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

Система сертификации и лицензирования деятельности по защите информации
(наименование учебной дисциплины)

10.05.02 Информационная безопасность, профиль «Управление безопасностью телекоммуникационных систем и сетей»
(код и наименование ОПОП ВО)

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ.

Тема 1. Оценочные стандарты в информационной безопасности

1. Какую роль играют стандарты информационной безопасности?
2. Что представляет собой «Оранжевая книга» как оценочный стандарт?
3. Охарактеризуйте международный стандарт ISO/IEC 15408?
4. Каковы критерии оценки безопасности информационных систем?
5. Дайте определение стандартам информационной безопасности
6. Дайте определение термину «стандарт»

Тема 2. Стандарты управления информационной безопасностью

1. Какие существуют стандарты управления информационной безопасностью?
2. Для чего предназначен стандарт BS 7799
3. Практическое применение стандарта ISO/IEC 17799?
4. Каковы основные положения, международного стандарта ISO/IEC 27001:2005?
5. Как проходит сертификация стандарта управления информационной безопасностью СУИБ на соответствие ISO 27001?
6. Дайте определение термину «сертификация»

Тема 3. Международные стандарты информационной безопасности

1. Какие функции выполняет Европейский институт стандартизации телекоммуникации?
2. Какие приняты стандарты комитета технической безопасности ETSI?
3. Что описывает стандарт «надлежащей практики»?
4. Североамериканская корпорация по надежности электроснабжения (NERC)?
5. Рамки информационной безопасности NIST (NIST CSF) RFC 2196 ISA
6. Какие существуют требования к системной безопасности и уровням безопасности согласно стандарту IEC-62443?

Тема 4. Стандартизация в области облачных технологий

1. Какие стандарты регулируют безопасность облачных услуг?
2. Охарактеризуйте совместимость систем управления облаком между провайдером и заказчиком.
3. Какие существуют проекты международных стандартов по облачным вычислениям?
4. Каковы функции российской стандартизации облачных вычислений?
5. Для чего предназначены облачные стандарты?
6. Применение немецкого стандарта BSI?

Тема 5. Управление рисками. Основные понятия

1. В чем заключается важность при выборе анализируемых объектов и уровня детализации их рассмотрения?
2. Как происходит выбор методики оценки рисков?
3. Что представляет собой инвентаризация активов?
4. Как происходит анализ угроз и их последствий?
5. Какова необходимость выявления уязвимых мест в защите?
6 Что представляет собой оценка рисков?

Тема 6. Методика оценки рисков информационной безопасности компании Digital Security

1. Дайте определение архитектуры информационных систем.
2. Какую информацию предоставляет программа (согласно описанию программного обеспечения, на сайте-разработчика DigitalSequrity) по результатам моделирования?
3. Как производится расчет рисков по угрозе конфиденциальность?
4. Как производится учет наличия доступа при помощи VPN?
5. Как обеспечивается расчет рисков по угрозе целостность?
6. Какие характеристики ИС определяются в результате работы алгоритма оценки рисков по методике от Digital Security?

Тема 7. Методики и технологии управления рисками

1. В чем особенность качественной методики управления рисками?
2. Какие основные аспекты организации режима информационной безопасности в компании определены в части 1: 2002 г. Стандарт ISO 17799?
3. Что позволяет определить методика COBRA?
4. В чем особенность количественной методики управления рисками?
5. В чем состоит метод CRAMM?
6. Что обеспечивает методика Method Ware?

Тема 8. Разработка корпоративной методики анализа рисков

1. Что обеспечивают методы оценивания информационных рисков?
2. Какими могут быть информационные риски?
3. Как происходит ранжирование угроз по значениям их фактора риска?
4. Какие существуют табличные методы оценки рисков?
5. Определите методику анализа рисков Microsoft
6. Как происходит определение уровня риска в зависимости от уровней угроз и уязвимостей?

Тема 9. Лицензирование деятельности в области ТЗИ.

1. Что представляет собой лицензирование?
2. Назовите этапы получения лицензии.
3. Какие документы необходимы при лицензировании?
4. В каких случаях происходит прекращение лицензии?

5. Перечислите виды деятельности на осуществление которых требуется получение лицензии.

6. Как обеспечивается контроль за соблюдением лицензионных требований и условий?

Тема 10. Объект информатизации. Классификация объектов защиты.

1. По каким основаниям классифицируют информацию?
2. На какие этапы классифицируются автоматизированные системы?
3. Назовите принципы классификации средств вычислительной техники?
4. Каковы принципы политики разграничения доступа?
5. Какие существуют классы информационной системы?
6. Комплекс средств защиты должен быть в состоянии осуществлять регистрацию следующих событий?

Тема 11. Общий порядок сертификации средств защиты информации

1. Дайте понятие сертификации.
2. Что включают органы по сертификации?
3. Назовите функции органов по сертификации.
4. Каковы этапы проведения процедуры сертификации?
5. Схемы проведения сертификации средств защиты информации.
6. Что представляет собой система сертификации средств защиты информации?

Тема 12. Порядок сертификации во ФСТЭК России

1. Как происходит подача заявки на сертификацию во ФСТЭК России?
2. Что входит в решение на проведение сертификационных испытаний?
3. Как происходит заключение договора с испытательной лабораторией?
4. Каковы этапы подготовки исходных данных?
5. Что представляют собой сертификационные испытания?
6. Назовите виды сертификационных испытаний.

Тема 13. Аттестация объекта информатизации по требованиям безопасности информации

1. В чем заключается необходимость проведения аттестации?
2. Какова структура органов, проводящих аттестацию?
3. Кто несет ответственность при проведении аттестации объектов информатизации?
4. Как происходит документальное сопровождение процедуры аттестации?
5. Что входит в структуру аттестата соответствия?
6. В каких случаях аттестация является обязательной?

Тема 14. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники

1. Что входит в структуру и содержание положения документа «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К)?

2. Каковы обязательные требования по технической защите конфиденциальной информации СТР-К?

3. Каковы желательные требования к объектам информатизации?

4. Назовите этапы обеспечения защиты информации в автоматизированных системах?

5. Какие существуют требования и рекомендации в зависимости от типа автоматизированных систем?

6. Дайте основные рекомендации по защите информации, составляющей коммерческую тайну.

Критерии оценки:

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

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

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

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ЛАБОРАТОРНЫХ РАБОТ

Практическая работа №1 «Определение класса государственной информационной системы (ГИС)»

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

Практическая №2 «Разработка структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации»

1. Как присваивать теги, которые описывают данный документ или область его применения, для последующей группировки.
2. Назовите основные государственные и международные стандарты в области информационных технологий
3. Дайте определению термину «теги»
4. Дайте определение термину «защита информации»
5. Что входит в понятие «информационная безопасность»?
6. Какова цель создания государственных и международных стандартов в области информационной безопасности и защиты информации?

Практическая работа №3 «Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности»

1. Как проводится сертификация средств защиты информации?
2. Что показывают характеристики данного средства защиты?
3. Какой регулятор контролирует данную область информационной безопасности?
4. Какая основная информация содержится в сертификате?
5. Что представляют собой средства защиты от несанкционированного доступа?
6. Охарактеризуйте средства контроля защищенности
7. Назовите средства криптографической защиты

Практическая работа №4 «Анализ заданного нормативно-правового акта Российской Федерации»

1. Какие части документа относятся к вопросам защиты информации?
2. Что показывают комментарии к данному документу?
3. Как менялся текст нормативного акта с момента его создания по настоящее время?
4. Какие нормативно-правовые акты регулируют вопросы защиты информации?
5. Перечислите основные федеральные законы, регулирующие вопросы защиты информации
6. Что регламентирует Федеральный закон ФЗ «О персональных данных»?

Критерии оценки:

3-4 балла (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

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

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

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

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1. Согласно закону «О техническом регулировании», стандарт - это

(1) документ, в котором в целях добровольного многократного использования сформулированы характеристики продукции

(2) требование соблюдения единообразия технических и иных характеристик

(3) изделие, характеристики которого считаются эталонными

2. Для передаваемых данных протокол передачи записей обеспечивает

(1) конфиденциальность

(2) целостность

(3) доступность

3. В число основных понятий обобщенного прикладного программного интерфейса службы безопасности входят:

(1) сервис безопасности

(2) механизм безопасности

(3) контекст безопасности

4. Обычно политика безопасности запрещает:

(1) разделять счета пользователей

(2) заводить новые счета пользователей

(3) ликвидировать счета пользователей

5. Согласно спецификации Internet-сообщества "Как реагировать на нарушения информационной безопасности", под нарушением информационной безопасности понимается:

(1) потеря конфиденциальности информации

(2) нарушение целостности информации

(3) несанкционированное копирование информации

6. В стандарте BS 7799 фигурируют следующие группы регуляторов безопасности:

(1) политика безопасности

(2) программа безопасности

(3) общеорганизационные аспекты защиты

7. В стандарте FIPS 140-2 фигурируют следующие группы требований безопасности:

(1) конечноавтоматная модель

(2) формальная модель политики безопасности

(3) поведенческая модель

8. В соответствии с курсом, к числу важнейших видов общих функциональных требований к сервисам безопасности принадлежат:

(1) идентификация (FIA_UID)

(2) аутентификация (FIA_UAU)

(3) выявление и реагирование на неудачи аутентификации (FIA_AFL)

9. Работа над стандартом ISO/IEC 15408-1999 началась в

(1) 1990 году

(2) 1993 году

(3) 1999 году

10. Версия 2.1 «Общих критериев» содержит

(1) 10 классов функциональных требований безопасности

(2) 11 классов функциональных требований безопасности

(3) 12 классов функциональных требований безопасности

11. Версия 2.1 "Общих критериев" содержит:

(1) 10 классов требований доверия безопасности

(2) 11 классов требований доверия безопасности

(3) 12 классов требований доверия безопасности

12. Согласно "Общим критериям", предположения безопасности

(1) являются частью описания среды, в которой функционирует объект оценки

(2) являются частью описания объекта оценки

(3) являются частью политики безопасности организации, эксплуатирующей объект оценки

13.Произвольное (дискреционное) управление доступом основывается на:

(1) атрибутах безопасности (FDP_ACF.1)

(2) иерархических атрибутах безопасности (FDP_IFF.2)

(3) управлении информационными потоками (FDP_IFC.1)

14. В проекте профиля защиты [PPMOS] предусмотрены максимальные квоты

(1) долговременной памяти

(2) суммарного времени сеансов

(3) суммарного сетевого трафика

15. Служба директорий предоставляет следующие группы операций:

(1) захват

(2) опрос

(3) верификация

16. Формирование контекстов безопасности в IPsec разделено на

(1) две фазы

(2) три фазы

(3) четыре фазы

17. В «Оранжевой книге» фигурируют понятия:

(1) ядро безопасности

(2) периметр безопасности

(3) центр безопасности

18. Если для передачи записей выстроится очередь сообщений разных типов, то приоритет прикладных данных окажется

(1) минимальным

(2) промежуточным

(3) максимальным

19. В обобщенном прикладном программном интерфейсе службы безопасности удостоверения выступают как средство

(1) аутентификации

(2) контроля целостности

(3) обеспечения конфиденциальности

20. В случае нарушения информационной безопасности следует предпочесть стратегию «защититься и продолжить», если

(1) активы организации недостаточно защищены

(2) активы организации надежно защищены

(3) нет достоверных сведений о защищенности активов организации

21. Согласно спецификации Internet-сообщества "Как реагировать на нарушения информационной безопасности", в документах группы реагирования должна быть приведена следующая контактная информация:

(1) адрес обычной почты

(2) адрес электронной почты

(3) адрес информационного сервера

22. В стандарте BS 7799 выделены следующие ключевые регуляторы безопасности:

(1) документ о политике информационной безопасности

(2) программа безопасности

(3) регулярное выявление уязвимых мест

23. Согласно стандарту FIPS 140-2, перед криптографическим модулем ставятся следующие высокоуровневые функциональные цели безопасности:

(1) предотвращение несанкционированной и необнаруживаемой модификации модуля и криптографических алгоритмов

(2) предотвращение несанкционированной модификации, подмены, вставки и удаления криптографических ключей

(3) предотвращение несанкционированной модификации ограниченного эксплуатационного окружения

24. Согласно спецификации X.800, ни на сетевом, ни на транспортном уровнях эталонной семиуровневой модели не реализуются следующие функции безопасности:

(1) избирательная конфиденциальность

(2) конфиденциальность трафика

(3) неотказуемость

25. Под изделием ИТ в «Общих критериях» может пониматься

(1) продукт

(2) система

(3) технология

26. Согласно версии 2.1 «Общих критериев», уровень протоколирования может быть:

(1) минимальным

(2) базовым

(3) максимальным

27. Элемент доверия может принадлежать следующим типам:

(1) элементы действий системного администратора

(2) элементы действий разработчика

(3) элементы физической защиты

28. В соответствии с требованиями компонента FAU_SEL.1, избирательность регистрации событий должна основываться по крайней мере на следующих атрибутах:

(1) тип события

(2) время события

(3) длительность события

29. В профилях защиты для межсетевых экранов политика безопасности базируется на принципе

(1) все разрешено

(2) все запрещено

(3) все, что не разрешено, запрещено

30. Для защиты от атак на доступность в проекте ПЗ СУБД [PPSUBD] предусмотрены:

(1) реализация квот, выделяемых пользователям

(2) базовые ограничения на параллельные сеансы

(3) обслуживание с учетом приоритетов

31. В число операций опроса, предоставляемых службой директорий, входят:

(1) поиск и чтение элементов, удовлетворяющих заданным фильтрам, в заданных частях Информационного Дерева

(2) выдача информации о текущем статусе незавершенной операции опроса

(3) отказ от незавершенной операции опроса

32. Согласно спецификациям IPsec, управляющие контексты являются

(1) двунаправленными

(2) однонаправленными

(3) ненаправленными

33. «Общие критерии» содержат следующие основные виды требований безопасности:

(1) архитектурные требования

(2) функциональные требования

(3) требования доверия

34. В обобщенном прикладном программном интерфейсе службы безопасности контекст безопасности - это

(1) пара структур данных - по одной локально хранимой структуре для каждого партнера по общению

(2) структура данных, аутентифицирующая партнера по общению

(3) элемент данных, пересылаемый между пользователями с целью защиты прикладной информации

35. В число мер для борьбы с нарушением безопасности входят:

(1) профилактика

(2) сдерживание

(3) наказание

36. Согласно спецификации Internet-сообщества "Как реагировать на нарушения информационной безопасности", услуги, оказываемые группой реагирования, можно разделить на следующие категории:

(1) действия, непосредственно связанные с реагированием на нарушения

(2) профилактические действия

(3) сбор свидетельств для судебного преследования нарушителя

37. Согласно стандарту BS 7799, меры по безопасному администрированию систем и сетей разбиты на следующие подгруппы:

(1) профилактическое обслуживание

(2) повседневное обслуживание

(3) сервисное обслуживание

38. Согласно стандарту FIPS 140-2, на втором уровне безопасности криптографического модуля требуются:

(1) ролевая аутентификация

(2) персональная аутентификация

(3) аутентификация с помощью одноразовых паролей

39. Стандарт FIPS 140-2 описывает следующие аспекты компьютерной криптографии:

(1) алгоритмический

(2) интерфейсный

(3) собственной защищенности

40. Согласно версии 2.1 "Общих критериев", в число семейств класса «приватность» входят:

(1) анонимность

(2) бесследность

(3) скрытность

41. Класс ADV (разработка) предусматривает следующие стили изложения спецификаций:

(1) неформальный

(2) текстовый

(3) графический

42. Рекомендуемые общие требования доверия безопасности предусматривают наличие

(1) функциональной спецификации

(2) проекта верхнего уровня

(3) проекта нижнего уровня

43. В профиле защиты, регламентирующем выпуск и управление сертификатами, предусмотрены следующие роли:

(1) администратора

(2) арбитра

(3) инспектора

44. Согласно проекту ПЗ [PPVPN], концами туннелей, реализующих виртуальные частные сети, целесообразно сделать

(1) межсетевые экраны, обслуживающие подключение организаций к внешним сетям

(2) маршрутизаторы поставщика сетевых услуг

(3) персональные межсетевые экраны сотрудников

45. В рекомендациях X.509 определены следующие виды сертификатов открытых ключей:

(1) сертификаты оконечных сущностей

(2) сертификаты контролирующих центров

(3) сертификаты удостоверяющих центров

46. Протокол AH защищает поля IP-заголовков, которые

(1) не меняются на маршруте доставки

(2) меняются предсказуемым образом

(3) меняются произвольным образом

47. Стандарты и спецификации подразделяются на

(1) оценочные стандарты

(2) технические спецификации

(3) нормативные спецификации

48. Семейство протоколов TLS имеет

(1) одноуровневую организацию

(2) двухуровневую организацию

(3) семиуровневую организацию

49. В число основных понятий обобщенного прикладного программного интерфейса службы безопасности входят:

(1) удостоверение

(2) билет

(3) мандат

50. Согласно «Руководству по информационной безопасности предприятия», политика безопасности отвечает на вопрос:

(1) что?

(2) как?

(3) когда?

51. Согласно спецификации Internet-сообщества «Как реагировать на нарушения информационной безопасности», группа реагирования обязана

(1) предоставлять помощь членам опекаемого сообщества в предотвращении нарушений

(2) предоставлять помощь членам опекаемого сообщества в ликвидации нарушений

(3) предоставлять помощь членам опекаемого сообщества в информировании общественности о последствиях нарушений

52. В стандарте BS 7799 фигурируют следующие группы регуляторов безопасности:

(1) администрирование систем и сетей

(2) управление доступом к приложениям

(3) управление доступом к системам и сетям

53. В стандарте FIPS 140-2 фигурируют следующие группы требований безопасности:

(1) спецификация криптографического модуля

(2) требования к портам и интерфейсам модуля

(3) спецификация политики безопасности криптографического модуля

54. В курсе рассматриваются профили защиты для следующих разновидностей сервисов безопасности:

(1) парольная аутентификация

(2) аутентификация с помощью смарт-карт

(3) биометрическая идентификация и аутентификация

55. «Общие критерии» включают следующие виды требований:

(1) функциональные требования

(2) требования доверия

(3) требования эффективности

56. Версия 2.1 «Общих критериев» содержит следующие классы функциональных требований безопасности:

(1) FAC - управление доступом

(2) FAU - аудит безопасности

(3) FIA - идентификация/аутентификация

57. В трактовке "Общих критериев" доверие - это

(1) основа для уверенности в том, что изделие ИТ отвечает целям безопасности

(2) основа для уверенности в том, что в изделии ИТ отсутствуют нерегламентированные функциональные возможности

(3) основа для уверенности в высокой квалификации и благонадежности разработчиков

58. Согласно "Общим критериям", в профиле защиты должны быть описаны:

(1) предположения безопасности

(2) регуляторы безопасности

(3) угрозы безопасности

59. В пакетных фильтрах решения по фильтрации потоков данных принимаются на основе набора правил, в которых могут фигурировать:

(1) исходный сетевой адрес

(2) протокол транспортного уровня

(3) протокол прикладного уровня

60. Использование виртуальных локальных сетей позволяет:

(1) повысить производительность и доступность сети

(2) повысить защиту передаваемых данных

(3) реализовать управление доступом пользователей к сетевым ресурсам

61. В число операций опроса, предоставляемых службой директорий, входят:

(1) чтение значений атрибутов элемента Директории

(2) модификация значений атрибутов элемента Директории

(3) создание новых атрибутов элемента Директории

62. Протоколы семейства IPsec обеспечивают:

(1) управление доступом

(2) безопасное восстановление

(3) конфиденциальность

63. Спецификация IPsec затрагивает вопросы

(1) доступности

(2) конфиденциальности

(3) целостности

64. Смена параметров шифрования

(1) относится к протоколу передачи записей

(2) относится к протоколу установления соединений

(3) выделена в самостоятельный протокол

65. Обобщенный прикладной программный интерфейс службы безопасности предоставляет услуги по:

(1) авторизации общающихся партнеров

(2) взаимной аутентификации общающихся партнеров

(3) протоколированию действий общающихся партнеров

66. В "Руководстве по информационной безопасности предприятия" фигурируют следующие классы активов:

(1) аппаратура

(2) программное обеспечение

(3) информационное обеспечение

67. Согласно спецификации Internet-сообщества "Как реагировать на нарушения информационной безопасности", в уставе группы реагирования должны присутствовать следующие разделы:

(1) виды деятельности

(2) клиентура

(3) порядок выбора руководящих органов

68. В стандарте BS 7799 выделены следующие ключевые регуляторы безопасности:

(1) антивирусные средства

(2) средства контроля защищенности

(3) средства выявления вторжений

69. Согласно стандарту FIPS 140-2, перед криптографическим модулем ставятся следующие высокоуровневые функциональные цели безопасности:

(1) применение и безопасная реализация утвержденных функций безопасности для защиты информации ограниченного доступа

(2) расширяемость, возможность поддержки новых функций безопасности

(3) эффективность, возможность обработки сколь угодно больших массивов данных

70. Стандарт BS 7799 описывает меры следующих уровней информационной безопасности:

(1) административного

(2) процедурного

(3) программно-технического

71. Согласно "Общим критериям", стойкость функции безопасности может быть

(1) низкой

(2) умеренной

(3) высокой

72. Согласно версии 2.1 "Общих критериев", в число семейств класса FTA "доступ к объекту оценки" входят:

(1) открытие сеанса

(2) блокирование сеанса

(3) закрытие сеанса

73. Оценочный уровень доверия 4 характеризуется:

(1) демонстрацией устойчивости к попыткам проникновения нарушителей с низким потенциалом нападения

(2) демонстрацией устойчивости к попыткам проникновения нарушителей с умеренным потенциалом нападения

(3) демонстрацией устойчивости к попыткам проникновения нарушителей с высоким потенциалом нападения

74. В число выделенных общих угроз безопасности входят:

(1) маскарад пользователя

(2) маскарад сети

(3) маскарад сервера

75. Компонент функциональных требований "Общих критериев" FAU_SAA.1

(1) ориентирован на обнаружение превышения порогов, заданных фиксированным набором правил

(2) служит для выявления нетипичной активности путем анализа профилей поведения

(3) направлен на выявление простых атак путем проведения сигнатурного анализа

76. Необычность смарт-карт как объекта оценки заключается в:

(1) ограниченности аппаратных ресурсов

(2) принадлежности неконтролируемой среде

(3) высокой стоимости ассоциированных активов

77. Рекомендации X.509 регламентируют следующие аспекты:

(1) каркас сертификатов открытых ключей

(2) каркас генерации открытых и секретных ключей

(3) каркас управления криптографическими ключами

78. Все реализации IPsec должны поддерживать селекцию следующих элементов:

(1) исходный и целевой IP-адреса

(2) исходный и целевой порты

(3) класс обслуживания

79. Согласно закону "О техническом регулировании", стандартизация – это:

(1) деятельность по выработке единых требований к техническим и иным характеристикам продукции

(2) деятельность по установлению правил и характеристик в целях их добровольного многократного использования

(3) деятельность по установлению единообразия в сфере производства и иных сферах

80. Для передаваемых данных протокол передачи записей обеспечивает

(1) конфиденциальность трафика

(2) конфиденциальность содержимого отдельных сообщений

(3) конфиденциальность типов сообщений

81. В число основных понятий обобщенного прикладного программного интерфейса службы безопасности входят:

(1) дескриптор

(2) идентификатор

(3) имя

82. Обычно политика безопасности запрещает:

(1) часто менять пароли

(2) использовать короткие пароли

(3) выбирать слабые пароли

83. Согласно спецификации Internet-сообщества "Как реагировать на нарушения информационной безопасности", под нарушением информационной безопасности понимается:

(1) неправомочное повышение цен на использование информационных услуг

(2) нарушение доступности информационных услуг

(3) неправомочное использование услуг, систем или информации

84. В стандарте BS 7799 фигурируют следующие группы регуляторов безопасности:

(1) физическая безопасность и безопасность окружающей среды

(2) безопасность персонала

(3) безопасность электронного бизнеса

85. В стандарте FIPS 140-2 фигурируют следующие группы требований безопасности:

(1) электромагнитная безопасность

(2) управление криптографическими ключами

(3) электромагнитная совместимость

86. В соответствии с курсом, к числу важнейших видов общих функциональных требований к сервисам безопасности принадлежат:

(1) аутентификация данных (FDP_DAU)

(2) политика управления доступом (FDP_ACC)

(3) функции управления доступом (FDP_ACF)

87. Работа над "Общими критериями" началась в:

(1) 1990 году

(2) 1993 году

(3) 1999 году

88. Версия 2.1 "Общих критериев" содержит:

(1) 66 семейств функциональных требований безопасности

(2) 77 семейств функциональных требований безопасности

(3) 88 семейств функциональных требований безопасности

89. Версия 2.1 "Общих критериев" содержит:

(1) 66 семейств требований доверия безопасности

(2) 55 семейств требований доверия безопасности

(3) 44 семейства требований доверия безопасности

90. Согласно "Общим критериям", достижение целей безопасности должно обеспечивать:

(1) устойчивость к угрозам безопасности

(2) проведение в жизнь политики безопасности

(3) отсутствие уязвимостей в объекте оценки

91. Принудительное (мандатное) управление доступом основывается на:

(1) атрибутах безопасности (FDP_ACF.1)

(2) иерархических атрибутах безопасности (FDP_IFF.2)

(3) ограниченном управлении информационными потоками (FDP_IFC.1)

92. В проекте профиля защиты [PPMOS] предусмотрены максимальные квоты:

(1) количества одновременно открытых окон

(2) оперативной памяти

(3) количества одновременно открытых сетевых соединений

93. Служба директорий предоставляет следующие группы операций:

(1) блокирование

(2) модификация

(3) откат

94. В семействе спецификаций IPsec определены:

(1) сетевой контекст

(2) управляющий контекст

(3) протокольный контекст

95. В "Гармонизированных критериях Европейских стран" фигурируют понятия:

(1) цель оценки

(2) система оценки

(3) объект оценки

96. В протоколе передачи записей вычисление имитовставки

(1) предшествует шифрованию

(2) выполняется параллельно с шифрованием

(3) следует за шифрованием

97. В рамках обобщенного прикладного программного интерфейса службы безопасности приложениям предоставляется

(1) прямой доступ к удостоверениям

(2) доступ к некоторым полям удостоверений

(3) доступ к дескрипторам удостоверений

98. В случае нарушения информационной безопасности следует предпочесть стратегию "выследить и осудить", если

(1) активы организации недостаточно защищены

(2) активы организации надежно защищены

(3) нет достоверных сведений о защищенности активов организации

99. Согласно спецификации Internet-сообщества "Как реагировать на нарушения информационной безопасности", в документах группы реагирования должна быть приведена следующая контактная информация:

(1) часы работы

(2) приемные часы

(3) часовой пояс

100. В стандарте BS 7799 выделены следующие ключевые регуляторы безопасности:

(1) распределение обязанностей по обеспечению информационной безопасности

(2) обучение и подготовка персонала к поддержанию режима информационной безопасности

(3) выработка и применение мер наказания нарушителей режима информационной безопасности

Задания в открытой форме

1) … – концептуальная модель, которая характеризует и стандартизирует коммуникационные функции телекоммуникационной или вычислительной системы без учета ее внутренней структуры и технологии.
2) … – сетевая модель, описывающая процесс передачи цифровых данных.
3) … – массовая рассылка корреспонденции рекламного характера лицам, не выражавшим желания её получить.
4) ... – процедура скрытного перенаправления жертвы на ложный IP-адрес.
5) ... – совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от определенного множества угроз и составляет необходимое условие безопасности системы.
6) … – уровень выносится управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.
7) … – разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников.
8) … – программные средства контроля доступа в систему, используемые для защиты уязвимой информации и программных средств.

9) … – процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно определяющий этого субъекта в информационной системе.
10) … – процедура проверки подлинности, например проверка подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных.
11) … – предоставление определенному лицу или группе лиц прав на выполнение определенных действий.
12) … – всестороннее обследова-ние, позволяющее оценить текущее состояние информационной безопасно-сти организации и спланировать дальнейшие шаги по повышению уровня защищенности.
13) … – основная функция систем межсетевых экранов (или брандмауэров), которая позволяет сетевому администратору распределить пользователям как доступ из внешней сети к службам компьютеров, находя-щимся внутри сети предприятия, или к защищенному сегменту сети, так и доступ пользователей из внутренней сети к соответствующим ресурсам внешней сети.
14) … – программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.
15) … – компьютерный вирус, записывающийся в первый сектор гибкого или жесткого диска и выполняющийся при загрузке компьютера.
16) … – разновидность вредоносной программы, проникающая в компьютер под видом легитимного программного обеспечения, в отличие от вирусов и червей, которые распространяются самопроизвольно.
17) … – вторжение в операционную систему удаленного компьютера.
18) … – степень адекватности реализованных в ней механизмов защиты информации существующим в данной среде функционирования рискам, связанным с осуществлением угроз безопасности информации.
19) … – возможность нарушения таких свойств информации, как конфиденциальность, целостность и доступность.
20) … – стандартизированный язык гипертекстовой разметки документов для просмотра веб-страниц в браузере.
21) … – мультипарадигменный язык программирования. Поддерживает объектно-ориентированный, императивный и функциональный стили.

Задание на установление соответствия

1. Установить соответствие:

1) Сертификации средств защиты информации по требованиям безопасности информации	а) «Положением о сертификации средств защиты информации по требованиям безопасности

	информации», утвержденным Приказом председателя Гостехкомиссии России от 27 октября 1995 г. N 199
2) Установлен перечень средств защиты информации, подлежащих сертификации	b) Локальный нормативный правовой акт, определяющий необходимость создания системы защиты информации
3) Принятие решения о необходимости защиты информации	c) Деятельность по подтверждению характеристик средств защиты информации требованиям государственных стандартов или иных нормативных документов по защите информации

2. Установить соответствие:

1) Классификация по требованиям защиты информации (по уровню защищенности информации)	Частная модель угроз безопасности информации
2) Определение актуальных угроз безопасности информации	Акт классификации по требованиям безопасности информации
3) Определение требований к системе защиты информации	ТЗ на создание системы защиты информации с указанием требований к мерам и средствам защиты информации

3. Установить соответствие:

1) Установка и настройка средств защиты информации	a) Протокол контроля уязвимостей программного обеспечения и технических средств
2) Внедрение организационных мер, разработка организационно-распорядительных документов	b) Акт установки средств защиты информации
3) Выявление и анализ уязвимостей	c) Документы по регламентации правил по эксплуатации и вывода из эксплуатации системы защиты информации

4. Установить соответствие:

1) Испытания и опытная эксплуатации системы защиты информации	a) Протоколы контроля оценки эффективности средств и оценки защищенности информации

2) Аттестационные испытания системы защиты информации	b) Рекомендации по обеспечению защищенности информации на аттестуемом объекте и Аттестат соответствия
3) Оформление результатов аттестационных испытаний	c) Протоколы и заключение по результатам аттестационных испытаний

5. Установить соответствие:

1) Органы по сертификации осуществляют сертификацию средств защиты информации	a) производят средства защиты информации в соответствии с требованиями по безопасности информации.
2) Испытательные лаборатории проводят сертификационные испытания	b) оформляют сертификаты соответствия средств защиты информации требованиям по безопасности информации
3) Изготовители разрабатывают и	c) средств защиты информации и по их результатам оформляют технические заключения и протоколы. Испытательные лаборатории должны обеспечивать полноту сертификационных испытаний средств защиты информации и достоверность их результатов

6. Установить соответствие:

1) Заявителями на осуществление сертификации являются изготовители	a) а также на материально-технических базах заявителя и (или) изготовителя, расположенных на территории Российской Федерации.
2) Заявители должны обеспечивать соответствие сертифицированных средств защиты информации требованиям по безопасности информации	b) а также осуществлять устранение недостатков и дефектов средств защиты информации, в том числе устранение уязвимостей и недекларированных возможностей программного обеспечения средств защиты информации, информирование потребителей об обновлении программного

	обеспечения средств защиты информации, доведение до потребителей обновлений программного обеспечения средств защиты информации, а также изменений в эксплуатационную документацию (далее - техническая поддержка средств защиты информации)
3) Сертификационные испытания средств защиты информации проводятся на материально-технической базе испытательной лаборатории	c) а также федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления и организации, планирующие применять средства защиты информации

7. Установить соответствие:

1) Объект информатизации	a) комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России (Гостехкомиссией России). Наличие аттестата соответствия в организации дает право обработки информации с уровнем секретности (конфиденциальности) на период времени, установленный в аттестате.
2) Аттестация объектов информатизации	b) совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они

	установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров
3) Аттестация производится в порядке	c) установленном "Положением по аттестации объектов информатизации по требованиям безопасности информации" от 25 ноября 1994 года. Аттестация должна проводится до начала обработки информации, подлежащей защите. Это необходимо в целях официального подтверждения эффективности используемых мер и средств по защите этой информации на конкретном объекте информатизации

8. Установить соответствие:

1) Требования ФСТЭК по защите конфиденциальной информации	a) подбираются с учетом структуры СЗИ, состава и мест размещения ее элементов. Если защищаемая ИС проектируется в составе центра обработки данных (ЦОД) рекомендуется использовать уже имеющиеся в ЦОД средства, меры защиты данных.
2) Методы и средства технической защиты информации	b) направлены на исключение неправомерного доступа, копирования, передачи или распространения сведений. Для обеспечения требований по безопасности конфиденциальной информации проводится оценка возможных уязвимостей ИС для внешних и внутренних нарушителей, возможных средств реализации этих уязвимостей.
3) Меры защиты информации в информационных системах	c) согласно требованиям ФСТЭК должны обеспечивать необходимый уровень безопасности при взаимодействии защищаемых ИС с другими ИС, при обработке и хранении информации. При этом

	предлагаемые на этапе проектирования меры должны быть реализуемы в конкретной ИС.

9. Установить соответствие:

1) RSA	a) семейство криптографических алгоритмов - однонаправленных хеш-функций, включающее в себя алгоритмы SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/256 и SHA-512/224
2) DES	b) криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел
3) SHA-2	c) алгоритм для симметричного шифрования, разработанный фирмой IBM и утверждённый правительством США в 1977 году как официальный стандарт (FIPS 46- 3)

10. Установить соответствие:

1) Mail-Worm	a) У данного типа червей, как и у почтовых червей, существуют два способа распространения червя по IRC-каналам, повторяющие способы, описанные выше.
2) IM-Worm	b) черви, распространяющиеся в формате сообщений электронной почты.
3) P2P-Worm	c) прочие сетевые черви, среди которых имеет смысл дополнительно выделить интернет-черви и LAN-черви
4) IRC-Worm	d) черви, распространяющееся при помощи пиринговых (peer-to-peer) файлообменных сетей.
5) Net-Worm	e) черви, использующие интернет-пейджеры.

11.Установить соответствие:

1) Информационная безопасность	a) Неправомерный доступ к КИ

2) Общественная нравственность	b) Распространение порнографии
3) Конституционные права и свободы	c) Нарушение авторских прав
4) Собственность	d) Компьютерное мошенничество

12. Установить соответствие:

1) правовые методы обеспечения информационной безопасности;	a) выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;
2)организационно-технические методы обеспечения информационной безопасности;	b) совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц;
3) экономические методы обеспечения информационной безопасности.	c) разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации.

13. Установить соответствие:

1 Управление качеством	a) ISO9000
2 Экологический менеджмент	b) ISO14000
3 Информационная безопасность	c) ISO27000
4 Энергетический менеджмент	d) ISO 50001

14. Установить соответствие:

1.Защита информации от утечки	a) Деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками
2. Защита информации от несанкционированного воздействия	b) Деятельность, направленная на предотвращение воздействия на

	защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации
3.Защита информации от непреднамеренного воздействия	c) Деятельность, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации
4.Защита информации от разглашения	d) Деятельность, направленная на предотвращение несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации

15. Установить соответствие:

1. Целостность	a) Свойство информации сохранять свою структуру и содержание в процессе передачи и хранения
2. Конфиденциальность	b) Статус, предоставленный данным и определяющий требуемую степень защиты
3. Доступность	c) Возможность субъекта ознакомления с информацией
4. Достоверность	d) Свойство информации, выражающееся в строгой

	принадлежности субъекту, являющемуся источником информации

16. Установить соответствие:

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

17. Установить соответствие:

1) Принцип разумной достаточности	a) защита не должна обеспечиваться только за счет секретности структурной безопасности и алгоритмов функционирования ее подсистемы.
2) Принцип разумной избыточности	b) Должны быть реализованы принципы гибкости управления, обеспечивающие возможность настройки механизмов в процессе функционирования системы.
3) Принцип гибкости управления и применения	c) на этапе разработки системы защиты в нее должна закладываться некий потенциал, который позволил бы увеличить срок ее жизнеспособности.
4) Открытость алгоритмов и механизмов защиты	d) Необходимо правильно выбрать тот уровень защиты, при котором затраты, риск

	взлома и размер возможного ущерба были бы приемлемыми.

18. Установить соответствие:

1) Первый фактор	a) прочность существующего механизма защиты, характеризующаяся степенью сопротивляемости этих механизмов попыткам их обхода или преодоления.
2) Второй фактор	b) величина ущерба, наносимого владельцу АСОД в случае успешного осуществления угроз безопасности
3) Третий фактор	c) каждый путь осуществления угрозы должен быть перекрыт соответствующим механизмом защиты

19. Установить соответствие:

1) Правовые	a) Реализуются в виде механических, электрических и электронных устройств, предназначенных для препятствования проникновению и доступу потенциального нарушителя к компонентам защиты.
2) Морально-этические	b) Представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры телекоммуникаций для обеспечения защиты информации
3) Административные	c) К ним относятся нормы поведения, которые традиционно сложились по мере

	распространения сетевых и информационных технологий.
4) Технические	d) Определяются законодательными актами страны, которыми регламентируется правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

20. Установить соответствие:

1) К сведениям особой важности следует относить	a) Все иные из числа сведений, составляющих государственную тайну.
2) К совершенно секретным сведениям следует относить	b) Такие сведения, распространение которых может нанести ущерб интересам министерства, ведомства или отраслям экономики РФ в одной или нескольких областях деятельности.
3) К секретным сведениям следует относить	c) Такие сведения, распространение которых может нанести ущерб интересам РФ в одной или нескольких областях деятельности.

21. Установить соответствие:

1) Уровень системы управления базами данных	a) Отвечает за взаимодействие с пользователем
2) Уровень прикладного программного обеспечения	b) Отвечает за хранение и обработку данных информационной системы.
3) Уровень операционной системы	c) Отвечает за взаимодействие узлов информационной системы
4) Уровень сети	d) Отвечает за обслуживание СУБД и прикладного программного обеспечения.

Задания на установление правильной последовательности

1. 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

2. Выберите правильную последовательность этапов в жизненном цикле атаки:
1) Выбор способа атаки
2) Закрепление
3) Эксплуатация
4) Достижение цели
5) Исполнение команд
6) Разведка и сбор данных
7) Доставка

3. Установите последовательность этапов совершения преступления в сфере компьютерной информации:
1) формирование умысла
2) приготовление
3) покушение
4) оконченное преступление

4. Укажите правильный порядок действий органа по аттестации при исполнении своих функций:
1) Разработка программы и методики аттестационных испытаний
2) Проведение анализа исходных данных по аттестуемому объекту
3) Проведение аттестации объектов информатизации

5. Выберите верный порядок действий:
1) Выбор СЗИ
2) Проведение классификации АС
3) Проверка эффективности СЗИ
4) Установка и настройка СЗИ

6. Определите верный порядок действий при проведении работ по аттестации объекта информатизации:
1) проведение аттестационных испытаний
2) оценка эффективности принятых мер по защите информации

3) разработка программы и методик аттестационных испытаний
4) оценка эффективности принятых мер по защите информации

7. Укажите правильный порядок степеней секретности:
1) Особо важный
2) Совершенно секретный
3) Секретный

8. В соответствии с документом, классификация АС включает следующие этапы:
1) Сравнение выявленных признаков АС с классифицируемыми.
2) Присвоение АС соответствующего класса защиты информации от НСД.
3) Выявление основных признаков АС, необходимых для классификации.
4) Разработка и анализ исходных данных.

9. Согласно модели PDCA (Цикл Шухарта – Деминга) выделяется 4 этапа создания системы обеспечения информационной безопасности (СОИБ) в следующей последовательности:
1) Планирование СОИБ
2) Реализация СОИБ
3) Проверка СОИБ
4) Совершенствование СОИБ

10. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации включает следующие действия:
1) испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);
2) проведение аттестационных испытаний объекта информатизации;
3) оформление, регистрация и выдача "Аттестата соответствия";
4) подачу и рассмотрение заявки на аттестацию;
5) разработка программы и методики аттестационных испытаний;
6) осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации;
7) предварительное ознакомление с аттестуемым объектом;
8) рассмотрение апелляций;
9) заключение договоров на аттестацию.

11. На этапе аттестационных испытаний объекта информатизации:
1) определяется правильность категорирования объектов ЭВТ и классификации АС (при аттестации автоматизированных систем), выбора и

применения сертифицированных и несертифицированных средств и систем защиты информации;
2)оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта информатизации в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта информатизации.
3) проводятся комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;
4) проводятся испытания несертифицированных средств и систем защиты информации на аттестуемом объекте или анализ результатов их испытаний в испытательных центрах (лабораториях) по сертификации;
5) осуществляется анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;
6) проверяется уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации;

12. Общий порядок сертификации:
1) Заключение Договора на проведение сертификационных испытаний
2) Подготовка исходных данных
3) Оформление Заявки на сертификацию
4) Экспертиза результатов сертификационных испытаний
5) Оформление Решения на проведение сертификации
6) Заключение Договора о проведении экспертизы результатов сертификационных испытаний в Органе по сертификации
7) Проведение сертификационных испытаний
8) Оформление Сертификата
9) Оформление Протоколов сертификационных испытаний и Технических заключений

13. Для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней, иногда - недель), поскольку за это время должны произойти следующие события:
1) заплаты должны быть установлены в защищаемой ИС.
2) должно стать известно о средствах использования пробела в защите;
3) должны быть выпущены соответствующие заплаты.

14. Установите последовательность этапов совершения преступления в сфере компьютерной информации:
1) формирование умысла
2) приготовление
3) покушение
4) оконченное преступление

15. Подход к реализации защитных мероприятий по обеспечению информационной безопасности должен соответствовать следующей последовательности:
1) Определение состава средств информационной системы
2) Анализ уязвимых элементов информационной системы и оценка угроз
3) Анализ риска
4) Определение способов защиты

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

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

18. Выберите правильную последовательность этапов жизненного цикла информационного сервиса:

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

19. Выберите правильную последовательность этапов построения системы защиты:
1) Анализ
2) Реализация системы защиты
3) Сопровождение системы защиты
4) Разработка системы защиты

20. Выберите последовательность приоритетных этапов защиты информации:
1) Защита информации от несанкционированного доступа
2) Защита информации в системах связи
3) Защита юридической значимости электронных документов
4) Защита конфиденциальной информации от утечки по каналам побочных электромагнитных излучений и наводок
5) Защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ
6) Защита от несанкционированного копирования и распространения программ и ценной компьютерной информации

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

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

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

Общий балл по промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости

в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

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

2.2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

Компетентностно-ориентированная задача № 1

В качестве входной информации берется текстовый файл, состоящий из ФИО студента, названия кафедры и специальности. Исходный поток данных соответствует последовательности бит, расположение которых определяется формулой, учитывающей порядковый номер студента по списку:

$$ci = (7i+n) \bmod 13 + 13i$$

Ключ скремблера соответствует номеру зачетки студента «слева направо», генератор псевдослучайных чисел - аналогично «справа налево». Порядок выполнения работы:

1) Сформировать блок исходных данных (не более 48 бит)

2) Рассчитать состояния скремблера для обработки входного блока

3) Рассчитать период зацикливания и период наибольшей длины скремблера

Компетентностно-ориентированная задача № 2

Обоснуйте необходимость проведения лицензирования выбранного вида деятельности фирмы ООО «Харддезигн» по производству компьютерной техники. Укажите порядок и необходимость (обязательная или добровольная) сертификации средств, используемых в выбранном виде деятельности.

Компетентностно-ориентированная задача № 3

Укажите перечень сертификационных документов, необходимых ООО «Харддезигн» для производства компьютерной техники. Какой орган отвечает за проведение сертификации?

Компетентностно-ориентированная задача № 4

При локальном доступе к информации на ресурсе необходимо найти коэффициент локальной защищенности информации на ресурсе. Расчет рисков по угрозе конфиденциальность: Коэффициенты защищенности:

	Коэфф. локальной защищен.	Коэфф. удаленной защищен.	Коэфф. локальной защищен. рабочего места	Наименьший коэфф.
Главный бухгалтер / бухгалтерский отчет	55	-	-	?
Бухгалтер / база клиентов Компании	-	22	43	?
Финансовый директор / база клиентов компании	-	22	-	?
Бухгалтер / база данных наименований товаров компании	30	-	-	?

Компетентностно-ориентированная задача № 5

Определите учет наличия доступа при помощи VPN.

	Наименьший коэффициент	Вес VPN-соединения	Результирующий коэффициент
Главный бухгалтер / бухгалтерский отчет	55	-	?
Бухгалтер / база клиентов Компании	22	20	?

Финансовый директор / база клиентов Компании	22	20	?
Бухгалтер / база данных наименований товаров Компании	30	-	?

Компетентностно-ориентированная задача № 6

Определите учет количества человек в группе и наличия у группы пользователей доступа в Интернет:

	Результирующий коэффиц.	Количество пользователей	Наличие у пользователей доступа в Интернет	Итоговый коэффиц.
Главный бухгалтер / бухгалтерский отчет	55	1	2	?
Бухгалтер / база клиентов Компании	42	1	1	?
Финансовый директор / база клиентов Компании	42	1	-	?
Бухгалтер / база данных наименований товаров Компании	30	1	1	?

Компетентностно-ориентированная задача № 7

В качестве входной информации берется текстовый файл, состоящий из ФИО студента, названия кафедры и специальности. Исходный поток данных соответствует последовательности бит, расположение которых

определяется формулой, учитывающей порядковый номер студента по списку:

$$ci = (7i+n) \bmod 13 + 13i$$

Ключ скремблера соответствует номеру зачетки студента «слева направо», генератор псевдослучайных чисел - аналогично «справа налево». Порядок выполнения работы:

1) Рассчитать период зацикливания и период наибольшей длины скремблера

2) Произвести скремблирование исходных данных

3) Подобрать скремблер минимальной разрядности, который не зациклится при обработке всего исходного файла.

Компетентностно-ориентированная задача № 8

Определите риск по угрозе конфиденциальность:

	Итоговая вероятность	Ущерб от реализации угрозы	Риск
Бухгалтерский отчет	0,0252	100	?
База клиентов Компании	0,0331	100	?
База данных наименований товаров Компании	0,0231	100	?

Компетентностно-ориентированная задача № 9

Для каждого вида угроз: умышленные несанкционированные действия людей, непредвиденные случайности, ошибки со стороны персонала, аварии оборудования, программного обеспечения и средств связи. Относящиеся к каждому типу негативных воздействий уровни рисков, соответствующих показателям ценности ресурсов, показателям угроз и уязвимостей, оценить при помощи таблицы 1.

Таблица 1. Уровни рисков, соответствующие показателям ценности ресурсов, угроз и уязвимостей

Показатель ценности ресурса	Уровень угрозы (оценка вероятности ее осуществления)								
	_____Уровень			_____ уровень			____уровень		
	Уровни уязвимостей								
	?	?	?	?	?	?	?	?	?
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6

3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Компетентностно-ориентированная задача № 10

Опишите технологию создания и управления учетными записями пользователей. Создайте учетные записи для двух разных пользователей. Для одного пользователя проверьте действенность флажка – требования смены пароля пользователя при следующей регистрации в системе, для другого – запрет на изменение пароля пользователем. Создайте локальную группу.

Поместите в локальную группу созданных вами пользователей и административного пользователя. Проделайте это двумя способами: через окно свойств группы и окно свойств пользователя.

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.