные проблемы авторизации субъекта доступа.

Шкала оценивания курсовых работ (или курсовых проектов): 100-балльная.

Критерии оценивания:

85-100 баллов (или оценка «отлично») выставляется обучающемуся, если тема курсовой работы раскрыта полно и глубоко, при этом убедительно и аргументированно изложена собственная позиция автора по рассматриваемому вопросу; курсовая работа демонстрирует способность автора к сопоставлению, анализу и обобщению; структура курсовой работы четкая и логичная; изучено большое количество актуальных источников, включая дополнительные источники, корректно сделаны ссылки на источники; самостоятельно подобраны убедительные примеры; основные положения доказаны; сделан обоснованный и убедительный вывод; сформулированы мотивированные рекомендации; выполнены требования к оформлению курсовой работы.

70-84 баллов (или оценка «хорошо») выставляется обучающемуся, если тема курсовой работы раскрыта, сделана попытка самостоятельного осмысления темы; структура курсовой работы логична; изучены основные источники, правильно оформлены ссылки на источники; приведены уместные примеры; основные положения и вывод носят доказательный характер; сделаны рекомендации; имеются незначительные погрешности в содержании и (или) оформлении курсовой работы.

50-69 баллов (или оценка «удовлетворительно») выставляется обучающемуся, если тема курсовой работы раскрыта неполно и (или) в изложении темы имеются недочеты и ошибки; отмечаются отступления от рекомендованной структуры курсовой работы; количество изученных источников менее рекомендуемого, сделаны ссылки на источники; приведены самые общие примеры или недостаточное их количество; вывод сделан, но имеет признаки неполноты и неточности; рекомендации носят

формальный характер; имеются недочеты в содержании и (или) оформлении курсовой работы.

0-49 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если тема курсовой работы не раскрыта и (или) в изложении темы имеются грубые ошибки; структура курсовой работы нечеткая или не определяется вообще; количество изученных источников значительно менее рекомендуемого, неправильно сделаны ссылки на источники или они отсутствуют; не приведены примеры или приведены неверные примеры; отсутствует вывод или автор испытывает затруднения с выводами; не соблюдаются требования к оформлению курсовой работы.

2.2 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1. Какой из перечисленных методов оценки риска основан на расчетах и анализе статистических показателей?
   1) Вероятностный метод
   2) Метод сценариев
   3) Учет рисков при расчете чистой приведенной стоимости
   4) Анализ чувствительности

2. Какой из перечисленных методов оценки риска дает представление о наиболее критических факторах инвестиционного проекта?
   1) Построение дерева решений
   2) Метод сценариев
   3) Учет рисков при расчете чистой приведенной стоимости
   4) Анализ чувствительности

3. Какой из перечисленных методов оценки риска используется в ситуациях, когда принимаемые решения сильно зависят от принятых ранее и определяют сценарии дальнейшего развития событий?
   1) Имитационное моделирование
   2) Вероятностный метод
   3) Учет рисков при расчете чистой приведенной стоимости
   4) Построение дерева решений

4. Каким образом при расчете чистой приведенной стоимости можно учитывать риск?
   1) В знаменателе формулы NPV посредством корректировки ставки дисконта
   2) Комбинация формул NPV посредством корректировки чистых денежных потоков

3) В числителе формулы NPV посредством корректировки чистых денежных поток
4) Все варианты верны

5. Какой из перечисленных методов оценки риска используется в ситуациях, когда принимаемые решения сильно зависят от принятых ранее и определяют сценарии дальнейшего развития событий?
1) Имитационное моделирование
2) Вероятностный метод
3) Учет рисков при расчете чистой приведенной стоимости
4) Анализ чувствительности
5) Построение дерева решений

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

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

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

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

10. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?

1) NIST и OCTAVE являются корпоративными
2) NIST и OCTAVE ориентирован на ИТ
3) AS/NZS ориентирован на ИТ
4) NIST и AS/NZS являются корпоративными

11. Как называют протокол IPX, переносящий данные в интрасеть филиалов предприятия?

1) Протокол-пассажир
2) Несущий протокол
3) Протокол туннелирования

12. Что, из перечисленного, понимается под термином частная виртуальная сеть?

1) Шифрованный туннель внутри обычной сети.
2) Локальная сеть в здании.
3) Программный комплекс для шифрования.

13. Одна из причин, по которой коммутаторы не должны использоваться для предоставления каких-либо возможностей межсетевого экрана

1) Коммутаторы не могут видеть передаваемый трафик.
2) Коммутаторы не могут предотвращать возможные DoS-атаки.
3) Коммутаторы не могут видеть порт, на который ушел пакет.
4) Коммутаторы не могут видеть порт, на который пришел пакет.

14. Основное свойство коммутаторов (выберите самое точное определение, один ответ)

1) Коммутаторы передают пакеты только нужному адресату.
2) Коммутаторы могут фильтровать трафик в зависимости от интерфейса, с которого ушел пакет.
3) Коммутаторы могут фильтровать трафик в зависимости от интерфейса, на который пришел пакет.
4) Коммутаторы могут фильтровать трафик в зависимости от типа трафика.

15. Политика безопасности – это (выберите самое точное определение, один ответ)

1) Совокупность административных мер, которые определяют порядок прохода в компьютерные классы.
2) Межсетевые экраны, используемые в организации.
3) Множество критериев для предоставления сервисов безопасности.
4) Совокупность как административных мер, так и множества критериев для предоставления сервисов безопасности.

16. Основные классы атак на передаваемые по сети данные

1) Удаленная и локальная.
2) Видимая и невидимая.
3) Активная и пассивная.
4) Внешняя и внутренняя.

17. Атака называется пассивной, если
1) Оппонент не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения.
2) Оппонент не предполагает проникновение в систему.
3) Оппонент не использует никаких инструментальных средств для выполнения атаки.
4) Оппонент не анализирует перехваченные сообщения.

18. Что не относится к replay-атаке
1) Изменение передаваемых данных.
2) Выполнение незаконного проникновения в систему.
3) Просмотр передаваемых данных.
4) Повторное использование нарушителем перехваченного ранее сообщения.

19. Невозможность получения сервиса законным пользователем называется
1) Атакой «man-in-the-middle».
2) Replay-атакой.
3) DoS-атакой.
4) Пассивной атакой.

20. При анализе производительности межсетевого экрана следует определить
1) Какое количество портов существует на выбранном экземпляре межсетевого экрана.
2) Возможна ли балансировка нагрузки и резервирование для гарантирования высокой отказоустойчивости.
3) Какую пропускную способность, максимальное количество одновременно открытых соединений, соединений в секунду может обеспечивать межсетевой экран.
4) Что является более предпочтительным – аппаратный или программный межсетевой экран.

21. Под безопасностью информационной системы понимается
1) Защита от неавторизованного доступа или модификации информации во время хранения, обработки или пересылки.
2) Отсутствие выхода в интернет.
3) Меры, необходимые для определения, документирования и учета угроз.
4) Защита от отказа в обслуживании законных пользователей.

22. Что не относится к понятию «оборона в глубину»

1) Использование нескольких взаимосвязанных между собой технологий.
2) Использование нескольких коммутаторов.
3) Использование нескольких межсетевых экранов.
4) Использование аппаратных средств разных производителей.

23. Риск — это
1) Вероятность того, что в системе остались неизвестные уязвимости.
2) Вероятность того, что конкретная атака будет осуществлена с использованием конкретной уязвимости.
3) Невозможность ликвидировать все уязвимости в информационной системе.
4) Невозможность исправить все ошибки в программном обеспечении.

24. Возможные стратегии управления рисками
1) Избежать риск.
2) Принять риск.
3) Уменьшить риск.
4) Передать риск.

25. Целостность – это
1) Невозможность несанкционированного доступа к информации.
2) Невозможность несанкционированного выполнения программ.
3) Невозможность несанкционированного изменения информации.

26. Невозможность несанкционированного просмотра информации.
Сервис, который обеспечивает невозможность несанкционированного изменения данных, называется
1) Конфиденциальностью.
2) Целостностью.
3) Аутентификацией.
4) Доступностью.

27. Многофакторная аутентификация означает
1) Аутентификация не может выполняться с помощью пароля.
2) Аутентификация должна выполняться с использованием смарт-карты.
3) Аутентифицируемой стороне необходимо предоставить несколько параметров, чтобы установить требуемый уровень доверия.
4) Аутентификация должна выполняться третьей доверенной стороной.

28. Гибкость технологии VLAN означает
1) VLAN обеспечивает эффективный способ аутентификации пользователей.
2) VLAN являются эффективным способом группирования пользователей и компьютеров в виртуальные рабочие группы, независимо от их физического расположения в сети.

3) VLAN являются эффективным способом групповой аутентификации пользователей.
4) VLAN обеспечивает эффективный способ шифрования трафика.

29. Если к маршрутизатору подключены коммутаторы или другие устройства (например, рабочие станции пользователей), не поддерживающие технологию VLAN
    1) На маршрутизаторе можно выполнить сегментацию на требуемое число виртуальных локальных сетей.
    2) На маршрутизаторе можно создать только две VLAN.
    3) На маршрутизаторе можно создать только одну VLAN.
    4) На маршрутизаторе нельзя выполнить сегментацию на виртуальные локальные сети.

30. VLAN-трафик называется
    1) Маркированным (tagged).
    2) Отброшенным (dropped).
    3) Туннелированным (tunneled).
    4) Отфильтрованным (filtered).

31. Технология VLAN описана в стандарте
    1) IEEE 802.3.
    2) IEEE 802.1Q.
    3) RFC 2401.
    4) ISO 9000.

32. Технология VLAN обладает следующими характеристиками
    1) Увеличение пропускной способности сети.
    2) Аутентификация на канальном уровне.
    3) Целостность на канальном уровне.
    4) Целостность некоторой последовательности дейтаграмм.

33. Широковещательные пакеты передаются
    1) Всем хостам в сети, определяемой маской подсети.
    2) Всем хостам сети, подключенным к lan-интерфейсам.
    3) Всем хостам сети, которые доступны со всех интерфейсов маршрутизатора.
    4) Всем хостам сети, подключенным ко всем интерфейсам маршрутизатора или коммутатора.

34. Технология VLAN обладает следующими характеристиками
    1) Гибкость, связанная с возможностью группирования пользователей в виртуальные рабочие группы.
    2) Шифрование трафика.
    3) Аутентификация на уровне пользователя.
    4) Повышение безопасности, связанное с уменьшением широковещательного домена.

35. Состояние TCP-соединения LISTEN

1) Состояние сервера после отправления клиенту пакета с флагами SYN, ACK.
2) Состояние сервера после получения от клиента пакета с установленными флагами SYN, ACK.
3) Состояние сервера, в котором он ожидает запрос от клиента на создание соединения.
4) Состояние сервера после получения от клиента пакета с установленным флагом SYN.

36. Анализ состояния в пакетном фильтре означает
1) Отслеживание состояния соединения и оповещение администратора о наличии пакета, который не соответствует ожидаемому.
2) Отслеживание состояния соединения и отбрасывание пакетов, которые не соответствуют ожидаемому.
3) Отслеживание состояния соединения и запрещение всего трафика, если обнаружен пакет, который не соответствует ожидаемому.
4) Отслеживание состояния соединения и вставка собственных пакетов, если обнаружен пакет, который не соответствует ожидаемому.

37. Прикладной уровень модели OSI
1) Посылает и получает данные конкретных приложений.
2) Выполняет фрагментацию/ дефрагментацию пакетов.
3) Выполняет шифрование трафика.
4) Обеспечивает маршрутизацию между локальными сетями.

38. Транспортный уровень модели OSI
1) Некоторые протоколы данного уровня гарантируют надежность соединения.
2) Все протоколы данного уровня гарантируют надежность соединения.
3) Предоставляет сервисы, ориентированные на соединение.
4) Некоторые протоколы данного уровня обеспечивают целостность соединения.

39. Адреса канального уровня называются
1) MAC-адресами.
2) Веб-именами.
3) IP-адресами.
4) DNS-именами.

40. Пакетные фильтры с поддержкой состояния
1) Анализирует правильную последовательность пакетов на транспортном уровне.
2) Анализируют состояние защищаемой локальной сети.
3) Анализируют состояние межсетевого экрана.
4) Анализирует правильную последовательность пакетов на прикладном уровне.

41. Сокетом называется
    1) Пара (MAC-адрес, IP-адрес).
    2) Пара (IP-адрес, порт).
    3) Пара (DNS-имя, IP-адрес).
    4) Пара (DNS-имя, порт).

42. Инициализация TCP-соединения выполняется
    1) Сервером.
    2) Клиентом.
    3) Третьей доверенной стороной.
    4) Администратором.

43. При установлении TCP-соединения
    1) Клиент посылает пакет ClientHello.
    2) Клиент посылает пакет с установленными битами SYN, ACK.
    3) Клиент посылает пакет с установленным битом Start.
    4) Клиент посылает пакет с установленным битом SYN.

44. Межсетевые экраны для веб-приложений располагают
    1) Перед защищаемым веб-сервером (трафик вначале передается межсетевому экрану, затем веб-серверу).
    2) Межсетевой экран и защищаемый им веб-сервер находятся в разных подсетях, но трафик между ними не запрещен.
    3) После защищаемого веб-сервера (трафик вначале передается веб-серверу, затем межсетевому экрану).
    4) Межсетевой экран и защищаемый им веб-сервер находятся в разных подсетях, трафик между ними запрещен.

45. Отличия выделенного прокси-сервера от прикладных прокси-шлюзов
    1) Выделенные прокси-сервера обладают меньшей производительностью.
    2) Выделенные прокси-сервера не могут выполнять аутентификацию пользователей.
    3) Выделенные прокси-сервера не могут анализировать заголовки транспортного уровня.
    4) Выделенные прокси-сервера имеют более ограниченные возможности межсетевого экранирования.

46. Недостатки межсетевых экранов прикладного уровня
    1) Производительность межсетевого экрана прикладного уровня ниже, чем у пакетного фильтра.
    2) Межсетевой экран прикладного уровня не может анализировать заголовки транспортного и сетевого уровней.
    3) Межсетевой экран прикладного уровня обеспечивает меньший уровень безопасности, чем пакетный фильтр.
    4) Межсетевой экран прикладного уровня обязательно разрывает TCP-соединение.

47. Прокси-сервер не может быть

1) Исходящим.
2) Шифрующим.
3) Входящим.
4) Туннелирующим.

48. Персональные межсетевые экраны для настольных компьютеров и ноутбуков являются
1) Исключительно программными.
2) Аппаратно-программными средствами защиты.
3) Не могут быть встроенными в ОС, которую они защищают; всегда реализованы внешними производителями.
4) Всегда встроены в ОС, которую они защищают; не могут быть реализованы внешними производителями.

49. При использовании прокси-шлюзов прикладного уровня
1) Прокси-шлюз является абсолютно прозрачным для клиента.
2) Внешние IP-адреса не видны изнутри.
3) Внутренние IP-адреса не видны вовне.
4) Прокси-шлюз изменяет IP-адрес источника на свой IP-адрес.

50. Недостатки использования системы унифицированного управления угрозами
1) Может существенно усложниться управление всеми устройствами.
2) Может существенно ухудшиться производительность, если системе унифицированного управления угрозами не будет хватать ресурсов.
3) Может существенно возрасти нагрузка на рабочие станции пользователей.
4) Может существенно возрасти нагрузка на прикладные сервера.

51. Ограниченность анализа межсетевого экрана
1) Не может выполнять аутентификацию пользователя.
2) Не может анализировать зашифрованные прикладные данные.
3) Не может анализировать данные прикладного уровня.
4) Не может отбрасывать пакеты.

52. Межсетевые экраны прикладного уровня могут
1) Выполнять авторизацию пользователя.
2) Автоматически распознавать новые протоколы.
3) Выполнять аутентификацию пользователя.
4) Шифровать данные пользователя.

53. Прокси-шлюзы прикладного уровня (выберите самое точное определение, один ответ)
1) Имеют базу данных пользователей, которым разрешен доступ к защищаемому ресурсу.
2) Имеют прокси-агента, являющегося посредником между клиентом и сервером.
3) Имеют базу данных IP-адресов, с которых разрешен доступ к защищаемому ресурсу.
4) Не разрывают TCP-соединение.

54. Персональные межсетевые экраны для настольных компьютеров и ноутбуков устанавливаются
    1) На маршрутизаторах, которые указаны на хосте в качестве шлюза по умолчанию.
    2) На конечных точках VPN.
    3) На отдельных компьютерах.
    4) На хостах, которые они защищают.

55. Выделенные прокси-серверы предназначены для того, чтобы обрабатывать трафик
    1) Конкретного пользователя.
    2) Конкретного уровня модели OSI.
    3) Конкретного адреса отправителя.
    4) Конкретного прикладного протокола.

56. Технология UPnP, которая позволяет приложению, установленному на компьютере за межсетевым экраном, автоматически запрашивать у межсетевого экрана открытие определенных портов
    1) По умолчанию должна быть разрешена.
    2) Должна быть всегда установлена на компьютере, не должно быть возможности ее запретить.
    3) По умолчанию должна быть запрещена.
    4) Не должна использоваться ни в каком случае.

57. Входящий трафик, IP-адресом получателя в котором является сам межсетевой экран
    1) Должен блокироваться, если только межсетевой экран не предоставляет сервисы для входящего трафика, которые требуют прямого соединения.
    2) Должен всегда блокироваться.
    3) Должен всегда разрешаться.
    4) Должен разрешаться, если в локальной сети расположены сервера, доступ к которым необходим извне.

58. Определение экстранет
    1) Сеть, логически состоящая из трех частей: две интранет соединены между собой через интернет с использованием VPN.
    2) Сеть, логически состоящая из двух локальных сетей, между которыми установлен межсетевой экран.
    3) Сеть, логически состоящая из локальной сети, имеющей выход в интернет через межсетевой экран прикладного уровня.
    4) Сеть, логически состоящая из локальной сети, имеющей выход в интернет через пакетный фильтр.

59. Примеры IP-адресов, которые не должны появляться в пакетах
    1) 192.168.254.0
    2) 0.0.0.0
    3) с 127.0.0.0 по 127.255.255.255
    4) 192.168.0.254

60. Использование GRE-туннеля для соединения двух локальных сетей через магистральную сеть
    1) Если необходимо доставить пакет из тупикового сегмента X в тупиковый сегмент Y, то маршрутизатор NAT для сегмента X инкапсулирует пакет в IP-заголовок с IP-адресом получателя, установленным в IP-адрес хоста в сегменте Y.
    2) Если необходимо доставить пакет из тупикового сегмента X в тупиковый сегмент Y, то маршрутизатор NAT для сегмента X никак не преобразует пакет.
    3) Если необходимо доставить пакет из тупикового сегмента X в тупиковый сегмент Y, то маршрутизатор NAT для сегмента X инкапсулирует пакет в IP-заголовок с IP-адресом получателя, установленным в глобальный IP-адрес устройства, выполняющего NAT для сегмента Y.
    4) Использование NAT вместе с GRE-туннелем невозможно.

61. Маршрутизатор NAT
    1) Расположен на границе между двумя областями адресов и преобразует адреса в IP-заголовках таким образом, что пакет корректно маршрутизируется при переходе из одной области в другую.
    2) Расположен на границе между двумя локальными сетями с разными требованиями к безопасности.
    3) Расположен на границе между локальной сетью и интернетом.
    4) Расположен на границе между двумя областями адресов, в одной из которых адреса принадлежат частной сети, а в другой – внешней.

62. Отличия двойного NAT от традиционного и двунаправленного NAT
    1) В двойном NAT IP-адреса не изменяются при пересечении дейтаграммой границы пространства адресов.
    2) В двойном NAT изменяются только адреса из внешней сети при пересечении дейтаграммой границы пространства адресов.
    3) В двойном NAT IP-адреса как источника, так и получателя модифицируются NAT при пересечении дейтаграммой границы пространства адресов.
    4) В двойном NAT изменяются только адреса из частной сети при пересечении дейтаграммой границы пространства адресов.

63. NAT используется
    1) В IPv32.
    2) В IPv64.
    3) В IPv6.
    4) В IPv4.

Задания в открытой форме

1) … - самый ценный ресурс в компании, а в некоторых случаях является и производственным ресурсом, от сохранности которого зависят важные технологические процессы.
2) … – это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.
3) … — это комплекс мероприятий, направленных на обеспечение информационной безопасности.
4) … защиты информации является информационная система (предприятия, коммерческой организации) или автоматизированная система обработки данных.
5) … система — взаимосвязанная совокупность средств, методов и персонала, которые используются для хранения, обработки, передачи и получения информации в интересах достижения поставленной цели.
6) … информации в ИС – это такое состояние всех компонент информационной системы, при котором обеспечивается защита информации от возможных угроз на требуемом уровне.
7) Под … в ИС понимается единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в ИС в соответствии с принятой политикой безопасности.
8) Цель …. – обеспечить бесперебойную работу организации и свести к минимуму ущерб от событий, таящих угрозу безопасности, посредством их предотвращения и сведения последствий к минимуму.
9) … — это защита от несанкционированного доступа к информации
10) Под .. информации подразумевается, ее защищенность от разрушения и несанкционированного изменения.
11) … — это возможность за приемлемое время получить требуемую информационную услугу.
12) … можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)).
13) … — законы и нормативны акты, затрагивающие ОО;
14) … — положения политик безопасности, затрагивающих ОО и учитывающих его особенности;
15) … — меры физической защиты, персонал и его специфика;
16) … — назначение ОО, предполагаемые области его применения.
17) … — типовой набор требований для некоторой категории ОО.
18) … — документ, содержащий требования безопасности для конкретной разработки, выполнение которых обеспечивает достижение поставленных целей безопасности.

19) … – любой контейнер, предназначенный для хранения информации, подверженный угрозам информационной безопасности (сервер, рабочая станция, переносной компьютер).
20) … – действие, которое потенциально может привести к нарушению безопасности
21) … – это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы.
22) …– ущерб, который понесет компания от потери ресурса
23) … – степень влияния реализации угрозы на ресурс, т.е. как сильно реализация угрозы повлияет на работу ресурса.

Задание на установление соответствия

1. Установить соответствие этапов CRAMM:

1) «Identification and Valuation of Assets»	a) — идентифицируются и оцениваются угрозы и уязвимости информационных активов компании.
2) «Threat and Vulnerability Assessment»	b) — четко идентифицируются активы, и определяется их стоимость. Расчет стоимости информационных активов однозначно позволяет определить необходимость и достаточность предлагаемых средств контроля и защиты.
3) «Risk Analysis»	c) — предлагаются меры и средства уменьшения или уклонения от риска.
4) «Risk management»	d) — позволяет получить качественные и количественные оценки рисков.

2. Установить соответствие ущерба репутации организации:

1) 2	a) — критика в средствах массовой информации, имеющая последствия в виде крупных скандалов, парламентских слушаний, широкомасштабных проверок и т. п.;
2) 4	b) — негативная реакция отдельных депутатов;
3) 6	c) — негативная реакция отдельных чиновников, общественных деятелей;
4) 8	d) — критика в средствах массовой информации, не имеющая широкого общественного резонанса;

5) 10	e) — негативная реакция на уровне Президента и Правительства.

3. Установить соответствие ущерба здоровью персонала:

1) 2	a) — ущерб среднего размера (необходимо лечение для одного или нескольких сотрудников, но длительных отрицательных последствий нет);
2) 4	b) — минимальный ущерб (последствия не связаны с госпитализаций или длительным лечением);
3) 6	c) — гибель людей.
4) 10	d) — серьезные последствия (длительная госпитализация, инвалидность одного или нескольких сотрудников);

4. Установить соответствие финансовых потерь, связанных с восстановлением ресурсов:

1) 2	a) — от $1000 до $10 000;
2) 4	b) — менее $1000;
3) 6	c) — от $10 000 до $100 000;
4) 10	d) — свыше $100 000.

5. Установить соответствие дезорганизации деятельности в связи с недоступностью данных::

1) 2	a) — отсутствие доступа к информации до 1 часа;
2) 4	b) — отсутствие доступа к информации до 15 минут;
3) 6	c) — отсутствие доступа к информации от 12 часов;
4) 8	d) — отсутствие доступа к информации до 3 часов;
5) 10	e) — отсутствие доступа к информации более суток.

6. Установить соответствие оценки уровня угрозы:

1) Очень высокий	a) Инцидент происходит в среднем, не

	чаще, чем каждые 10 лет
2) Высокий	b) Инцидент происходит в среднем один раз в 3 года
3) Средний	c) Инцидент происходит в среднем раз в год
4) Низкий	d) Инцидент происходит в среднем один раз в четыре месяца
5) Очень низкий	e) Инцидент происходит в среднем раз в месяц

7. Установить соответствие оценки рисков в зависимости от факторов:

1) Высокий риск	a) Предполагается, что без снижения таких рисков обращение к информационной системе предприятия может оказать отрицательное влияние на бизнес;
2) Существенный риск	b) Здесь требуется эффективная стратегия управления рисками, которая позволит уменьшить или полностью исключить отрицательные последствия нападения;
3) Умеренный риск	c) Усилия по управлению рисками в данном случае не будут играть важной роли.
4) Незначительный риск	d) В отношении рисков, попавших в эту область, достаточно применить основные процедуры управления рисками;

8. Установить соответствие:

1) Угроза безопасности	a) Это некая неудачная характеристика системы, которая делает возможным возникновение угрозы.
2) Уязвимость	b) Это угроза раскрытия информации.
3) Атака	c) Это потенциально возможное происшествие, которое может оказать воздействие на информацию в системе.
4) Угроза конфиденциальности	d) Это действие по использованию уязвимости; реализация угрозы.

9. Установить соответствие:

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

10. Установить соответствие:

1) High-severity vulnerabilities	a) Список уязвимостей, которые надо устранить в ближайшее время
2) Middle-severity vulnerabilities	b) Список уязвимостей, в отношении которых не требуется немедленных действий
3) Low-severity vulnerabilities	c) Список уязвимостей, которые надо устранить немедленно оборудования

11. Установить соответствие:

1) Командный интерфейс	a) Движения
2) SILK	b) Последовательности символов
3) WIMP	c) Манипулятор

12. Установить соответствие этапов RiskWatch:

1) Первый этап	a) ввод данных, описывающих конкретные характеристики системы.

2) Второй этап	b) Определение предмета исследования.
3) Третий этап	c) Генерация отчетов.
4) Четвертый этап	d) Количественная оценка риска

13. Установить соответствие:

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

14. Установить соответствие:

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

	доступ к внутренним службам этих приложений

15. Установить соответствие:

1) Режим государственной границы	a) Совокупность правил въезда (прохода), временного пребывания лиц и транспортных средств в пограничной полосе; осуществление в ее пределах хозяйственной, промысловой и тон деятельности; проведение массовых общественно-политических, культурных и других мероприятий
2) Пограничный режим	b) Совокупность правил, устанавливающих порядок ее содержания, пересечения гражданами и транспортными средствами; перемещения через границу товаров и животных; ведения на ней хозяйственной, промысловой и иной деятельности;
3) Пограничная полоса	c) Часть территории российской федерации, непосредственно прилегающей к государственной границе на всем ее протяжении.

16. Установить соответствие:

1) Линейная структура процесса вычислений	a) Предполагает, что для получения результата некоторые действия необходимо выполнить несколько раз.
2) Разветвленная структура процесса вычислений	b) Предполагает, что конкретная последовательность операций зависит от значений одной или нескольких переменных.
3) Циклическая структура процесса вычислений	c) Предполагает, что для получения результата необходимо выполнить некоторые операции в определенной последовательности.

17. Установить соответствие:

1) Правильность	a) Возможность проверки получаемых результатов;
2) Универсальность	b) Обеспечение полной повторяемости результатов, т. Е. Обеспечение их правильности при наличии различного рода сбоев;
3) Надежность	c) Обеспечение правильной работы при любых допустимых данных и защиты от неправильных данных;
4) Проверяемость	d) Функционирование в соответствии с техническим заданием;

18. Установить соответствие:

1) Точность результатов	a) Возможность совместного функционирования с некоторым оборудованием
2) Защищенность	b) Возможность совместного функционирования с другим программным обеспечением
3) Программная совместимость	c) Обеспечение конфиденциальности инф ормации;
4) Аппаратная совместимость	d) Обеспечение погрешности результатов не выше заданной;

19. Установить соответствие:

1) Превентивные	a) Меры безопасности, направленные на обнаружение инцидентов. Например, антивирусная защита или система обнаружения вторжений.
2) Восстановительные	b) Меры безопасности, которые предотвращают появление инцидента информационной безопасности. Например, распределение прав доступа.
3) Обнаруживающие	c) Меры безопасности, направленные на уменьшение потенциального ущерба в случае инцидента. Например,

	резервное копирование.
4) Подавляющие	d) Меры безопасности, направленные на восстановления после инцидента. Например, восстановление резервных копий, откат на предыдущее рабочее состояние и т.п.
5) Корректирующие	e) Меры безопасности, которые противодействуют попыткам реализации угрозы, то есть инцидентам.

20. Установить соответствие:

1. Сертификат ключа подписи	a) Документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.
2. Сертификат средств электронной цифровой подписи	b) Документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра.
3. Электронная цифровая подпись	c) Документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа
4. Открытый ключ электронной цифровой подписи	d) Уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Задание на установление правильной последовательности

1. Установить этапы системы управления:
   1) Планирование.
   2) внедрение.
   3) мониторинг и анализ.
   4) совершенствование.

2. Основные этапы разработки системы управления информационной безопасностью:
   1) обработка информационных рисков (в том числе определение конкретных мер для защиты ценных активов);
   2) контроль выполнения и эффективности выбранных мер.
   3) оценка защищенности информационной системы;
   4) оценка информационных рисков;
   5) инвентаризация активов;
   6) внедрение выбранных мер обработки рисков;
   7) категорирование активов;

3. Установить предпочтительную последовательность этапов внедрения межсетевого экрана:
   1) конфигурирование
   2) планирование
   3) тестирование
   4) развертывание
   5) управление

4. Установите основные этапы оценки риска:
   1) Сопоставление вероятности возникновения
   2) Определение контрмер
   3) Документирование
   4) Идентификация угроз
   5) Определение защищаемых активов

5. Установите фазы анализа OCTAVE:
   1) разработка профиля угроз, связанных с активом;
   2) идентификация инфраструктурных уязвимостей;
   3) разработка стратегии и планов безопасности.

6. Установите этапы PDCA:
   1) планирование
   2) проверка
   3) действие
   4) выполнение

7. Установите этапы этапы создания СУИБ:
    1) Внедрение и функционирование системы управления информационной безопасности.
    2) Проведение мониторинга и анализа системы управления информационной безопасности.
    3) Разработка системы управления информационной безопасности.
    4) Поддержка и улучшение системы управления информационной безопасности.

8. Установить этапы разработки:
    1) Проектирование
    2) Реализация
    3) Внедрение
    4) Анализ и планирование требований пользователей

9. Установить этапы разработки программной документации:
    1) Разработка технического проекта.
    2) Комплексное внедрение программной документации.
    3) Подготовка технического специального задания.
    4) Составление подробного эскизного варианта проекта.
    5) Оформление рабочего документа.

10. Установите этапы процесса управления рисками:
    1) Выбор анализируемых объектов и уровня детализации их рассмотрения.
    2) Инвентаризация активов.
    3) Анализ угроз и их последствий, выявление уязвимых мест в защите.
    4) Оценка рисков.
    5) Выбор методики оценки рисков.
11. Установите этапы процесса управления рисками:
    1) Реализация и проверка выбранных мер.
    2) Выбор защитных мер.
    3) Обработка рисков.
    4) Оценка остаточного риска.

12. Установите этапы стратегии управления рисками Microsoft:
    1) – определение допустимого уровня рисков (то есть того уровня рисков,
    2) который приемлем);
    3) – оценка вероятности возникновения каждого риска;
    4) – присвоение стоимости каждому риску;
    5) – расстановка приоритетов.

13. Выберите правильную последовательность этапов по созданию системы защиты персональных данных:
    1) Опытная и промышленная эксплуатация
    2) Проектный этап
    3) Аттестация или декларирование
    4) Предпроектный этап

14. Выберите правильную последовательность этапов разработки профиля защиты.
    1) Анализ среды применения ИТ-продукта с точки зрения
    2) безопасности.
    3) Выбор профиля-прототипа.
    4) Синтез требований.

15. Выберите правильную последовательность этапов защиты информации, информационных технологий и автоматизированных систем от атак:
    1) Анализ рисков для активов организации, включающий в себя выявление ценных активов и оценку возможных последствий реализации атак с использованием скрытых каналов
    2) Реализация защитных мер по противодействию скрытых каналов
    3) Организация контроля за противодействием скрытых каналов.
    4) Выявление скрытых каналов и оценка их опасности для активов организации

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

17. Выберите последовательность проведения моделирования угроз:
    1) Определение негативных последствий от угроз безопасности информации.
    2) Определение объектов воздействия угроз безопасности информации.
    3) Оценка возможности реализации угроз и их актуальности.

18. Установите этапы процессной модели:

1) Проверка.
2) Планирование.
3) Реализация
4) Действие.

19. Установите этапы методики анализа рисков Microsoft:
    1) Распознавание (идентификация) рисков.
    2) Определение размера риска.
    3) Разработка плана управления рисками.
    4) Текущий контроль и управление рисками.

20. Установите этапы процесса управления рисками в методике CRAMM:
    1) «Initiation».
    2) «Identification and Valuation of Assets».
    3) «Risk Analysis».
    4) «Threat and Vulnerability Assessment».

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

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

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

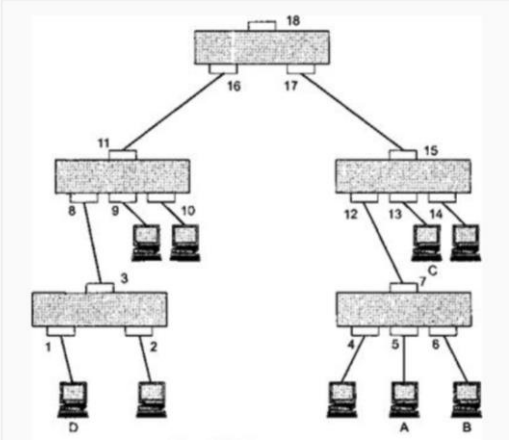
Общий балл по промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

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

2.2КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

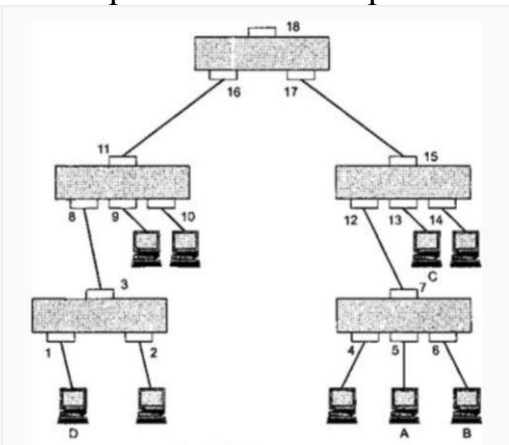
1. Определить минимальную длину кодового слова с возможностью исправления 3-х кратных ошибок при кодировании информации длиной 8 бит.
2. С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 10 Мбит/с и состоит из 200 узлов.
3. Определить максимальную длину кодового слова с возможностью исправления 3-х кратных ошибок при кодировании информации длиной 8 бит.
4. Определить минимальную длину кодового слова с возможностью исправления 1-х кратных ошибок при кодировании информации длиной 16 бит.
5. Определить минимальную длину кодового слова с возможностью исправления 3-х кратных ошибок при кодировании информации длиной 32 бит.
6. С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 8 Мбит/с и состоит из 120 узлов.
7. С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 10 Мбит/с и состоит из 50 узлов.
8. С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 10 Мбит/с и состоит из 80 узлов.
9. В дейтаграммной сети между узлами A и B существует три потока и три альтернативных маршрута. Можно ли направить каждый поток по отдельному маршруту?
10. Если все коммуникационные устройства в приведенном на рис. 1 фрагменте сети являются концентраторами, то на каких портах появится кадр, если его отправил компьютер A компьютеру B?



11. Определить максимальную длину кодового слова с возможностью исправления 3-х кратных ошибок при кодировании информации длиной 32 бит.

12. Определить максимальную длину кодового слова с возможностью исправления 3-х кратных ошибок при кодировании информации длиной 16 бит.

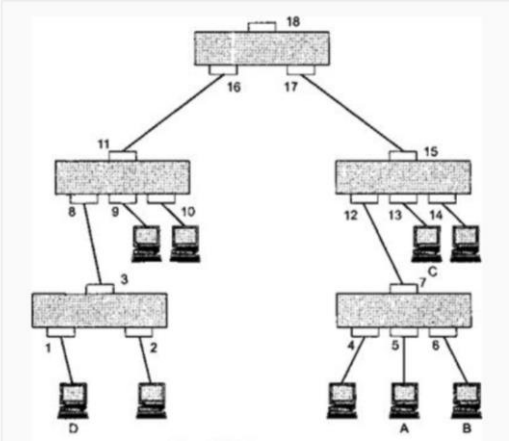
13. Если все коммуникационные устройства в приведенном на рис. 1 фрагменте сети являются коммутаторами, то на каких портах появится кадр, если его отправил компьютер A компьютеру B?



14. Сеть может передавать данные в двух режимах: с помощью дейтаграмм и по виртуальным каналам. Какие соображения вы бы приняли во внимание при выборе того или иного режима для передачи ваших данных, если главным критерием выбора для вас является скорость и надежность доставки?

15. В сети, поддерживающей технику виртуальных каналов, между узлами A и B существует три потока и три альтернативных маршрута. Можно ли направить каждый поток по отдельному маршруту?

16. Если все коммуникационные устройства в приведенном на рис. 1 фрагменте сети являются коммутаторами, кроме одного концентратора, к которому подключены компьютеры A и B, то на каких портах появится кадр, если его отправил компьютер A компьютеру D?



17. С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 9 Мбит/с и состоит из 50 узлов.

18. С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 8 Мбит/с и состоит из 180 узлов.

19. С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 10 Мбит/с и состоит из 180 узлов.

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

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

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

Соответствие 100-балльной и 5-балльной шкал

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

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

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

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

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

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