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

Программно-аппаратные средства защиты информации
(наименование учебной дисциплины)

10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий»
(код и наименование ОПОП ВО)

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

Тема 1. Введение.

1. Предмет и задачи изучения дисциплины
2. Необходимость использования дополнительных программных и аппаратных СЗИ
3. Требования руководящих органов по использованию программно-аппаратных СЗИ

Тема 2. Доступ к данным. Идентификация и аутентификация субъектов доступа.

1. Процедура доступа к данным в современных компьютерных системах
2. Как осуществляется выбор объекта для доступа
3. Форма хранения прав доступа субъектов к объектам
4. Средства осуществления доступа к объектам со стороны пользователей

Тема 3. Аппаратная идентификация пользователей.

1. Причины использования аппаратной идентификации пользователей в компьютерных системах
2. Виды аппаратных идентификаторов, присутствующих на рынке, их характеристики и области применения
3. Технологии биометрической идентификации пользователей (перечислить)
4. Области использования различных систем биометрической идентификации

Тема 4. Технологии аутентификации.

1. Термины и определения
2. Виды аутентификации
3. Преимущества и недостатки одного из методов аутентификации
4. Пример практической реализации одного из методов аутентификации
5. Предложите схему интеграции одного из методов аутентификации в существующую информационную систему

Тема 5. Системы аппаратной поддержки механизмов разграничения доступа.

1. Варианты реализации средств аппаратной поддержки механизмов обеспечения ИБ
2. Пример использования аппаратной идентифкации пользователя

3. Существующие на рынке решения, использующие механизмы аппаратной поддержки механизмов разграничения доступа

Тема 6. Принципы организации контроллера защиты информации.

1. Назначение контроллера защиты информации
2. Преимущества и недостатки использования контроллеров защиты информации
3. Интеграция контроллера ЗИ в компьютерную систему
4. Дополнительные функции, возникающие у СЗИ с использованием контроллеров ЗИ
5. Области применения контроллеров ЗИ
6. Назовите факторы, препятствующие использованию контроллеров ЗИ

Тема 7. Аппаратные системы разграничения доступа.

1. Примеры аппаратных систем разграничения доступа
2. Предложите вариант реализации исключительно аппаратной СЗИ для защиты определённого компонента компьютерной системы
3. Недостатки аппаратных СЗИ
4. Трудности интеграции аппаратных СЗИ в существующие информационные системы
5. Предложите модель злоумышленника и модель нарушителя, для нейтрализации которых требуются аппаратные СЗИ
6. Предложите модель злоумышленника в систем с использованием исключительно аппаратного СЗИ

Тема 8. Программно – аппаратные криптосистемы. Технологии шифрования.

1. Технологии шифрования (перечислить, указать области примененния)
2. Существующие на рынке решения в области криптографической защиты информации
3. Дать сравнительные характеристики программных и аппаратных криптосистем
4. Предложите модель угроз для программной и аппаратной СЗИ

Тема 9. Защита программ от несанкционированного копирования

Классификация методов защиты программного обеспечения от копирования

1. Предложите оптимальные варианты реализации схемы защиты от копирования для: прикладной программы, программы математического моделирования, операционной системы, программного СЗИ
2. Трудности использования средств защиты от копирования
3. Критерии выбора средств защиты ПО от несанкционированного копирования

Тема 10. Защита программ от изучения.

1. Правовые основы защиты программного обеспечения от изучения
2. Модель нарушителя целостности и конфиденциальности программного кода
3. Средства изучения программного кода
4. Последствия взлома программного обеспечения
5. Методы противодействия изучению и отладке программного обеспечения
6. Правовые основы использования антиотладочных средств
7. Устранение человеческого фактора при проектировании защищённого программного обеспечения

Тема 11. Деструктивные программные воздействия.

1. Классифицируйте деструктивные программные воздействия по методам реализации угроз безопасности
2. Опасность самореплицирующихся программ
3. Классификация разработчиков деструктивного программного беспечения
4. Классификация компьютерных вирусов
5. Классификация программ-шпионов
6. Организационные меры противодействия деструктивным программным воздействиям
7. Технические средства противодействия деструктивным программным воздействиям различных типов
8. Классифицируйте разработчиков деструктивного программного обеспечения

Тема 12. Кейлоггеры.

1. Угрозы безопасности, исходящие от кейлоггеров
2. Типы программных кейлоггеров
3. Оцените опасность различных типов кейлоггеров
4. Создайте модель злоумышленника, реализующего различные типы кейлоггеров
5. Меры борьбы с программными кейлоггерами различных типов
6. Опасность аппаратных кейлоггеров
7. Предложите организационные меры борьбы с аппаратными кейлоггерами
8. Технические меры противодействия аппаратным кейлоггерам

Критерии оценки:

- 2 балла по шкале БРС выставляется обучающемуся, если даны точные ответы, демонстрируется знание дополнительной литературы и материала, не раскрытого на лекции;

- 1 балла по шкале БРС выставляется обучающемуся, если имеется знание терминов и понятий, понимаются основные взаимосвязи процессов и явлений;
- 0 балла по шкале БРС выставляется обучающемуся, отсутствует знание базовых терминов и понятий, отсутствие понимания взаимосвязи понятий.

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ЛАБОРАТОРНЫХ РАБОТ

Лабораторная работа № 1

1. Для чего предназначена система Secret Net Studio?
2. Какие существуют группы функциональных компонентов клиентской части СЗИ SecretNet?
3. Что такое базовая защита в системе Secret Net Studio?
4. Для чего служит подсистема локальной аутентификации в системе Secret Net Studio ?

Лабораторная работа №2

1. Что требуется для функционирования серверной части СЗИ SecretNet ?
2. Какие действия необходимо выполнить перед установкой компонентов Secret Net Studio для централизованного управления?
3. Что необходимо предпринять при установке в системе первого сервера безопасности?
4. Для чего предназначен домена безопасности?

Лабораторная работа №3

1. Каково назначение СЗИ DallasLock 8.0 ?
2. Назовите основные компоненты структуры
3. За что отвечает подсистема обнаружения вторжений назначение СЗИ DallasLock 8.0?
4. За что отвечает подсистема контроля целостности назначение СЗИ DallasLock 8.0?

Лабораторная работа №4

1. Идентификация и аутентификации пользователя это?
2. Путём каких процедур должна быть выполнена любая доверенная загрузка?
3. Назовите порядок использования идентификаторов
4. Какие особенности у архитектуры СЗИ НСД Аккорд-АМДЗ?

Лабораторная работа №5

a. Кратко опишите функцию управления входом пользователя Secret Net Studio в ПАК "Соболь" с помощью идентификатора,

инициализированного и присвоенного пользователю в системе Secret Net Studio

b. Перечислите перечень используемых ключей шифрования Для обеспечения защиты данных в процессе централизованного управления ПАК "Соболь" в Secret Net Studio?
c. Каково назначение симметричного ключв ЦУ ?
d. Дайте определение термина - Аутентификатор .

Лабораторная работа №6

1.Что такое структура?
2.Назовите классификации ЭВМ
3.Разделите классификацию ЭВМ на три группы
4.Производительность ЭВМ это

Лабораторная работа №7

1. Для чего необходима отладка программных средств?
2. Какие существуют методы и средства отладки программ?
3. Чем отличаются отладчики уровня пользователя от отладчиков уровня ядра?
4. Назовите выполняемые программными системами защиты информации машинные команды, которые являются наиболее критичными с точки зрения обеспечения информационной безопасности
5. Назовите основные приѐмы изменения хода исполнения программ
6. Что такое патч и каким образом происходит его создание?

Критерии оценки:

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

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

1 балл (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит

недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

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

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1. Возможность за приемлемое время получить требуемую информационную услугу называется:

1. Конфиденциальность
2. Доступность
3. Целостность
4. Непрерывность

2. К аспектам информационной безопасности не относится:

1. Доступность
2. Целостность
3. Конфиденциальность
4. Защищенность

3. По каким критериям нельзя классифицировать угрозы:

1. по расположению источника угроз
2. по аспекту информационной безопасности, против которого угрозы направлены в первую очередь
3. по способу предотвращения
4. по компонентам информационных систем, на которые угрозы нацелены

4. Главное достоинство парольной аутентификации – …

1. простота
2. надежность
3. секретность
4. запоминаемость

5. Сколько уровней включает в себя сетевая модель OSI?

1. 5
2. 7

3. 6
4. 8

6. Межсетевой экран (Брандмауэр, firewall) – это…
1. Комплекс аппаратных средств
2. Комплекс программных средств
3. Комплекс аппаратных или программных средств
4. Комплекс аппаратных и программных средств

7. На каком уровне сетевой модели OSI не работает межсетевой экран:
1. Физический
2. Сеансовый
3. Сетевой
4. Транспортный

8. Межсетевого экрана какого класса не существует:
1. экранирующий маршрутизатор
2. экранирующий коммутатор
3. экранирующий транспорт
4. экранирующий шлюз

9. Что из перечисленного не входит в состав программного комплекса антивирусной защиты:
1. Подсистема сканирования
2. Подсистема управления
3. Подсистема обнаружения вирусной активности
4. Подсистема устранения вирусной активности

10. На каком этапе заканчивается жизненный цикл автоматизированной системы?
1. Бета-тестирование системы
2. Внедрение финальной версии системы в эксплуатацию
3. Прекращение сопровождения и технической поддержки системы
4. Альфа-тестирование системы

11. Какие задачи выполняет теория защиты информации:
1. предоставлять полные и адекватные сведения о происхождении, сущности и развитии проблем защиты
2. аккумулировать опыт предшествующего развития исследований, разработок и практического решения задач защиты информации
3. формировать научно обоснованные перспективные направления развития теории и практики защиты информации
4. выполняет все вышеперечисленные

12. Какой из протоколов не относится к протоколам защищенной передачи данных в сети Интернет:
1. SSL
2. SET
3. HTTP
4. IPSec

13. Какого метода разграничения доступа не существует:
1. разграничение доступа по спискам
2. разграничение доступа по уровням секретности и категориям
3. локальное разграничение доступа
4. парольное разграничение доступа

14. К основным функциям подсистемы защиты операционной системы относятся:
1. идентификация, аутентификация, авторизация, управление политикой безопасности и разграничение доступа
2. криптографические функции
3. сетевые функции
4. все вышеперечисленные

15. Ценность информации определяется:
1. степенью ее полезности для владельца
2. истинностью или достоверностью
3. конфиденциальностью

16. Объектом защиты информации является:
1. работа, посвященная защите информации в автоматизированных системах
2. компьютерная система или автоматизированная система обработки данных
3. комплекс средств, предназначенных для автоматизированного сбора

17. Компьютерная система- это...
1. вычислительные комплексы и системы
2. вычислительные сети
3. комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации

18. Под системой защиты информации в КС понимается:
1. состояние всех компонент компьютерной системы, при котором обеспечивается за-щита информации от возможных угроз на требуемом уровне

2. одно из основных направлений обеспечения безопасности государства, отрасли, ведомства, государственной организации или частной фирмы
3. единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности

19. Сеть ЭВМ - это...
1. процессы сбора, обработки, накопления, хранения, поиска и распространения информации
2. это совокупность ЭВМ, взаимосвязанных каналами передачи данных, и необходимых для реализации этой взаимосвязи программного обеспечения и (или) технических средств, предназначенных для организации распределенной обработки данных
3. информация, возникающая в ходе ведения разговоров, работы систем связи, звуко - усиления и звуковоспроизведения

20. Под информационной системой понимают:
1. упорядоченную совокупность документов и массивов документов и информационных технологий, реализующих информационные процессы
2. процессы сбора, обработки, накопления, хранения, поиска и распространения информации
3. информация циркулирует в технических средствах обработки и хранения информации, а также в каналах связи при ее передаче

21. Информационными ресурсами называют:
1. процесс создания оптимальных условий для удовлетворения информационных потребностей граждан, организаций, общества и государства в целом
2. документы и массивы документов, существующие отдельно или в составе информационных систем
3. государственные тайны и конфиденциальную информацию

22. Разглашение - это...
1. доведение защищаемой информации до неконтролируемого количества получателей информации
2. получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней
3. деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

23. Несанкционированное воздействие на защищаемую информацию - это…
1. предотвращение ущерба собственнику, владельцу или пользователю информации

2. совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации
3. воздействие с нарушением правил ее изменения

24. Шифрованием информации называют:
1. процесс ее преобразования, при котором содержание информации становится не-понятным для не обладающих соответствующими полномочиями субъектов
2. известность ее содержания только имеющим соответствующие полномочия субъектам
3. совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации

25. Политика безопасности - это...
1. состояние защищенности информационной среды, обеспечивающее ее формирование и развитие
2. это набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа
3. это известность ее содержания только имеющим соответствующие полномочия субъектам
4. основное устройство системы, производящее идентификацию пользователя и дающее разрешение на проход, в случае если считанный с идентификатора код совпадает с кодом, хранящимся в памяти контроллера
5. это набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа
6. это известность ее содержания только имеющим соответствующие полномочия субъектам

26. Основной характеристикой контроллера являются:
1. комбинированные методы
2. поддерживаемые режимы работы - автономный или сетевой через линию связи с использованием компьютера
3. при помощи особых устройств, генерирующих модулированный ультразвуковой, инфракрасный или радиосигнал

27. Идентификация - это...
1. пользователь подтверждает идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе
2. информационных ресурсов, систем и технологий является субъект с полномочиями владения и пользования указанными объектами. Под пользователем информации будем понимать субъекта, обращающегося к

информационной системе за получением необходимой ему информации и пользующегося ею
3. пользователь сообщает системе по ее запросу свое имя

28. Основной недостаток подобных систем аутентификации:
1. информацией в данном случае служит ключ, на котором выполняется шифрование случайного числа. Как видно из схемы обмена, данный ключ никогда не передается по сети, а лишь участвует в вычислениях, что составляет несомненное преимущество протоколов данного семейства
2. необходимость иметь на локальном компьютере клиентский модуль, выполняющий шифрование
3. сервер расшифровывает полученную информацию на том же ключе и сравнивает с исходным случайным числом

29. Самый главный недостаток протокола Kerberos:
1. необходимость в нескольких специальных серверах
2. В случае успешной проверки билета сервер TGS генерирует еще один случайный ключ для шифрования сеансов связи между пользователем, желающим получить доступ, и целевым сервером
3. необходимость иметь на локальном компьютере клиентский модуль, выполняющий шифрование

30. Выбрать правильный ответ, характеризующий протокол идентификации CHAP:
1. проверяющая система отправляет запрос удаленному устройству, которое запросило подключение к сети
2. применяет простую процедуру двустороннего обмена для идентификации систем
3. использует специальный алгоритм для расчета значения, известного только прове-ряющей системе и удаленному устройству

31. Хешированием информации называют
1. способность обеспечения беспрепятственного доступа субъектов к интересующей их информации
2. состояние защищенности информационной среды, обеспечивающее ее формирование и развитие
3. процесс ее преобразования в хеш -значение фиксированной длины

32. Множество объектов и типов доступа к ним субъекта может изменяться:
1. в соответствии с некоторыми правилами, существующими в данной системе
2. статично т.е. не может изменяться вообще
3. это никак не связано с субъектами

33. Основой избирательной политики безопасности является избирательное управление доступом, которое подразумевает, что:
1. все субъекты и объекты системы должны быть идентифицированы
2. права доступа субъекта к объекту системы определяются без правил
3. все субъекты и объекты системы должны быть не аутентифицированы

34. Избирательное управление доступом:
1. концепция доступа субъектов к информационным ресурсам по грифу секретности разрешенной к пользованию информации, определяемому меткой секретности
2. метод управления доступом субъектов системы к объектам, основанный на идентификации и опознавании пользователя, процесса и/или группы, к которой он принадлежит
3. в метод управления доступом субъектов системы к объектам, основанный на опознавании пользователя без любой регистрации

35. Мандатное управление доступом:
1. метод управления доступом субъектов системы к объектам, основанный на идентификации и опознавании пользователя, процесса и/или группы, к которой он принадлежит
2. метод доступа субъектов к информационным ресурсам с полной разрешенностью к пользованию информаци
3. концепция доступа субъектов к информационным ресурсам по грифу секретности разрешенной к пользованию информации, определяемому меткой секретности

36. Матрица доступа представляет собой:
1. прямоугольную матрицу, в которой объекту системы соответствует строка, а субъекту столбец
2. треугольную матрицу, в которой объекту системы соответствует столбец, а субъекту строка
3. квадратную матрицу, в которой объекту системы соответствует строка, а субъекту столбец

37. Что является копированием документов?

1. Контактное или бесконтактное подсоединение к различного рода линиям и проводам с целью несанкционированного доступа к информации, образующейся или передаваемой в них тем или иным путем;

2. Получение разведывательной информации за счет приема сигналов электромагнитной энергии пассивными средствами приема, расположенными, как правило, на достаточно безопасном расстоянии от источника конфиденциальной информации;

3. Получения информации, к которой субъект не допущен, но при определенных условиях он может получить возможность узнать ее.

4. Процесс изготовления копий с оригиналов;

38. От чего зависит эффективность обнаружения и распознавания объектов:

1. Яркость объекта;

2. Контраст объекта/фона;

3. Угловой размер объекта;

4. Угловой размер поля обзора;

5. Временя наблюдения объекта;

6. Все вышеперечисленное.

39. Что такое просветление?

1.Способы уменьшения отражения света от поверхности стекла путем нанесения на него тонкой пленки с коэффициентом преломления меньше преломления стекла линзы.

2. Способность объектива передавать мелкие детали изображения

3. способности объектива передавать контраст деталей объекта и измеряется отношением контрастности деталей определенных размеров на изображении и на объекте.

4. величиной геометрического относительного отверстия, равного к=D/F, где D-диаметр входного отверстия объектива (апертура), F-фокусное расстояние

40. Что относится к условиям наблюдения за объектом:

1. Высокая проникающая способность световых лучей в видимом диапазоне;

2. Сильная зависимость условий наблюдения от состояния атмосферы климатических и погодных условий;

3. Увеличение поля обзора;

4. Низкая контрастность объекта с окружающим фоном

41. Как называется совокупность условий и факторов, создающих потенциальную угрозу или реально существующую опасность нарушения безопасности информации?

1. атака

2. угроза
3. источник угрозы
4. цель злоумышленника

42. Как называется совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация?

1. несанкционированный канал утечки информации
2. технический канал утечки информации
3. параметрический канал утечки информации
4. физический канал утечки информации

43.Что является носителем информации в оптическом канале утечки информации?

1. акустическая волна
2. электрическое поле
3. электромагнитное поле
4. световая волна

44.В каком техническом канале утечки информации носителем является упругая акустическая волна?

1. оптический
2. акустический
3. материально-вещественный
4. радиоэлектронный

45.Как называется технический канал утечки информации, заключающийся в перехвате электромагнитных излучений на частотах работы передатчиков систем и средств связи?

1. электромагнитный
2. электрический
3. индукционный

46. Техническая разведка (при классификации по физической природе носителя информации) состоит из следующих видов:

1. радиационная разведка (носитель – излучения радиоактивных веществ);
2. радиоэлектронная разведка (носитель – электромагнитное поле в радиодиапазоне или электрический ток);
3. химическая разведка (носитель – частицы веществ);
4. все вышеперечисленное

47. Технология добывания информации предусматривает следующие этапы:
1. организация добывания;
2. организация добывания, добывание данных и сведений;
3. организация добывания, добывание данных и сведений, информационная работа.

48. Технические демаскирующие признаки можно разделить на:
1. прямые демаскирующие признаки
2. косвенные демаскирующие признаки
3. альтернативные демаскирующие признаки

49. Основными источниками информации являются следующие:
1. люди;
2. интеллектуальные средства обработки информации;
3. черновики и отходы производства;
4. все вышеперечисленное

50. Выберите верные варианты видов носителей информации:
1. люди;
2. материальные тела (макрочастицы);
3. поля;
4. элементарные частицы (микрочастицы).

51. Из известных полей в качестве носителей применяются:

1. акустические;
2. акустические, электрические;
3. акустические, электрические, магнитные и электромагнитные (в диапазоне видимого и инфракрасного света, в радиодиапазоне).

52. Процессы памяти. Выберите верные варианты:
1. запоминание
2. сохранение
3. воспроизведение
4. забывание

53. По степени активности протекания процесса принято выделять 2 вида запоминания:
1. преднамеренное, случайное
2. непреднамеренное
3. преднамеренное, непреднамеренное
4. случайное

54. Классификация памяти по продолжительности сохранения информации:
1. мгновенная память
2. кратковременная память
3. оперативная память
4. долговременная память

55. К биометрической системе защиты относятся:

1. антивирусная защита
2. защита паролем
3. идентификация по отпечаткам пальцев
4. физическая защита данных

56. Какой из биометрических методов относится к «динамическим методам»?
1. по почерку
2. по отпечатку пальца
3. по рисунку радужной оболочки глаза
4. по форме ладони

57. Что такое информационная война?
1. это действия, предпринятые для достижения информационного превосходства путем нанесения ущерба информации, процессам, основанным на информации, и информационным системам противника при одновременной защите собственной информации, процессов, основанных на информации, и информационных систем
2. это совокупность технических и программных средств хранения, обработки и передачи информации, а также политические, экономические и культурные условия реализации процессов информатизации
3. это совокупность законов, нормативных актов и других форм правового регулирования в сфере обращения и производства информации и применения ИКТ

58. Как называется бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена?
1. угроза
2. утечка
3. уязвимость
4. атака

59. В каком техническом канале утечки информации в качестве носителей выступают электрические, электромагнитные и магнитные поля?

1. оптический
2. радиоэлектронный
3. акустический
4. материально-вещественный

60. В каких целях осуществляется контроль излучений радиоэлектронных средств и (или) высокочастотных устройств?

1. в целях проверки соблюдения пользователем радиочастотным спектром правил его использования
2. в целях выявления не разрешенных для использования радиоэлектронных средств и прекращения их работы
3. в целях выявления источников радиопомех
4. в целях выявления нарушения порядка и правил использования радиочастотного спектра, национальных стандартов, требований к параметрам излучения (приема) радиоэлектронных средств и (или) высокочастотных устройств

61. Средства связи, иные радиоэлектронные средства и высокочастотные устройства, являющиеся источниками электромагнитного излучения:

1. вопрос о регистрации решается каждой организацией самостоятельно, но регистрация рекомендуема
2. не подлежат регистрации
3. подлежат регистрации

62. Какие преимущества имеет квантовый компьютер в сравнении с классическим компьютером:

1. Может иметь память экспоненциально большого размера.
2. Любой алгоритм для квантового компьютера эффективнее алгоритма для классического компьютера.
3. Некоторые алгоритмы для квантового компьютера эффективнее соответствующих алгоритмов для классического компьютера.
4. Может параллельно выполнять массивные вычисления.

63. Какие недостатки имеет квантовый компьютер в сравнении с классическим компьютером:

1. Не может иметь память большого размера.
2. Чтение состояния кубита разрушает это состояние.

3. Корректный ответ можно получить лишь с некоторой вероятностью.
4. Не способен выполнять параллельные вычисления.

64. Какие утверждения справедливы относительно понятия «кубит»:
1. Это кубический бит.
2. Единица памяти квантового компьютера.
3. Может рассматриваться как вектор единичной длины на плоскости.

65. Какие значения может хранить кубит:
1. Только 0 и 1.
2. Любые положительные значения.
3. Любые значения от 0 до 1 включительно.

66. Укажите корректные высказывания:

1.Квантовые процессоры должны быть полностью изолированы от окружающей среды, сохраняя при этом контроль и управление вычислениями.
2.Значение кубита можно интерпретировать как суперпозицию с весами a и b значений двух классических битов 0 и 1.
3.Технология создания квантовых компьютеров хорошо проработана, а теоретическая база (физика и математика) недостаточно.

67. Инженерно-техническая защита решает задачи по предотвращению или уменьшению угроз, вызванных:

1. Попытками злоумышленников проникнуть к местам хранения источников информации
2. Организованной или случайной утечкой информации с использованием различных технических средств
3. Стихийными носителями угроз
4. Нет верного ответа

68. Цели инженерно-технической защиты информации:

1. Предотвращение проникновения злоумышленника к источникам информации с целью уничтожения, хищения или изменения
2. Защита носителей информации от уничтожения в результате различных природных и техногенных воздействий
3. Выполнение анализа рисков внедрения
4. Предотвращение утечки информации по различным техническим каналам

69. По функциональному назначению средства инженерно-технической защиты подразделяются на следующие группы:

1. Инженерные, аппаратные
2. Аппаратные, криптографические
3. Инженерные, программные, криптографические

Инженерные, аппаратные, программные, криптографические

70. Основные факторы, влияющие на эффективность защиты информации от угроз воздействия:

1. Предотвращение и нейтрализация преднамеренных и случайных воздействий на источник информации
2. Изучение условий образования технического канала утечки информации
3. Вероятность распознавания объекта защиты по добываемым признакам
4. Скрытие информации и ее носителей от органа разведки на всех этапах добывания информации

71. Что относится к физической защите ИТЗИ:

1. Инженерная защита
2. Маскировка
3. Пространственное скрытие
4. Дезинформирование

72. Дезинформирование – это:

1. Особый тип информации, формирующей неверное сознание, порождающее неадекватные стремления и формы поведения, что соответствует замыслу дезинформатора
2. Неадекватная информация, которая формирует неверную картину действительности
3. Способ манипуляции, заключающейся в снабжении заведомо ложной, неполной, либо устаревшей информацией, в результате чего объект дезинформирования принимает решение в интересах манипулятора
4. Это отсутствие информации

73. Чем обусловлена утечка информации в электромагнитных каналах?

1. Излучения элементов ТСПИ
2. Излучения на частотах работы высокочастотных (ВЧ) генераторов ТСПИ
3. Излучения на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ.
4. Нет верного ответа

74. Какие причины утечки информации по цепям заземления?

1. Побочные электромагнитные излучения
2. Наведение в цепях заземления ЭДС полями побочных электромагнитных излучений
3. Протекание тока заземления по контуру заземления
4. Экранирование электрического поля заземления

75. Чем обусловлены наводки в сети электропитания?

1. Наводки возникают от работы электрических машин и электронных устройств
2. Наводки возникают от техногенных влияний
3. Наводки возникают от воздействия электрических, магнитных или электромагнитных полей, электрических токов или напряжений внешнего или внутреннего источника
4. Наводки возникают от внешних и внутренних факторов

76. Примеры полупроводниковых носителей информации.

1. Жесткие диски
2. CD-ROM
3. SSD диск
4. Дискеты

77. Возможность за приемлемое время получить требуемую информационную услугу называется:
1. Конфиденциальность
2. Доступность
3. Целостность
4. Непрерывность

78. К аспектам информационной безопасности не относится:
1. Доступность
2. Целостность
3. Конфиденциальность
4. Защищенность

79. По каким критериям нельзя классифицировать угрозы:
1. по расположению источника угроз
2. по аспекту информационной безопасности, против которого угрозы направлены в первую очередь
3. по способу предотвращения
4. по компонентам информационных систем, на которые угрозы нацелены

80. Главное достоинство парольной аутентификации – …
1. простота
2. надежность
3. секретность
4. запоминаемость

81. Сколько уровней включает в себя сетевая модель OSI?
1. 5
2. 7
3. 6
4. 8

82. Межсетевой экран (Брандмауэр, firewall) – это…
1. Комплекс аппаратных средств
2. Комплекс программных средств
3. Комплекс аппаратных или программных средств
4. Комплекс аппаратных и программных средств

83. На каком уровне сетевой модели OSI не работает межсетевой экран:
1. Физический
2. Сеансовый
3. Сетевой
4. Транспортный

84. Межсетевого экрана какого класса не существует:
1. экранирующий маршрутизатор
2. экранирующий коммутатор
3. экранирующий транспорт
4. экранирующий шлюз

85. Что из перечисленного не входит в состав программного комплекса антивирусной защиты:
1. Подсистема сканирования
2. Подсистема управления
3. Подсистема обнаружения вирусной активности
4. Подсистема устранения вирусной активности

86. На каком этапе заканчивается жизненный цикл автоматизированной системы?

1. Бета-тестирование системы
2. Внедрение финальной версии системы в эксплуатацию
3. Прекращение сопровождения и технической поддержки системы
4. Альфа-тестирование системы

87. Какие задачи выполняет теория защиты информации:
1. предоставлять полные и адекватные сведения о происхождении, сущности и развитии проблем защиты
2. аккумулировать опыт предшествующего развития исследований, разработок и практического решения задач защиты информации
3. формировать научно обоснованные перспективные направления развития теории и практики защиты информации
4. выполняет все вышеперечисленные

88. Какой из протоколов не относится к протоколам защищенной передачи данных в сети Интернет:
1. SSL
2. SET
3. HTTP
4. IPSec

89. Какого метода разграничения доступа не существует:
1. разграничение доступа по спискам
2. разграничение доступа по уровням секретности и категориям
3. локальное разграничение доступа
4. парольное разграничение доступа

90. К основным функциям подсистемы защиты операционной системы относятся:
1. идентификация, аутентификация, авторизация, управление политикой безопасности и разграничение доступа
2. криптографические функции
3. сетевые функции
4. все вышеперечисленные

91. Ценность информации определяется:
1. степенью ее полезности для владельца
2. истинностью или достоверностью
3. конфиденциальностью

92. Объектом защиты информации является:

1. работа, посвященная защите информации в автоматизированных системах
2. компьютерная система или автоматизированная система обработки данных
3. комплекс средств, предназначенных для автоматизированного сбора

93. Компьютерная система- это...
1. вычислительные комплексы и системы
2. вычислительные сети
3. комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации

94. Под системой защиты информации в КС понимается:
1. состояние всех компонент компьютерной системы, при котором обеспечивается за-щита информации от возможных угроз на требуемом уровне
2. одно из основных направлений обеспечения безопасности государства, отрасли, ведомства, государственной организации или частной фирмы
3. единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности

95. Сеть ЭВМ - это...
1. процессы сбора, обработки, накопления, хранения, поиска и распространения информации
2. это совокупность ЭВМ, взаимосвязанных каналами передачи данных, и необходимых для реализации этой взаимосвязи программного обеспечения и (или) технических средств, предназначенных для организации распределенной обработки данных
3. информация, возникающая в ходе ведения разговоров, работы систем связи, звуко - усиления и звуковоспроизведения

96. Под информационной системой понимают:
1. упорядоченную совокупность документов и массивов документов и информационных технологий, реализующих информационные процессы
2. процессы сбора, обработки, накопления, хранения, поиска и распространения информации
3. информация циркулирует в технических средствах обработки и хранения информации, а также в каналах связи при ее передаче

97. Информационными ресурсами называют:
1. процесс создания оптимальных условий для удовлетворения информационных потребностей граждан, организаций, общества и государства в целом

2. документы и массивы документов, существующие отдельно или в составе информационных систем
3. государственные тайны и конфиденциальную информацию

98. Разглашение - это...
1. доведение защищаемой информации до неконтролируемого количества получателей информации
2. получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней
3. деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

99. Несанкционированное воздействие на защищаемую информацию - это…
1. предотвращение ущерба собственнику, владельцу или пользователю информации
2. совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации
3. воздействие с нарушением правил ее изменения

100. Шифрованием информации называют:
1. процесс ее преобразования, при котором содержание информации становится не-понятным для не обладающих соответствующими полномочиями субъектов
2. известность ее содержания только имеющим соответствующие полномочия субъектам
3. совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации

Задания в открытой форме

1. Идентификация – это…
2. Аутентификация-это…
3. Ядро безопасности-это…
4. Ядро системы защиты представляет собой…
5. Подсистема регистрации является…
6. Подсистема управления представляет средства…
7. База данных СЗИ предназначена для…
8. Механизм замкнутой программной среды позволяет ……
9. Функциональный контроль предназначен для…
10. PTS StrongDisk позволяет располагать …
11. Метод экспериментов заключается в проведении …

12. Логические бомбы -это…
13. Червями называются…
14. Троянские кони-это…
15. Программы шпионы-это…
16. Программы показа рекламы-это…
17. Программы удаленного доступа-это…
18. Сетевые вирусы используют для своего распространения …
19. Самошифрование и полиморфичность используются …
20. Криптография занимается…

Задания на установление соответствия

1. Установите взаимно однозначное соответствие

1	Идентификация	А	Может быть охарактеризован тем, какой пользователь обращается
2	Аутентификация	Б	Процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации – за счѐт этого каждый субъект или объект системы должен быть однозначно идентифицируем.
3	Запрос на доступ к ресурсу	В	Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа к ресурсу)

2. Установите взаимно однозначное соответствие функции памяти

1	Proximity	А	Чтение/Запись
2	Стандарт ISO/IEC 14443	Б	Чтение/Запись
3	Стандарт ISO/IEC 15693	В	Только чтение

3. Установите взаимно однозначное соответствие

1	аутентификации Kerberos	А	Принимает от пользователей запросы на аутентификацию
2	аутентификации RADIUS	Б	Был разработан специально для того, чтобы обеспечить надежную аутентификацию пользователей
3	Клиент RADIUS	В	рассматривается как механизм аутентификации и авторизации удалѐнных пользователей в условиях распределѐнной сетевой инфраструктуры, предоставляющий централизованные услуги по проверке подлинности и учѐту для служб удалѐнного доступа
4	Сервер RADIUS	Г	Заключается в централизованной обработке информации, предоставленной клиентами

4. Установите взаимно однозначное соответствие методы реализации систем одноразовых паролей

1	Метод "запрос-ответ"	А	В качестве исходной строки в нем используется не время, а количество успешных процедур аутентификации, проведенных до текущей
2	Метод "только ответ"	Б	В начале процедуры аутентификации пользователь отправляет на сервер свой логин. В ответ на это последний генерирует некую случайную строку и посылает ее обратно.
3	Метод "синхронизация по времени"	В	При этом в процессе создания строки используется значение предыдущего запроса

4	Метод "синхронизация по событию"	Г	При этом обычно используется не точное указание времени, а текущий интервал с установленными заранее границами (например, 30 секунд).

5. Установите взаимно однозначное соответствие

1	Ядро безопасности	А	Является одним из элементов ядра системы и предназначена для управления регистрацией в журнале событий, связанных с работой системы защиты
2	Ядро системы защиты	Б	локализованная, чѐтко ограниченная, изолированная совокупность программных и аппаратных механизмов, правильно реализующих функцию диспетчера доступа
3	Подсистема регистрации	В	Предоставляет средства для настройки защитных механизмов системы
4	Подсистема управления	Г	Представляет собой программу, которая автоматически запускается на защищаемом компьютере при его включении и функционирует на протяжении всего времени работы компьютера

6. Установите взаимно однозначное соответствие

1	Замкнутая программная среда	А	Предназначен для обеспечения гарантии того, что к моменту завершения загрузки ОС все ключевые компоненты СЗИ загружены и функционируют. Функциональный контроль осуществляется перед входом пользователя в

			систему
2	Функциональный контроль	Б	Предназначена для комплексной защиты информационных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах
3	Подсистема контроля аппаратной конфигурации компьютера	В	Позволяет сформировать для любого пользователя компьютера программную среду, определив индивидуальный перечень программ, разрешенных для запуска
4	СЗИ «Страж NT 2.0»	Г	Предназначена для своевременного обнаружения изменений в аппаратной конфигурации компьютера и реагирования на эти изменения и поддержания в актуальном состоянии списка устройств компьютера.

7. Установите взаимно однозначное соответствие

1	Пофайловое шифрование	А	Если зашифрован весь диск целиком, то операционная система не сможет запуститься, пока какой-либо механизм не расшифрует файлы загрузки
2	Шифрование каталогов	Б	Пользователь сам выбирает файлы, которые следует зашифровать
3	Шифрование виртуальных дисков	В	Пользователь создает папки, все данные в которых шифруются автоматически
4	Защита процесса загрузки	Г	Концепция виртуальных дисков реализована в некоторых утилитах компрессии, например

			Stacker или Microsoft DriveSpace

8. Установите взаимно однозначное соответствие

1	Контроль входа на компьютер	А	Это не позволит злоумышленнику в ваше отсутствие изменить какие-либо данные.
2	Контроль целостности файлов операционной системы	Б	При включении ПК устройство требует от пользователя ввести персональную информацию (например, вставить дискету с ключами)
3	Блок управления	В	Через него осуществляется основной обмен данными между устройством и компьютером.
4	Контроллер системной шины ПК	Г	основной модуль шифратора, который управляет работой всех остальных

9. Установите взаимно однозначное соответствие

1	Энергонезависимое запоминающее устройство	А	набор регистров, сумматоров, блоков подстановки и прочих элементарных схем, связанных между собой шинами передачи данных
2	Шифропроцессор	Б	обычно на базе микросхем флэш-памяти
3	Вычислитель	В	аппаратно реализованная программа (комбинационная схема конечного автомата), управляющая вычислителем
4	Блок управления	Г	специализированная микросхема или микросхема программируемой логики PLD

10. Установите взаимно однозначное соответствие

1	Несанкционированные	А	Процессы,

	(сторонние) процессы		содержащие ошибки, ставшие известными, использование которых позволяет осуществить НСД к информации.
2	Критичные процессы	Б	Это процессы, которые не требуются пользователю для выполнения своих служебных обязанностей и могут несанкционированно устанавливаться на компьютер (локально, либо удаленно) с различными целями, в том числе, и с целью осуществления НСД к информации
3	Скомпрометированные процессы	В	К этой группе мы отнесем процессы, являющиеся средой исполнения (виртуальные машины как среды исполнения скриптов и апплетов, и офисные приложения как среды исполнения макросов).
4	Процессы, обладающие недекларированными (документально не описанными) возможностями	Г	К ним относят две группы процессов: те, которые запускаются в системе с привилегированными правами, например, под учетной записью System, и те, которые наиболее вероятно могут быть подвержены атакам, например, сетевые службы.

11.Установите взаимно однозначное соответствие

1	Контактное считывание	А	подразумевает сочетание нескольких различных способов считывания
2	Бесконтактный (дистанционный) способ считывания	Б	подразумевает непосредственный контакт идентификатора и считывающего устройства

3	Комбинированный	В	способ считывания не требует чѐткого позиционирования идентификатора и считывающего устройства

12.Установите взаимно однозначное соответствие

1	Генерация случайных чисел	А	При включении ПК устройство требует от пользователя ввести персональную информацию (например, вставить дискету с ключами)
2	Контроль входа на компьютер	Б	При каждом вычислении подписи ему необходимо новое случайное число.
3	Контроль целостности файлов операционной системы	В	Это не позволит злоумышленнику в ваше отсутствие изменить какиелибо данные

13.Установите взаимно однозначное соответствие

1	Привязка файлов программного продукта к их физическому расположению на диске	А	Во время проверки делается попытка записи 1 по такому адресу и считывание еѐ
2	Запись в неиспользуемый участок последнего кластера, распределенного файлу, контрольной информации	Б	Метод основан на том, что при восстановлении файлов на другом компьютере они будут располагаться в других секторах диска
3	Прожигание лазером (или прокалывание) отверстия в оригинальном диске по заранее определенному адресу	В	причем сам пароль не хранится в программе, а обрабатывается введенная строка и по полученному адресу вызывается следующая выполняемая подпрограмма
4	Опрос пароля при загрузке программы	Г	При выгрузке и восстановлении файлов эти неиспользуемые участки файлов пропадают

14. Установите взаимно однозначное соответствие

1	Метод экспериментов	А	контрольные суммы
2	Динамический режим изучения алгоритма программы	Б	заключается в проведении многократных экспериментов с изучаемой программой и сравнительном анализе полученных результатов
3	CRC	В	предполагает выполнение трассировки программы

15. Установите взаимно однозначное соответствие

1	Логические бомбы	А	программы, предназначенные для слежения за деятельностью пользователя и несанкционированного чтения обрабатываемой им информации
2	Червями	Б	программы или их части, постоянно находящиеся в ЭВМ и выполняемые только при соблюдении определенных условий
3	Троянские кони	В	называются программы, которые обладают способностью перемещаться в системе или сети и самовоспроизводить копии
4	Программы-шпионы	Г	это программы, полученные путем явного изменения или добавления команд в пользовательские программы

16. Установите взаимно однозначное соответствие

1	Программы показа рекламы	А	программы, которые изменяют или прерывают работу компьютера способом, который их

			создатель счел смешным или, наоборот, пугающим
2	Программы-шутки	Б	программы, которые позволяют получить доступ к компьютеру извне по сети Интернет для сбора информации, атаки на компьютер пользователя или внесения в него изменений
3	Программы удаленного доступа	В	программы, применяемые хакерами для получения несанкционированного доступа к компьютеру пользователя
4	Средства взлома	Г	отдельные или дополняющие программы, которые втайне собирают через Интернет информацию о пользователе и отправляют ее на другой компьютер

17.Установите взаимно однозначное соответствие

1	Угрозы для безопасности	А	записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор.
2	Загрузочные вирусы	Б	угрозы, которые не соответствуют в точности определению вируса, троянского коня, червя и других категорий угроз, но могут представлять угрозы для компьютера и хранящихся на нем данных
3	Макро-вирусы	В	используют для своего распространения протоколы или команды компьютерных сетей и электронной почты
4	Сетевые вирусы	Г	заражают файлы-документы

			и электронные таблицы нескольких популярных редакторов

18. Установите взаимно однозначное соответствие

1	Порядковое кодирование	А	Кодирование реквизитов-признаков, при котором все кодируемые значения сведены в список и кодовой комбинацией каждого значения является его номер в списке
2	Пословное кодирование	Б	Кодирование, при котором последовательность кодов – делится на группы, объединяющие объекты по какому-либо признаку
3	Серийно-порядковое кодирование	В	Способ кодирования реквизитов-признаков, состоящий в последовательном кодировании каждого смыслового объекта входного документа

19. Установите взаимно однозначное соответствие

1	Архивация	А	это преобразование информации, делающее ее нечитаемой для посторонних
2	Шифрование	Б	запись информации в электронном виде для долговременного хранения
3	Использование самогенерирующих кодов	В	это исполняемые коды программы, полученные в результате выполнения некоторого набора арифметических и/или логических операций над определенным, заранее рассчитанным, массивом данных

20. Установите взаимно однозначное соответствие

1	Криптография	А	это перевод информации с одного языка на другой
2	Кодирование	Б	наука о методах обеспечения конфиденциальности
3	Скремблирование	В	обратимое преобразование цифрового потока без изменения скорости

Задания на установление правильной последовательности

1. Установить этапы защиты от угроз безопасности:

1. Предоставление персоналу защищенный удаленный доступ к информационным ресурсам

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

3. Защита внешних каналов передачи информации

4. Разработка политики информационной безопасности

5. Анализ угрозы безопасности

2. Установить этапы стадии исполнения компьютерных вирусов:

1. Выполнение деструктивных функций

2. Передача управления программе-носителю вируса

3. Поиск жертвы

4. Заражение найденной жертвы

5. Загрузка вируса в память

3. Установить этапы построения системы антивирусной защиты сети:

1. Реализация плана антивирусной безопасности

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

3. Разработка политики антивирусной безопасности

4. Разработка плана обеспечения антивирусной безопасности

4. Установить этапы построения программы обеспечения безопасности:

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

2. Регулярный контроль пошаговой реализации плана безопасности

3. Установление уровня безопасности

4. Формирование политики безопасности организации

5. Определение ценности технологических и информационных активов организации

5. Установить действия этапа анализа рисков:

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

2. Оценка рисков технологических и информационных активов

3. Идентификация и оценка стоимости технологических и информационных активов

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

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

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

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

3. Совокупность событий должна сравниваться с заранее установленной пороговой величиной

4. Каждое нарушение безопасности должно генерировать системное событие

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

1. Дата, время
2. Протокол
3. Порт получателя
4. Номер агента
5. IP-адрес атакующего
6. Тип атаки

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

1. ISO 27001:2005
2. ISO/IEC 17799
3. ISO/IEC 15408
4. «Критерии оценки доверенных компьютерных систем»

9. Расположить этапы процесса управления рисками информационной безопасности:

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

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

3. Выбор, реализация и проверка защитных мер

4. Оценка остаточного риска

5. Идентификация активов и ценности ресурсов, нуждающихся в защите

6. Выбор анализируемых объектов и степени детальности их рассмотрения

10. Расположить этапы проведения аудита информационной безопасности:

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

11. 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

12. 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

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

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

14. Расположить этапы процесса комплекса превентивных мер

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

15. Расположить этапы проведения аудита информационной безопасности:

1. Разработка рекомендаций по повышению уровня защиты автоматизированной системы
2. Анализ полученных данных

3. Сбор исходных данных
4. Разработка регламента проведения аудита

16. Восстановите алгоритм испытаний

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

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

18. 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.

19. Последовательность слов для понятия Компьютерная сеть – это
1. Обеспечивающего передачу
2. Устройства связи
3. Связанных с помощью
4. Данных между ними
5. Группа компьютеров

20. 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.

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

Представьте в виде схемы классификацию ЭВМ: по принципу действия, по поколению, по назначению, по размерам

Компетентностно-ориентированная задача №2
Представьте в виде схемы основные компоненты параллельного компьютера с описанием их функций

Компетентностно-ориентированная задача №3
Представьте в виде рисунка классификацию архитектур ЭВМ, предложенную Майклом Флинном

Компетентностно-ориентированная задача №4
Составьте функциональную схему АЛУ и опишите её составляющие

Компетентностно-ориентированная задача №5
Составьте упрощенную функциональную схему устройства управления

Компетентностно-ориентированная задача №6
Составьте схему мультипроцессорной памяти и опишите её составляющие

Компетентностно-ориентированная задача №7
Используя интернет, выбрать такую конфигурацию компьютера, который будет эффективно справляться с профессиональными задачами, связанными с вашей профессиональной деятельностью. Подобрать основные и дополнительные устройства. Рассчитать стоимость

Компетентностно-ориентированная задача №8
Опишите технологический процесс обработки информации. Перечислите и охарактеризуйте технологические процессы процесса обработки информации. Какие режимы обработки информации вам известны? Перечислите устройства защиты технических устройств информатизации от изменения напряжения и тока их электропитания.

Компетентностно-ориентированная задача №9
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.

Компетентностно-ориентированная задача №10

Опишите параметры локальной политики безопасности операционной системы Windows, параметры и значения параметров Политики учетной записи, параметры и значения параметров Политики паролей. Измените параметр «Пароль должен отвечать требованиям сложности» Политики паролей на «Включен» и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль.

Компетентностно-ориентированная задача №11
Создайте папку, в которую поместите текстовый файл и приложение в виде файла с расширением exe. Установите для этой папки разрешения полного доступа для одного из пользователей группы Администраторы и ограниченные разрешения для пользователя с ограниченной учетной записью. Установите общий доступ к папке и подключитесь к ней через сеть с другого виртуального компьютера. Предложите стратегию регулирования безопасности при коллективном доступе к общим папкам для различных групп пользователей.

Компетентностно-ориентированная задача №12
Опишите параметры и значения параметров Политики аудита. Просмотрите события в журнале событий. Информация о каких событиях сохраняется в системном журнале? Какие данные по каждому событию отображаются в журнале? Включите аудит успеха и отказа всех параметров.

Компетентностно-ориентированная задача №13
Опишите причины возникновения остаточной информации. Приведите примеры устройств уничтожения информации с магнитных носителей. Перечислите основные требования к современным устройствам уничтожения информации с магнитных носителей. Охарактеризуйте программные методы уничтожения информации. Обоснуйте выбор устройства уничтожения информации с магнитных носителей.

Компетентностно-ориентированная задача №14
Опишите разделы реестра Windows. В каких разделах реестра хранится информация о выбранной политике безопасности? Опишите возможности программы REGEDIT.EXE. Проведите исследование реестра Windows для нахождения следов активности вредоносного ПО.

Компетентностно-ориентированная задача №15
Создайте новую книгу для проведения простых вычислений суммы, разности, произведения над числами, удовлетворяющими некоторому условию, на основе данных, вводимых пользователем. Задайте проверку выполнения условия (например, только положительные, только отрицательные, только целые из определенного диапазона значений и т.п.) для ячеек, в которые будет осуществляться ввод данных. Установите защиту:

ячейки для ввода данных должны быть разблокированы, остальное содержимое листа – защищено от изменений; формулы, по которым производятся вычисления, – скрыты. При установке защиты листа разрешить всем пользователям настраивать ширину столбцов и высоту строк, менять заливку ячеек.

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.