

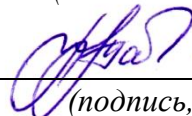
Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 23.03.2023 13:58:35
Уникальный программный ключ:
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

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

Защищённые информационные системы

(наименование учебной дисциплины)

10.04.01 Информационная безопасность, направленность (профиль)
«Защищенные информационные системы»

(код и наименование ОПОП ВО)

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

Тема 1. Основные аспекты построения системы информационной безопасности.

1. Чем регулируется ответственность нарушений информационной безопасности во внешней среде?
2. Что такое программа информационной безопасности?
3. Опишите структуру модели информационной безопасности.
4. Какие параметры СЗИ можно оценить с помощью системы количественных метрик?
5. Какие существуют модели и алгоритмы классификации СЗИ?
6. Опишите требований к системе информационной безопасности.
7. Назовите этапы обеспечения информационной безопасности.

Тема 2. Мероприятия по защите информации.

1. Перечислите мероприятия по ЗИ в нормативно-законодательном аспекте.
2. Перечислите мероприятия по ЗИ в процедурном аспекте.
3. Перечислите мероприятия по ЗИ в организационном аспекте.
4. Перечислите мероприятия по ЗИ в программно-техническом аспекте.
5. Понятие «политика информационной безопасности».
6. Особенности реализации политики ИБ при разработке СЗИ.
7. Опишите системное содержание политики информационной безопасности.
8. Этапы реализации политики ИБ.
9. Уровни политики ИБ

Тема 3. Требования к архитектуре ИС для обеспечения безопасности ее функционирования.

1. Что нужно учитывать при выборе компонент СЗИ и связей между ними?
2. Назовите основные принципы разработки СЗИ.
3. Как влияет простота структуры ЗИС на качество выполняемых ею функций?
4. Для чего нужна стандартизация подходов при разработке СЗИ?
5. Перечислите основные стандарты, в которых изложены требования к защищённым информационным системам.
6. Опишите структуру и содержание стандарта ISO 13335.
7. Опишите структуру профиля защиты ИТ-продукта.
8. Критерии рентабельности защищённой информационной системы.
9. Как зависит эффективность и рентабельность защиты от величины максимального ущерба?

10. Как зависит эффективность и рентабельность системы защиты от величины общих ресурсов?

Тема 4. Требования к архитектуре ИС для обеспечения безопасности ее функционирования.

1. Понятие оценочного стандарта
2. Назовите основные термины «Оранжевой книги»
3. Назовите характеристики монитора информационной безопасности.
4. Для чего нужен механизм подотчётности при реализации политики информационной безопасности?
5. Что такое операционная гарантированность и что она в себя включает?
6. Понятие класса безопасности и критерии отнесения ЗИС к определённому классу.
7. Механизмы информационной безопасности, описываемые в оценочных критериях

Тема 5. Критерии оценки безопасности информационных технологий.

1. Опишите иерархию сущностей в "Критериях оценки безопасности информационных технологий".
2. Назовите основные термины, описанные в "Критериях оценки безопасности информационных технологий".
3. Опишите структуру класса «приватность».
4. Опишите структуру класса «использование ресурсов».
5. Что такое требования доверия безопасности и для чего они нужны?
6. Что такое уровни доверия?
7. Какие существуют механизмы обеспечения безопасности в распределённых системах?

Тема 6. Руководящие документы ФСТЭК России.

1. Назовите основные документы, которыми руководствуются разработчики ЗИС?
2. Назовите основные классы безопасности, фигурирующие в документах ФСТЭК, и критерии отнесения систем к каждому из них.
3. Какие требования предъявляют регулирующие документы к ЗИС? Какие СЗИ классифицированы.

Тема 7. Понятие информационной системы и рассмотрение архитектур применяемы.

1. Что такое информационная система?
2. Классифицируйте информационные системы по различным признакам.
3. Типы обеспечивающих подсистем.
4. Что такое техническое обеспечение?

Тема 8. Оценочные стандарты и технические спецификации.

1. Что такое политика безопасности?
2. Что такое уровень гарантированности?
3. Главные характеристики доверенной вычислительно базы.
4. Что такое периметр безопасности?

Тема 9. Перечень потенциальных источников атак и определение их возможностей (модель нарушителя).

1. По каким критериям определяются модели нарушителя?
2. Из каких категорий персонала может быть внутренний нарушитель?
3. Чем могут быть вызваны действия злоумышленника?
4. Что такое горячий информатор?

Тема 10. Определение уровня защищенности данных в информационной системе.

1. Чем обусловлена необходимость классификации угроз информационной безопасности?
2. Что такое уязвимость объекта?
3. Назовите проявления возможного ущерба.
4. Основные группы источников угроз информации.

Тема 11. Описание угроз безопасности информации (модель угроз безопасности информации)

1. Порядок определения угроз безопасности информации при ее обработке в ИС.
2. Кто относится к внешним нарушителям?
3. Анализ способов реализации угроз безопасности информации
4. Что такое нарушение целостности?

Тема 12. Методы выбора системы защиты информации

1. Что такое методы защиты информации?
2. Назовите группы методов защиты.
3. Задачи специалиста по безопасности.
4. Что такое идентификация?

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

Лабораторная работа №1 «Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение»

1. Дать определение понятию «безопасность информации».
2. Какие действия понимаются под безответственностью пользователя?
3. Критерии оценки информационных систем.
4. Какие параметры защиты не учитываются концепцией защиты информации?
5. На чем основан механизм одобрения для защищенных систем?

Лабораторная работа №2 «Определение показателей защищенности информации при несанкционированном доступе»

1. В каких случаях используется способ декомпозиции задачи оценки эффективности защищенности системы?
2. Схема многозвенной защиты объекта информатизации
3. Требования к показателям защищенности шестого класса.
4. Что можно отнести к основным угрозам?

Лабораторная работа №3 «Критерии оценки и выбора CASE-средств.

1. Функциональные характеристики критериев
2. Что такое построение диаграмм ?
3. Что такое имитационное моделирование?
4. Что такое прототипирование?
5. Назовите общие функции.

Лабораторная работа №4 «Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности»

1. Для чего служит Доктрина информационной безопасности?
2. Что выступает в качестве средств защиты информации, подлежащих сертификации в Системе сертификации средств защиты информации по требованиям безопасности информации?
3. Основные схемы сертификации средств защиты информации.
4. Какие функции осуществляет ФСТЭК России в пределах своей компетенции?

Лабораторная работа №5 «Создание модели вероятного нарушителя»

1. Составляющие модели нарушителя.
2. Цели и задачи вероятного нарушителя.
3. Четыре категории нарушителя.
4. Что такое неформализованная модель?
5. Что такое формализованная модель?

Лабораторная работа №6 «Оценка защищённости информационной системы на основании методики ФСТЭК»

1. В каких случаях обязательно выполнение рекомендаций регулятора?
2. Что регламентируют нормы ФСТЭК?
3. Что относится к документам государственной организации?
4. Методы проверки в ходе аттестации.

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.

1.3 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа №1 «Описание особенностей информационной системы, влияющих на её защищённость»

1. Характеристика архитектурной безопасности.
2. Причины минимизации объема защитных средств.
3. Что такое гарантированность безопасности?
4. Последствия нарушения безопасности.

Практическая работа №2 «Соотнесение требований стандартов информационной безопасности с характеристиками информационной системы»

1. Какие функции выполняют стандарты в области информационной безопасности?
2. Основные области стандартизации информационной безопасности.
3. Классификации стандартов информационной безопасности.

4. Какие процедуры должны быть выполнены разработчиком при разработке средства?

5. Что должно предусматривать проектирование средства, соответствующего шестому уровню доверия?

Практическая работа №3 «Описание физических и логических взаимосвязей между компонентами информационной системы. Оценка их влияния на итоговую защищённость»

1. Что такое физическая взаимосвязь между компонентами?
2. Понятие логических взаимосвязей между компонентами.
3. Что такое внутренние сетевые углы?
4. Кто считается собственником информационного ресурса?

Практическая работа №4 «Описание функциональных и технологических взаимосвязей между компонентами информационной системы»

1. Понятие и информационной системы.
2. Функции, определяющие процессы в информационной системе.
3. Подсистема «Программное обеспечение».
4. Что такое суперкомпьютеры?
5. Что относится к средствам коммуникационной техники?

Практическая работа №5 «Составление модели угроз безопасности информационной системы»

1. Принципы разработки модели угроз безопасности информации
2. Связь «фактор риска - угроза»
3. Связь «угроза - контрмера»
4. Содержание модели угроз

Практическая работа №6 «Выбор метода защиты информации»

1. От каких угроз информации нужна защита?
2. Составляющие защиты информации.
3. Понятие системы защиты информации.
4. Что такое техническая защита информации?
5. Криптографическая защита информации

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.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1. Что отражает модель жизненного цикла информационной системы?

1) все события, происходящие с системой в процессе ее создания и использования

2) процесс создания системы

3) процессы, связанные с использованием системы

4) все события в системе во время ее эксплуатации

2. Для чего производится предварительное обследование объекта автоматизации?

1) для формирования концепции создания системы

2) для создания прототипа системы

3) для выяснения готовности предприятия к автоматизации

4) для формирования команды, которая будет работать над созданием системы

3. Укажите основную цель детального обследования объекта автоматизации.

1) формирование технического задания на систему

2) подбор исполнителя для создания системы

3) определение целей автоматизации

4) выбор технических и программных инструментов

4. Отметьте методы сбора информации при проведении обследования объекта автоматизации.

1) анкетирование

2) интервьюирование

3) метод аналогий

4) создание "фотографии рабочего дня"

5) метод проб и ошибок

6) метод Монте-Карло

5. Какие данные обрабатываются в фактографических информационных системах?

1) структурированные данные в виде текстов и чисел

2) любые изображения

3) только числовые

4) исторические факты

6. Какая методология моделирования систем использует понятие "Прецедент"?

1) методология объектно-ориентированного моделирования

2) структурное моделирование

3) визуальное моделирование

4) функциональное моделирование

7. В основе архитектурного проектирования лежат понятия:

- 1) Проектирование – как средство достижения поставленного результата
- 2) Архитектура – как результат
- 3) Архитектура – как видение
- 4) Проектирование – как инструмент планирования разработки

8. Проектирование - это

- 1) вид активности направленный на создание уникального продукта (услуги), последовательность этапов реализации которого, будет определяться «внешними» факторами, и определять его конечные преимущества и недостатки
- 2) видение конечного результата реализации информационной системы
- 3) процесс формирования структуры проекта
- 4) анализ текущего состояния структуры компании и предложение идей об улучшении бизнес-процессов

9. Архитектурное проектирование - это

- 1) процесс реализации пожеланий Стэйкхолдеров
- 2) работы по подготовке структуры взаимодействия систем в организации
- 3) вид активности, который своей целью ставит создание архитектуры в процессе выполнения проекта
- 4) вид работ по определению границ проекта

10. Архитектурное проектирование программного обеспечения, одной из задач ставит

- 1) бесперебойное функционирование информационных систем компании
- 2) поддержку и развитие существующих процессов и информационных систем компании
- 3) формирование особого видения, всех участников проекта, на конечный продукт

4) создание артефакта (архитектуры), который должен обеспечить достижение результатов деятельности организаций, использующих программные продукты для реализации своих процессов

11. Программные продукты – это

1) исполняемые процедуры

2) реализация требований Спонсоров проекта

3) взаимосвязанные информационные сущности, выполняющие запросы Пользователей

4) основной элемент большинства современных высокотехнологичных доменов деятельности

12. Причиной развития темы архитектуры программного обеспечения является

1) рост издержек предприятий

2) развитие технологий

3) нарастающая конкуренция

4) требования к качеству информационных продуктов

13. Шаблоны проектирования (design patterns) представляет собой

1) руководство по реализации

2) универсальный свод информации

3) проектная документация на разработку

4) ограничения по реализации

14. Архитектурные решения - это

1) соглашения, учитывающие и удовлетворяющие различные точки зрения, «силы», принципы, как технического, так и не технического характера

2) соглашения, между Архитектором и Командой по реализации

3) тип используемых методик проектирования

4) видение конечного результата реализации

15. Выбор стиля использования шаблонов производится на основании

1) имеющихся ресурсов

2) конкурентной среды

3) политики организации

4) требований

16. Сложность обеспечения информационной безопасности является следствием:

1) злого умысла разработчиков информационных систем

2) объективных проблем современной технологии программирования

3) происков западных спецслужб, встраивающих "закладки" в аппаратуру и программы

17. Сложность обеспечения информационной безопасности является следствием:

1) невнимания широкой общественности к данной проблематике

2) все большей зависимости общества от информационных систем

3) быстрого прогресса информационных технологий, ведущего к постоянному изменению информационных систем и требований к ним

18. Что из перечисленного относится к числу основных аспектов информационной безопасности:

1) подотчетность - полнота регистрационной информации о действиях субъектов

2) приватность - сокрытие информации о личности пользователя

3) конфиденциальность - защита от несанкционированного ознакомления

19. Компьютерная преступность в мире:

- 1) остается на одном уровне
- 2) снижается
- 3) растет

20. Что из перечисленного не относится к числу основных аспектов информационной безопасности:

- 1) доступность
- 2) целостность
- 3) защита от копирования
- 4) конфиденциальность

21. Укажите, с какой целью строятся диаграммы для экспозиции (FEO).

- 1) для иллюстрации отдельных фрагментов модели
- 2) для иллюстрации альтернативной точки зрения
- 3) для иллюстрации специальных целей
- 4) для иллюстрации взаимосвязи между работами

22. Укажите, что показывает диаграмма дерева узлов.

- 1) иерархическую зависимость работ
- 2) взаимосвязи между работами
- 3) глубины детализации

23. Укажите, что входит в определение контекста модели.

- 1) определение субъекта моделирования
- 2) определение цели моделирования
- 3) определение точки зрения

4) определение количества уровней декомпозиции

24. Какие типы элементарных моделей используются для построения организационно-функциональной структуры?

1) древовидные модели (классификаторы)

2) процессные модели

3) матричные модели

25. Какая модель отвечает на вопросы: *зачем* компания занимается именно этим бизнесом, *почему* предполагает быть конкурентоспособной, *какие* цели и стратегии для этого необходимо реализовать?

1) стратегическая модель целеполагания

2) организационно-функциональная модель

3) функционально-технологическая модель

4) процессно-ролевая модель

5) модель структуры данных

26. Сформулируйте цель методологии проектирования ИС

1) регламентация процесса проектирования ИС и обеспечение управления этим процессом с тем, чтобы гарантировать выполнение требований как к самой ИС, так и к характеристикам процесса разработки

2) формирование требований, направленных на обеспечение возможности комплексного использования корпоративных данных в управлении и планировании деятельности предприятия

3) автоматизация ведения бухгалтерского аналитического учета и технологических процессов

27. Выделите утверждение, верное в отношении защиты сетей.

1) уровень защищенности сети определяется уровнем защищенности ее самого «сильного» звена

2) уровень защищенности сети определяется суммой уровней защищенности ее звеньев

3) уровень защищенности сети определяется уровнем защищенности ее самого «слабого» звена

4) уровень защищенности сети не зависит напрямую от защищенности ее отдельных звеньев

28. Как называется мера доверия, которая может быть оказана архитектуре, инфраструктуре, программно-аппаратной реализации системы и методам управления её конфигурацией и целостностью?

1) эффективность безопасности

2) гарантированность безопасности

3) непрерывность безопасности

4) надежность безопасности

29. Каким термином обозначается анализ регистрационной информации системы защиты?

1) мониторинг

2) аудит

3) аккредитация

4) сертификация

30. Какие компоненты присутствуют в модели системы защиты с полным перекрытием?

1) область угроз

2) область рисков

3) защищаемая область

4) система защиты

5) область безопасности

31. Как называется возможность осуществления угрозы Т в отношении объекта О?

- 1) слабость
- 2) неполнота
- 3) уязвимость
- 4) риск

32. Что означает система защиты с полным перекрытием?

- 1) для половины (и более) уязвимостей есть устраняющие барьеры
- 2) для любой уязвимости есть устраняющий ее барьер
- 3) у любой уязвимости есть риск ее реализации
- 4) количество уязвимостей меньше, чем количество препятствующих им барьеров

33. Чем характеризуется степень сопротивляемости механизма защиты?

- 1) вероятностью его преодоления
- 2) количеством угроз, которым этот механизм препятствует
- 3) величиной потерь в случае успешного прохождения
- 4) стоимостью механизма защиты

34. При отсутствии в системе барьеров, «перекрывающих» выявленные уязвимости, степень сопротивляемости механизма защиты принимается равной...

- 1) 0
- 2) 1

35. Защищенность системы защиты определяется как величина...

- 1) обратная суммарному количеству рисков
- 2) обратная остаточному риску

3) обратная уязвимости

4) равная сумме всех уязвимостей

36. В чем заключается идеология открытых систем информационной безопасности?

1) в строгом соответствии систем информационной безопасности законодательству страны, которым они созданы

2) в строгом соблюдении совокупности профилей, протоколов и стандартов де-факто и де-юре

3) в открытости информации о стоимости реализации конкретной системы защиты

4) в открытости программных кодов средств защиты от производителей разных стран

37. Для чего в первую очередь нужна идеология открытых систем информационной безопасности?

1) для удешевления средств защиты информации

2) для минимизации рисков от реализации угроз

3) для совместимости компонент различных информационных систем

38. В чем заключается принцип минимизации привилегий?

1) выделение полных прав доступа только администраторам системы

2) выделение только тех прав, которые необходимы для реализации своих должностных обязанностей

3) выделение прав доступа в зависимости от величины возможного ущерба

39. В чем заключается принцип эшелонирования обороны?

1) в том, чтобы использовать максимально возможное количество защитных средств

2) в простоте и управляемости информационной системы

3) в усилении самого надежного защитного рубежа

4) в том, чтобы не полагаться на один защитный рубеж

40. Что из нижеперечисленного относится к оперативным методам повышения безопасности?

1) систематическое тестирование

2) предотвращение ошибок в CASE-технологиях

3) обязательная сертификация

4) программная избыточность

41. то из нижеперечисленного относится к мерам предотвращения угроз безопасности?

1) систематическое тестирование

2) предотвращение ошибок в CASE-технологиях

3) обязательная сертификация

4) программная избыточность

42. Выделите внутренние по отношению к объекту уязвимости дестабилизирующие факторы и угрозы безопасности:

1) ошибки персонала при эксплуатации

2) ошибки программирования

3) сбой и отказы аппаратуры ЭВМ

4) ошибки алгоритмизации задач

43. На каких принципах должна строиться архитектура ИС?

1) проектирование на принципе закрытых систем

2) проектирование на принципе открытых систем

3) усиление самого сильного звена

4) усиление самого слабого звена

5) эшелонирование обороны

44. Какие органы исполнительной власти являются ключевыми в области технической защиты информации?

1) ФСТЭК России

2) ФСБ России

3) СВР России

4) МВД России

5) Роскомнадзор

45. Какой орган государственной власти осуществляет контроль и надзор за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных?

1) ФСТЭК России

2) ФСБ России

3) СВР России

4) МВД России

5) Роскомнадзор

46. Какой орган исполнительной власти осуществляет контроль в области криптографической защиты информации?

1) ФСТЭК России

2) ФСБ России

3) МВД России

4) Роскомнадзор

47. Какой орган исполнительной власти осуществляет сертификацию средств защиты информации, систем и комплексов телекоммуникаций, технических средств, используемых для выявления электронных устройств,

предназначенных для негласного получения информации, в помещениях и технических средствах?

- 1) ФСТЭК России
- 2) ФСБ России
- 3) МВД России
- 4) Роскомнадзор

48. Какой орган исполнительной власти в настоящее время выполняет функции Гостехкомиссии России в области технической защиты информации?

- 1) ФСТЭК России
- 2) ФСБ России
- 3) МВД России
- 4) Роскомнадзор

49. Какой орган исполнительной власти реализует контрольные функции в области обеспечения защиты (некриптографическими методами) информации?

- 1) ФСТЭК России
- 2) ФСБ России
- 3) МВД России
- 4) Роскомнадзор

50. Какой орган исполнительной власти проводит лицензирование деятельности по оказанию услуг в области защиты государственной тайны в части, касающейся противодействия техническим разведкам и/или технической защиты информации?

- 1) ФСТЭК России
- 2) ФСБ России
- 3) МВД России
- 4) Роскомнадзор

Задания в открытой форме

1. Информационная система-это...
2. Информационные системы можно классифицировать по признакам...
3. Подсистема-это...
4. Унифицированные системы документации-это...
5. В концепции обеспечения информационной безопасности предприятия определяются...
6. Конфиденциальную информацию обычно классифицируют...
7. Обеспечение безопасности должно основываться на...
8. Для обеспечения мероприятия для защиты информации необходимо произвести...
9. К принципам построения технической системы безопасности относятся...
10. Архитектура системы должна быть...
11. В качестве объектов уязвимости рассматриваются...
12. Наличие и полнота политики безопасности-это...
13. Механизм одобрения для защищенных систем основан на...
14. Владелец информации и владелец ресурсов могут быть...
15. Формирование защиты в ИС основывается на...
16. Организационное обеспечение-это...
17. В структуру информационного обеспечения входит...
18. На этапе хранения данных информационная система охватывает...
19. База данных-это...
20. На этапе публикации (представления) информации ИО включает...

Задания на установление соответствия

1. Установите взаимно однозначное соответствие

1	Информационная система (ИС)	А	предназначена для эффективной эксплуатации экономической ИС
2	Автоматизированная ИС	Б	система сбора, хранения, накопления, поиска и передачи информации, применяемая в процессе управления или принятия решений.
3	Автоматизированная ИС	В	совокупность информ., экономико-математических методов и моделей, аппаратных, программных, организационных, технологических средств и специалистов

2. Установите взаимно однозначное соответствие

1	ИС управления технологическими процессами	А	предназначены для автоматизации функций инженеров-проектировщиков, конструкторов, архитекторов, дизайнеров при создании новой техники или технологии.
2	ИС автоматизированного проектирования	Б	используются для автоматизации всех функций фирмы и охватывают весь цикл работ от планирования деятельности до сбыта продукции.
3	Интегрированные (корпоративные) ИС	В	оказывает устойчивую тенденцию роста спроса на информационные системы организационного управления.
4	Анализ современного состояния рынка ИС	Г	служат для автоматизации функций производственного персонала по контролю и управлению производственными операциями.

3. Установите взаимно однозначное соответствие

1	Гибкость системы-	А	определяется как частное от деления фактического количества группировок на величину емкости системы.
2	Емкость системы-	Б	это способность допускать включение новых признаков, объектов без разрушения структуры классификатора.
3	Степень заполненности системы-	В	это наибольшее количество классификационных группировок, допускаемое в данной системе классификации.

4. Установите взаимно однозначное соответствие

1.	Выявление критически важной информации	А	на этом этапе выполняется непосредственно специалистами, проводящими аудит. От результатов этой работы зависит выбор схемы построения информационной
----	--	---	--

			безопасности
2	Выявление слабых мест в корпоративной безопасности	Б	Это завершающий этап аудита, в ходе которого на основании проведенного анализа составляется список конкретных мер, которые необходимо принять для охраны корпоративных секретов компании
3	Оценка возможностей защиты информации	В	на этом этапе происходит определение тех документов и данных, безопасность которых имеет огромное значение для компании, а утечка – несет огромные убытки.

5. Установите взаимно однозначное соответствие

1	Конфиденциальный аспект	А	Это комплексная работа при защите данных, которая обеспечит защиту от сбоев в работе и уничтожения самих данных.
2	Целостностный аспект	Б	Включает в себя обеспечение надежного и эффективного доступа к защищаемой информации только проверенных лиц.
2	Аспект доступности	В	Означает, что нужно тщательно контролировать работу с данными, чтобы устранить возможность их утечки, а также предотвратить несанкционированный доступ к ним со стороны неизвестных людей

6. Установите взаимно однозначное соответствие

1	Аппаратная угроза	А	есть вероятность некорректной работы программного обеспечения
2	Вероятность утечки	Б	существует вероятность нарушения работоспособности оборудования
3	Нестабильность ПО	В	возможен

			несанкционированный доступ к данным и их потеря
--	--	--	---

7. Установите взаимно однозначное соответствие

1	Антивирусная программа-	А	специализированное программное обеспечение, предназначенное для защиты компании от утечек информации
2	CloudAV-	Б	специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ .
3	DLP-решения-	В	заключается в преобразовании ее составных частей (слов, букв, слогов, цифр) с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении ее к неявному виду
4	Криптографическое преобразование-	Г	одно из облачных решений информационной безопасности, что применяет легкое программное обеспечение агента на защищенном компьютере, выгружая большую часть анализа информации в инфраструктуру провайдер

8. Установите взаимно однозначное соответствие

1.	Защита информации-	А	это желаемый результат защиты информации. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного
----	--------------------	---	---

			воздействия на информацию.
2	Объект защиты-	Б	это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
3	Цель защиты информации-	В	степень соответствия результатов защиты информации поставленной цели
4	Эффективность защиты информации-	Г	информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации

9. Установите взаимно однозначное соответствие

1	Защита информации от утечки-	А	деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации.
2	Защита информации от разглашения-	Б	деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.
3	Защита информации от НСД-	В	Деятельность по предотвращению несанкционированного

			доведения защищаемой информации до неконтролируемого количества получателей информации.
4	Система защиты информации -	Г	совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

10. Установите взаимно однозначное соответствие

1	Доступ к информации -	А	это способность информации или некоторого информационного ресурса быть доступными для конечного пользователя в соответствии с его оперативными потребностями.
2	Оперативность доступа к информации-	Б	субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.
3	Собственник информации-	В	получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.
4	Владелец информации -	Г	субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.

11. Установите взаимно однозначное соответствие

1	Способ защиты информации -	А	совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения информационной безопасности системы (сети).
2	Средство защиты информации-	Б	порядок и правила применения определенных принципов и средств защиты информации.
3	Комплекс средств защиты (КСЗ)-	В	средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.
4	Техника защиты информации-	Г	Техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации

12. Установите взаимно однозначное соответствие

1	Операционная гарантированность	А	охватывает весь жизненный цикл ИС, то есть периоды проектирования, реализации, тестирования, продажи и сопровождения.
2	Технологическая гарантированность	Б	это совокупность защитных механизмов ИС
3	Доверенная вычислительная база	В	относится к архитектурным и реализационным аспектам системы

13. Установите взаимно однозначное соответствие

1	Произвольное управление доступом-	А	Представляют собой свойства (характеристики) объектов и (или) субъектов доступа
2	Безопасность повторного использования объектов-	Б	основано на сопоставлении меток безопасности субъекта и объекта.

3	Метки безопасности-	В	это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит.
4	Принудительное (или мандатное) управление доступом-	Г	важное дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения конфиденциальной информации из "мусора"

14. Установите взаимно однозначное соответствие

1	Ядро безопасности-	А	проверка подлинности идентификаторов сущностей с помощью различных (преимущественно криптографических) методов.
2	Аутентификация-	Б	показатель реально обеспечиваемого уровня безопасности, отражающий степень эффективности и надежности реализованных средств защиты и их соответствия поставленным задачам
3	Идентификация-	В	совокупность аппаратных, программных и специальных компонентов ВС, реализующих функции защиты и обеспечения безопасности.
4	Адекватность-	Г	процесс распознавания сущностей путем присвоения им уникальных меток

15. Установите взаимно однозначное соответствие

1	Математическое и программное обеспечение	А	совокупность правовых норм, определяющих создание,
---	--	---	--

	(МО, ПО)-		юридический статус и функционирование информационных систем, регламентирующих порядок получения, преобразования и использования информации
2	Организационное обеспечение (ОО)-	Б	совокупность математических методов, моделей, алгоритмов и программ для реализации целей и задач информационной системы, а также нормального функционирования комплекса технических средств
3	Правовое обеспечение (Пр.О) -	В	совокупность методов и средств, регламентирующих взаимодействие работников с техническими средствами и между собой в процессе разработки и эксплуатации информационной системы.

16. Установите взаимно однозначное соответствие

1	Сопровождение-	А	проверка функционального соответствия системы показателям, определенным на этапе анализа
2	Функционирование-	Б	обеспечение штатного процесса эксплуатации системы на предприятии заказчика.
3	Внедрение-	В	штатный процесс эксплуатации в соответствии с основными целями и задачами ИС
4	Тестирование-	Г	установка и ввод системы в действие

17. Установите взаимно однозначное соответствие

1	Принцип интеграции	А	заключается в том, что при декомпозиции должны быть установлены такие связи
---	--------------------	---	---

			между структурными компонентами системы, которые обеспечивают цельность корпоративной системы и ее взаимодействие с другими системами
2	Принцип системности	Б	предполагает рассмотрение всех сторон объекта исследования в его связи и зависимости с другими процессами и явлениями
3	Принцип комплексности	В	заключается в том, что обрабатываемые данные (документы) вводятся в систему только один раз и затем многократно используются для решения возможно большего числа задач

18. Установите взаимно однозначное соответствие

1	CRM-	А	программная система, охватывающая ключевые процессы деятельности и управления, позволяющая получить самый общий взгляд на работу предприятия
2	SCM-	Б	система планирования потребностей в материалах, одна из наиболее популярных в мире логистических концепций, на основе которой разработано и функционирует большое число микрологистических систем
3	MRP-	В	управления цепочками поставок
4	ERP-	Г	управление отношениями с клиентами - бизнес-стратегия, предназначенная для оптимизации доходов, прибыльности и

			удовлетворенности клиентов
--	--	--	----------------------------

19. Установите взаимно однозначное соответствие

1	Специальные категории ПДн-	А	данные, характеризующие биологические или физиологические особенности субъекта и используемые для установления личности, например, фотография или отпечатки пальцев
2	Биометрические ПДн-	Б	обработка персональных данных субъектов, не являющихся работниками вашей организации
3	Общедоступные ПДн-	В	относится информация о национальной и расовой принадлежности субъекта, о религиозных, философских либо политических убеждениях, информацию о здоровье и интимной жизни субъекта
4	Иные категории ПДн-	Г	сведения о субъекте, полный и неограниченный доступ к которым предоставлен самим субъектом

20. Установите взаимно однозначное соответствие

1	Соответствие направлению импортозамещения-	А	наличие и состав индивидуально настраиваемых параметров, гибкость настройки позволят оценить применимость решения к принятой парадигме развития процессов обеспечения ИБ
2	Функциональные особенности-	Б	наличие развитых встроенных и интегрируемых подсистем позволит в начальном периоде эксплуатации ограничиться использованием одного продукта, без увеличения

			количества используемых интерфейсов
3	Интеграционные возможности-	В	отчетность, и удобство, и глубина погружения при навигации в рамках интерфейса системы
4	Дополнительные критерии-	Г	позволит оценить, можно ли использовать решение в рамках государственных инициатив по поддержке отечественного производителя и борьбе с санкциями.

Задания на установление правильной последовательности

1. Установить последовательность этапов стадии создания системы защиты информации

1. Внедрение системы защиты информации (этап установки, настройки, испытаний)
2. Формирование требований к системе защиты информации (предпроектный этап)
3. Подтверждение соответствия системы защиты информации (этап оценки)
4. Разработка системы защиты информации (этап проектирования)

2. Установить последовательность этапов внедрения системы безопасности

1. Внедрение организационных мер защиты информации, в том числе, разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в ходе эксплуатации объекта
2. Выявление и анализ уязвимостей программных и технических средств, принятие мер по их устранению
3. Установка и настройка средств защиты информации
4. Испытания и опытная эксплуатации системы защиты информации

3. Установить порядок проведения аттестации информационных систем по требованиям безопасности информации

1. Проведение аттестационных испытаний объекта
2. Предварительное ознакомление с аттестуемым объектом (при необходимости)
3. Оформление, регистрация и выдача аттестата соответствия
4. Подача и рассмотрение заявки на аттестацию

5. Разработка программы и методики аттестационных испытаний
4. Определить этапы уровня защищенности персональных данных
 1. классификация информационной системы
 2. сбор и анализ исходных данных по информационной системе
 3. установление уровня защищенности персональных данных и его документальное оформление
 4. формирование модели угроз и определение категории нарушителя
5. Установить последовательность этапов принципа действия сетевых червей
 1. Поиск "жертв»
 2. Подготовка копий
 3. Проникновение в систему
 4. Распространение копий
 5. Активация
6. Установить последовательность этапов методического процесса построения корпоративной системы защиты от вирусов
 1. Разработка политики антивирусной безопасности
 2. Проведение анализа объекта защиты и определение основных принципов обеспечения антивирусной безопасности
 3. Реализация плана антивирусной безопасности
 4. Разработка плана обеспечения антивирусной безопасности
7. Установить порядок обеспечения защиты информации
 1. Проверяется эффективность принятых мер
 2. Составляется перечень коммерческих тайн и сведений, не подлежащих разглашению
 3. Разрабатываются способы хранения информации (использование электронных носителей, бумажных документов, технических средств обработки)
8. Установить последовательность клиент-серверной архитектуры
 1. клиентские компьютеры выступают потребителями
 2. серверы являются поставщиками услуг (сервисов)
 3. информационная система
9. Установить последовательность многозвенной архитектуры
 1. Уровень данных
 2. Представление

3. Уровень логики
4. Данные
5. Уровень представления

10. Установить последовательность этапов архитектуры распределенных систем с репликацией

1. Репликация
2. Сервер без данных
3. Клиентская ЭВМ
4. Репликация

11. Установить последовательность итерационного процесса разработки и реализации политики ИБ

1. Принципы контроля состояния систем защиты информации
2. Вопросы резервного копирования данных и информации
3. Принципы администрирования системы ИБ и управление доступом к вычислительным и телекоммуникационным средствам, программам и информационным ресурсам,
4. Принципы использования информационных ресурсов персоналом компании и внешними пользователями
5. антивирусную защиту и защиту против действий хакеров

12. Установить последовательность распределения ответственности за обеспечение безопасности

1. Назначение для каждого ресурса (или процесса) ответственного сотрудника из числа руководителей
2. Определение и документальное закрепление для каждого ресурса списка прав доступа (матрицы доступа)
3. Определение ресурсов, имеющих отношение к информационной безопасности по каждой системе

13. Установить последовательность ролевого управления доступом

1. Сеанс работы пользователя
2. Объект
3. Пользователь
4. Роль
5. Операция

14. Установить последовательность Метода OCTAVE

1. Осуществляется оценка организационных аспектов

2. Проводится разработка стратегии обеспечения безопасности
3. Высокоуровневый анализ ИТ-инфраструктуры организации
4. Определяются требования безопасности
5. Строится профиль угроз для каждого критического ресурса

15. Установить последовательность возникновения плана обработки рисков метода OSTATE

1. Атака на данные системы электронного документооборота
2. Выход из строя системы эл. документооборота или изменение/уничтожение данных на ресурсе
3. Атака на данные сервера разработки
4. Выход из строя сервера разработки или уничтожение изменение данных на данном ресурсе

16. Установить последовательность полной обработки рисков

1. Выход из строя сервера разработки или изменение/ уничтожение данных
2. Выход из строя СЭД или изменение/уничтожение данных
3. Угроза
4. Атака на данные СЭД
5. Атака на данные сервера разработки

17. Установить последовательность этапов проектирования информационных систем

1. Требуемой пропускной способности системы
2. Определения цели проекта
3. Требуемой функциональности системы и уровня ее адаптивности к Изменяющимся условиям функционирования
4. Безотказной работы системы
5. Простоты эксплуатации и поддержки системы

18. Установить последовательность этапов ЖЦ построения и последовательного преобразования ряда согласованных моделей

1. Требований к приложениям
2. Организации
3. Проекта ИС
4. Требований к ИС

19. Установить последовательность этапов создания ИС

1. Реализация

2. Формирование требований к системе
3. Ввод в действие
4. Тестирование
5. Проектирование

20. Установить последовательность совокупности архитектурой программных систем

1. Выбор структурных элементов, составляющих систему и их интерфейсов
2. Объединение элементов в подсистемы
3. Организации программной системы
4. Поведение элементов во взаимодействии с другими элементами

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

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

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

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

Соответствие 100-балльной и 5-балльной шкал

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

2.2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

1. Реализуйте схему объекта информатизации
2. Реализуйте параметры локальной сети и список сотрудников
3. Реализуйте классификацию угроз по источнику
4. Реализуйте классификацию угроз по последствиям
5. Реализуйте перечень нормативно-правовых актов в области информационной безопасности
6. Реализуйте поиск и удаление временных файлов вручную
7. Реализуйте шифрование и дешифрование данных с помощью программ
8. Реализуйте схему построения модели СЗИ
9. Реализуйте архитектуру Веб-приложений
10. Реализуйте защиту от вирусов в Интернете
11. Реализуйте Защиту программы от несанкционированного использования с помощью USB-ключей
12. Реализуйте защиту папок и файлов
13. Реализуйте восстановление удаленных файлов и необратимое удаление информации
14. Реализуйте перечень антивирусных программ, указывая преимущества и недостатки
15. Реализуйте признаки заражения вредоносным ПО
16. Реализуйте характеристику оценочных стандартов
17. Реализуйте защитные средства программно-технического уровня для построения эшелонированной обороны информационной системы
18. Реализуйте процесс стеганографии и объясните принцип работы
19. Реализуйте свойства подписи на бумаге и электронной подписи
20. Реализуйте примеры нарушений целостности данных

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.