МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование ф-та полностью)
М.О. Таныгин
(подпись, инициалы, фамилия)
« 29 » августа 2023 г.

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

Технологии обеспечения информационной безопасности объектов
(наименование учебной дисциплины)

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

Курск – 2023

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

Тема №1 «Понятия и определения технических средств охраны. Структура автоматизированной системы охраны»

1. Что такое технические средства охраны (ТСО)?
2. Назначение и цели ТСО.
3. Основные виды ТСО.
4. Дайте определение термину «Техническая безопасность».
5. Дайте определение термину «Компьютерная безопасность».
6. Что такое канал сигнализации? Как можно классифицировать ССОИ.
7. Что подразумевается под техническими средствами охраны?
8. Какие основные виды технических средств охраны существуют?
9. Какие функции выполняют технические средства охраны?
10. Какова структура автоматизированной системы охраны?

Тема №2 «Варианты программно-аппаратной реализации ТСО»

1. Что такое диалог человека и КТСО и для чего он нужен?
2. Нарисуйте структурную схему, поясняющую принцип контроля состояния СО и объясните её.
3. Каким образом можно представить схему функционирования ССОИ?
4. Перечислите и охарактеризуйте методы отображения информации, применяемые в ССОИ.
5. Как можно организовать информационный обмен ССОИ с подсистемами КТСО или с другими самостоятельными системами специальной защиты?
6. Какие программные средства используются для реализации технических средств охраны?
7. Какая роль аппаратного обеспечения в программно-аппаратной реализации ТСО?
8. Какие типы датчиков могут быть использованы в программно-аппаратной реализации ТСО?
9. Каким образом программно-аппаратная реализация ТСО может быть интегрирована с системой видеонаблюдения?
10. Какие возможности предоставляют программно-аппаратные комплексы для обработки и анализа данных, получаемых от технических средств охраны?

Тема №3 «Методология разработки концепции комплексного обеспечения безопасности объектов охраны»

1. Перечислите укрупненные признаки, по которым принято классифицировать ССОИ.

2. Что такое ТСО, каковы основные подходы к их классификации? Приведите пример их классификации.

3. Что такое ЧЭ, каковы основные подходы к их классификации? Приведите пример и классификации.

4. Перечислите виды ССОИ в зависимости от структурной схемы построения.

5. Перечислите виды ССОИ в зависимости от способа подключения средства обнаружения (СО).

6. Какой признак классификации характеризует степень безопасности канала сигнализации? Перечислите виды ССОИ в зависимости от этого признака.

7. Какие основные шаги включает методология разработки концепции комплексного обеспечения безопасности объектов охраны?

8. Какие аспекты учитываются при определении требований к комплексному обеспечению безопасности объектов охраны?

9. Какой подход используется при анализе и выборе технических средств охраны в рамках разработки концепции комплексного обеспечения безопасности?

10. Как осуществляется оценка эффективности разработанной концепции комплексного обеспечения безопасности объектов охраны?

Тема №4 «Общий подход к категорированию объектов охраны»

1. Назовите категории объектов охраны.

2. Каковы факторы внешней среды, влияющие на выбор тактико-технических характеристик СО?

3. Как разделяются ССОИ по способам обеспечения контроля работоспособности аппаратуры?

4. Перечислите основные функции, выполняемые ССОИ в составе комплексов ТСО.

5. Как разделяются ССОИ по возможности хранения и документирования (распечатки) оперативной информации?

6. Что подразумевается под категорированием объектов охраны?

7. Какие основные критерии используются при категорировании объектов охраны?

8. Какие типы угроз обычно учитываются при определении категории объекта охраны?

9. Какие меры безопасности могут быть рекомендованы для каждой категории объектов охраны?

10. Какова роль и ответственность службы охраны при категорировании объектов охраны?

Тема №5 «Классификация нарушителей информационной безопасности, угроз ИБ и технических средств охраны»

1. Что такое "модель" нарушителя, какие типы "моделей" нарушителей рассматриваются?

2. Назовите типы моделей нарушителей, сформулируйте их отличительные признаки.

3. Нарисуйте и прокомментируйте структурную схему передачи информации о наличии нарушителя.

4. Назовите типы ССОИ в зависимости от их устойчивости к обходу, сформулируйте их отличительные признаки.

5. Решение каких задач предполагает "Системная концепция обеспечения комплексной безопасности?

6. Расскажите о классификации нарушителей, исходя из их "моделей" и способов реализации угроз безопасности.

7. Как осуществляется классификация нарушителей информационной безопасности?

8. Какие типы угроз информационной безопасности обычно выделяются при классификации?

9. Какие факторы учитываются при выборе и использовании технических средств охраны?

10. Какие основные категории технических средств охраны существуют и в каких случаях они применяются?

Критерии оценки:

9-16 баллов 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.

1-8 баллов выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

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

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРАКТИЧЕСКИМ РАБОТАМ

Контрольные вопросы для защиты практической работы №1.

1. Дать определение термину «Система охраны объекта».
2. В чем заключается суть абстрактно-типизированного подхода?
3. Сколько уровней защиты объекта существует? Раскройте каждый из них.
4. Кем регламентируется отнесение конкретных объектов к той или иной категории важности?
5. Какие объекты попадают под AI и AII?
6. Какие объекты попадают под AI и AII?
7. Какие объекты попадают под БI и БII
8. В соответствии с каким документом проводится обследование состояния технической укрепленности объекта?
9. Какие методы и процедуры применяются при организации и проведении обследования объектов на предмет состояния инженерно-технического укрепления?
10. Какие критерии и показатели оцениваются при обследовании объектов для определения состояния и эффективности их инженерно-технического укрепления?

Контрольные вопросы для защиты практической работы №2.

1. Физические основы акустического канала утечки.
2. Способы пассивной защита акустического ТКУ КИ.
3. Способы активной защиты акустического ТКУ КИ.
4. Как выбираются частоты сигнала при оценке защищенности акустического ТКУ КИ?
5. Что такое октавная полоса звуковых частот?
6. Как образуется виброакустический ТКУ КИ?
7. В чем состоят различия акустического и виброакустического сигналов утечки КИ?
8. Метод оценки утечки КИ по виброакустическому ТКУ.
9. Основные режимы работы МПП ST-031 «Пиранья».
10. Какими датчиками комплектуется МПП ST-031 для контроля акустического и виброакустического ТКУ КИ, их принцип работы и основные характеристики?
11. Достоинства и недостатки пассивных средств защиты речевой КИ.
12. Достоинства и недостатки активных средств защиты речевой КИ.
13. Рекомендации по установке излучателей СВАЗ «Соната».

Контрольные вопросы для защиты практической работы №3.

1. Принцип действия ЛГШ-104 как средства активной защиты КИ.
2. От каких факторов зависит эффективность работы (площадь эффективной зоны подавления КИ) ЛГШ?
3. Какие технические характеристики ЛГШ влияют на эффективность защиты речевой КИ?
4. Особенности воздействия ЛГШ разных типов на диктофоны в сотовых телефонах.
5. Каковы правила размещения и эксплуатации ЛГШ-104?
6. Основные типы подавителей диктофонов и особенности их функционирования.
7. По каким критериям выбираются подавители диктофонов?
8. Как можно исключить применение диктофонов, размещенных в мобильных телефонах, для перехвата речевой КИ?
9. В каких случаях целесообразно камуфлировать средства подавления диктофонов и как это можно сделать на практике?
10. Объясните физические явления, на основании которых работает подавитель диктофонов.

Контрольные вопросы для защиты практической работы №4.

1. Каким образом можно классифицировать СОТ?
2. Дать определение термину «Видеоконтроль».
3. Какие системы входят в Класс III?
4. Дать определение термину «Объект контроля».
5. Какие системы входят в Класс II?
6. Дать определение термину «"Мертвая" зона».
7. Дать определение термину «Разрешающая способность (разрешение) СОТ».
8. Какие системы входят в Класс V?
9. Какие системы входят в Класс IV?
10. Назовите основные цели при проектировании системы.

Критерии оценки:

2 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.

1 балл (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.

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

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

1.3 КОНТРОЛЬНЫЕ ВОПРОСЫ К ЛАБОРАТОРНЫМ РАБОТАМ

Контрольные вопросы для защиты лабораторной работы №1.

1. Что такое РЭП ?
2. Основная цель РЭП и решаемые ею задачи ?
3. Какие аспекты инфокоммуникационной безопасности СБС нарушает РЭП ?
4. Что такое эффективность РЭП, какие известны виды реализуемого ущерба ?
5. Основной показатель для оценки эффективности РЭП, как он определяется ?
6. Какие условия необходимо выполнить для эффективного подавления СБС?
7. Основной критерий для оценки эффективности РЭП, как он определяется ?
8. Что такое коэффициент подавления и от каких факторов он зависит ?
9. Из каких этапов состоит процесс решения прямой задачи РЭП ?
10. Что такое электромагнитная доступность СБС?
11. Какие факторы влияют на предельную дистанцию Rп РЭП УКВ радиосвязи ?
12. Какие факторы влияют на величину коэффициента подавления Квх на входе приемного устройства подавляемого канала связи ?

Контрольные вопросы для защиты лабораторной работы №2.

1. Сколько требований и какие в связи с РЭБ предъявляются к РТКС?
2. Что такое РЭБ ?
3. В чем состоит суть метода скремблирования и каково его основное назначение в ТКС?
4. Какие свойства скремблирования цифровых сообщений позволяют его использовать для повышения степени их защиты от несанкционированного доступа ?
5. Что такое скремблер и дескремблер ?
6. Что является основной частью скремблера ?
7. Сколько и какие известны основных типов скремблеров и дескремблеров ?
8. Изобразить схему СС-скремблера и дескремблера, объяснить принцип их работы и указать основные недостатки ?
9. Изобразить схему АД-скремблера и дескремблера, объяснить принцип их работы и указать основные недостатки ?
10. В чем сущность шифрования сообщения по ГОСТ 28147—89?
11. Изобразить функциональную схему передачи сообщений с криптозащитой по ГОСТ 28147—89?

Контрольные вопросы для защиты лабораторной работы №3.

1. Защита от каких классов воздействий рассматривается в теории защиты информации?
2. Как осуществляется защита информации, передаваемой по каналам связи, от случайных помех?
3. Как осуществляется защита информации, передаваемой по каналам связи, от преднамеренных помех?
4. Что такое имитозащита?
5. В чем состоит сущность имитозащиты?
6. Что такое имитовставка?
7. Чему равна вероятность правильного угадывания злоумышленником значений избыточных бит информации?
8. Что такое имитозащита в контексте защиты информации в системах беспроводной связи?
9. Каким образом работает имитозащита для защиты передаваемых сообщений в беспроводных системах связи?
10. Какие методы и техники применяются для реализации имитозащиты в сетях беспроводной связи?

Контрольные вопросы для защиты лабораторной работы №4.

1. На сколько классов и каких разделяется помехозащита?

2. Какими факторами определяется вероятность ошибки на бит в приемнике подавляемой РЭС?

3. Какие факторы и как повышают помехозащиту радиолинии?

4. Привести выражение для уравнения помехозащиты и
пояснить параметры, входящие в это выражение

5.Изобразить функциональную схему помехозащищенной радиолинии и пояснить принцип ее работы.

6. Пояснить принцип работы РЭС с ППРЧ на примере частотно-временной диаграммы с ППРЧ-сигнала.

7. Какие методы сигнальной помехозащиты применяются для защиты радиолиний?

8. Что такое частотная помехозащита и как она работает?

9. Что такое временная помехозащита и как она применяется для защиты радиолиний?

10. Какие техники и алгоритмы используются в цифровой помехозащиты радиолиний?

Контрольные вопросы для защиты лабораторной работы №5.

1. Что такое спутниковая система связи?

2. Что такое отбор мощности ретранслятора помехой?

3. Какие факторы и как влияют на эффект отбора мощности ретранслятора помехой?

4. Сколькими видами методов и какими могут осуществляться радио-(РМ) ирадиотехническая (РМ) маскировки?

5. Что такое пассивная РМ и РТМ?

6. Сколько различают видов организационных мероприятий пассивной РМ и РТМ и какие?

7. Сколько при наличии внешних угроз различают режимов использования РЭС и какие?

8. Сколько различают видов технических мероприятий при пассивной маскировке РЭС и какие?

9. Какие факторы влияют на эффективность помехозащиты в спутниковых линиях связи?

10. Как проводится оценка помехозащищенности спутниковой связи?

11. Какие методы используются для улучшения помехозащиты в спутниковых линиях связи?

Контрольные вопросы для защиты лабораторной работы №6.

1. Что такое скрытность РЭС?

2. На сколько видов и каких подразделяются демаскирующие признаки РЭС?

3. Что такое технические признаки РЭС, сколько различают их типов и какие?

4. Что такое оперативно-тактические демаскирующие признаки РЭС, сколько различают их типов и какие?

5. Что такое радиоэлектронная маскировка (РЭМ), сколько типов РЭМ различают и какие?

6. Что такое активная РМ и РТМ?

7. Что такое непроизвольные (паразитные) электромагнитные излучения и внешние (видовые) признаки, сколько предусмотрено видов мер скрытия этих признаков и какие?

8. Какие методы повышения скрытности могут использоваться в радиоэлектронных системах (РЭС)?

9. Как осуществляется оценка эффективности применения методов повышения скрытности в РЭС?

10. Какие факторы могут влиять на результаты оценки эффективности методов повышения скрытности в РЭС?

Критерии оценки:

2 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.

1 балл (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.

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

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

1.4 ПРОИЗВОДСТВЕННЫЕ ЗАДАЧИ

1. Разработка и внедрение системы контроля доступа: Ваша компания получила заказ на разработку и внедрение системы контроля доступа для физического объекта, такого как офисное здание или производственный цех. Задача состоит в выборе соответствующих технологий, таких как биометрические считыватели, электронные пропускные системы или видеонаблюдение, и создании интегрированной системы контроля доступа.
2. Создание политики управления уязвимостями: Ваша компания решает создать политику управления уязвимостями для своих объектов, чтобы обеспечить надлежащую защиту от потенциальных угроз. Задача состоит в определении процессов и процедур по выявлению, анализу и устранению уязвимостей в информационных системах объектов, а также внедрении соответствующих технологий для обнаружения и предотвращения атак.
3. Разработка и реализация плана резервного копирования данных: Ваша компания осознает важность регулярного резервного копирования данных и решает разработать и реализовать план резервного копирования для своих объектов. Задача состоит в выборе подходящих технологий и инструментов для резервного копирования, определении расписания и процедур резервного копирования, а также внедрении механизмов проверки целостности и восстановления данных.
4. Аудит безопасности объектов: Ваша компания получила задание провести аудит безопасности для своих объектов, включая оценку физической безопасности, защиты информационных систем и сетевой инфраструктуры. Задача состоит в проведении всестороннего анализа безопасности объектов, выявлении слабых мест и уязвимостей, а также в предоставлении рекомендаций по улучшению безопасности с применением соответствующих технологий.
5. Разработка и внедрение системы контроля доступа: Ваша компания получила заказ на разработку и внедрение системы контроля доступа для физического объекта, такого как офисное здание или производственный цех. Задача состоит в выборе соответствующих технологий, таких как биометрические считыватели, электронные пропускные системы или видеонаблюдение, и создании интегрированной системы контроля доступа.
6. Создание политики управления уязвимостями: Ваша компания решает создать политику управления уязвимостями для своих объектов, чтобы обеспечить надлежащую защиту от потенциальных угроз. Задача состоит в определении процессов и процедур по выявлению, анализу и устранению уязвимостей в информационных системах объектов, а также внедрении соответствующих технологий для обнаружения и предотвращения атак.

7. Разработка и реализация плана резервного копирования данных: Ваша компания осознает важность регулярного резервного копирования данных и решает разработать и реализовать план резервного копирования для своих объектов. Задача состоит в выборе подходящих технологий и инструментов для резервного копирования, определении расписания и процедур резервного копирования, а также внедрении механизмов проверки целостности и восстановления данных.

8. Аудит безопасности объектов: Ваша компания получила задание провести аудит безопасности для своих объектов, включая оценку физической безопасности, защиты информационных систем и сетевой инфраструктуры. Задача состоит в проведении всестороннего анализа безопасности объектов, выявлении слабых мест и уязвимостей, а также в предоставлении рекомендаций по улучшению безопасности с применением соответствующих технологий.

9. Разработка и внедрение системы биометрической идентификации: Вам было поручено разработать и внедрить систему биометрической идентификации для физического доступа к объекту. Задача состоит в выборе подходящих биометрических технологий (например, отпечатков пальцев, распознавания лица или сетчатки глаза), разработке соответствующей инфраструктуры и интеграции системы с существующими системами безопасности.

10. Разработка и внедрение системы контроля доступа: Ваша компания решает улучшить систему контроля доступа к объекту. Задача состоит в разработке и внедрении системы, которая обеспечит эффективный контроль доступа с использованием технологий, таких как электронные пропускные системы, ключ-карты или бесконтактные технологии. Ваша задача также включает настройку правил доступа, создание журналов событий и обеспечение интеграции системы контроля доступа с другими системами безопасности.

Критерии оценки:

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

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

1 балл (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно

четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

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

1.5 КЕЙС-ЗАДАЧИ

1. Компания А является провайдером информационной безопасности и была нанята финансовым учреждением для обеспечения безопасности и защиты их информационных систем, включая клиентскую информацию, финансовые данные и транзакционные операции. Кейс задачи включает следующие аспекты:

1) Анализ уязвимостей: Ваша задача состоит в проведении анализа уязвимостей информационной инфраструктуры финансового учреждения. Это включает оценку сетевых уязвимостей, слабых мест в программном обеспечении и возможных уязвимостей в физической инфраструктуре. Вы должны выявить уязвимости, определить их уровень серьезности и потенциальный риск для безопасности учреждения.

2) Разработка политики безопасности: Вам необходимо разработать политику безопасности, которая будет определять набор правил, мероприятий и процедур для обеспечения безопасности информационных систем финансового учреждения. Эта политика будет включать в себя требования к паролям, управлению доступом, защите данных, обнаружении вторжений и реагированию на инциденты. Вы должны учитывать соответствующие регуляторные требования и стандарты безопасности, применимые к финансовым учреждениям.

3) Разработка системы мониторинга и обнаружения инцидентов: Ваша задача состоит в разработке и внедрении системы мониторинга и обнаружения инцидентов, которая будет автоматически отслеживать и анализировать активность в информационных системах финансового учреждения. Это включает мониторинг сетевого трафика, журналов событий, обнаружение вторжений и аномального поведения пользователей. Система должна предупреждать о потенциальных инцидентах безопасности и предоставлять возможность реагировать на них.

4) Внедрение системы шифрования данных: Ваша задача состоит в разработке и внедрении системы шифрования данных для защиты конфиденциальности и целостности информации

2. Ситуация: Банковское учреждение столкнулось с увеличивающимся числом кибератак и утечек данных. Руководство банка осознает важность обеспечения информационной безопасности и нанимает вашу компанию для разработки и внедрения современных технологий обеспечения безопасности.

Ваша задача:

1) Анализ угроз: Провести анализ угроз информационной безопасности банковского учреждения, учитывая особенности банковской сферы. Выявить потенциальные уязвимости и основные угрозы, такие как фишинг, мошенничество с использованием кредитных карт, DDoS-атаки и несанкционированный доступ к банковским данным.

2) Разработка стратегии обеспечения безопасности: Разработать стратегию обеспечения информационной безопасности, учитывая выявленные угрозы и уязвимости. Включить в нее различные аспекты, такие как сетевая безопасность, контроль доступа, шифрование данных, мониторинг и обнаружение инцидентов.

3) Внедрение технологий безопасности: Предложить и внедрить соответствующие технологии обеспечения безопасности, включая системы межсетевой безопасности (firewalls), системы обнаружения вторжений (IDS/IPS), системы аутентификации пользователей, системы шифрования данных и системы мониторинга событий и инцидентов.

4) Обучение персонала: Провести обучение сотрудников банка основам информационной безопасности, включая правила использования паролей, обработку фишинговых писем, предотвращение утечек данных и осведомленность о текущих угрозах.

3. Компания В занимается консалтингом по информационной безопасности и была нанята финансовой организацией для обеспечения безопасности и защиты их информационных систем и конфиденциальных данных клиентов. Задача состоит в том, чтобы разработать и внедрить соответствующие технологии и меры для обеспечения безопасности объекта.

Ключевые задачи включают:

1) Анализ угроз: Провести анализ угроз, с которыми сталкивается финансовая организация, и оценить их потенциальные последствия. Включите в анализ как внутренние, так и внешние угрозы, такие как кибератаки, утечка данных или мошенничество. Разработайте методику оценки уровня риска каждой угрозы.

2) Аудит безопасности: Провести аудит безопасности информационных систем финансовой организации. Оценить существующие меры безопасности и выявить потенциальные уязвимости. Разработать рекомендации по улучшению безопасности на основе результатов аудита.

3) Разработка политики безопасности: Разработать и внедрить политику безопасности, которая будет регулировать использование информационных систем и защиту конфиденциальных данных. Определить

требования по доступу к данным, пароли, шифрование, резервное копирование и другие меры безопасности. Обеспечить соответствие политики безопасности нормативным требованиям и стандартам отрасли.

4) Защита периметра сети: Разработать и внедрить технологии защиты периметра сети финансовой организации. Включить межсетевые экраны, системы обнаружения вторжений, фильтрацию трафика и другие меры, чтобы предотвратить несанкционированный доступ к сети и защитить ее от внешних угроз.

4. Компания С занимается консультированием и внедрением технологий информационной безопасности. Вы получили заказ от крупного финансового учреждения для обеспечения безопасности и защиты их информационных систем и клиентских данных. Задача состоит в том, чтобы разработать и реализовать комплексный план мероприятий по обеспечению информационной безопасности финансового учреждения.

Вам предстоит выполнить следующие задачи:

1) Анализ текущей информационной инфраструктуры: Провести аудит существующих систем и инфраструктуры финансового учреждения, выявить слабые места и уязвимости, а также оценить уровень защищенности.

2) Разработка политики безопасности: Создать и внедрить политику безопасности, которая определит правила и рекомендации для сотрудников и клиентов финансового учреждения. Политика должна охватывать аспекты, такие как пароли, доступ к данным, шифрование, физическая безопасность и прочие меры.

3) Защита сетевой инфраструктуры: Разработать и внедрить меры защиты сетевой инфраструктуры финансового учреждения. Включить в это межсетевые экраны, системы обнаружения вторжений, виртуальные частные сети (VPN) и другие средства защиты.

4) Защита клиентских данных: Разработать и внедрить меры по защите конфиденциальных данных клиентов финансового учреждения. Включить в это шифрование данных, контроль доступа, резервное копирование и системы мониторинга для обнаружения несанкционированного доступа.

5) Обучение сотрудников: Провести обучение сотрудников финансового учреждения по вопросам информационной безопасности. Обучение должно включать правила использования компьютеров и сети, распознавание фишинговых атак, защиту паролей и другие аспекты информационной безопасности.

5. Корпорация Y решила улучшить информационную безопасность своего офисного здания, чтобы защитить конфиденциальные данные клиентов, важную корпоративную информацию и предотвратить несанкционированный доступ к системам и ресурсам компании. Ваша задача

- разработать и внедрить комплексные технологии обеспечения информационной безопасности для объекта.

Вам предстоит выполнить следующие задачи:

1) Анализ угроз: Определите основные угрозы информационной безопасности, с которыми может столкнуться корпоративное офисное здание. Рассмотрите физические, социальные и технические угрозы, такие как несанкционированный доступ к зданию, взлом системы контроля доступа, кража данных и т.д.

2) Разработка системы контроля доступа: Разработайте и внедрите систему контроля доступа, которая позволит эффективно управлять физическим доступом к зданию и его помещениям. Включите в нее технологии, такие как электронные ключи, биометрическая идентификация, системы видеонаблюдения и системы тревожной сигнализации.

3) Защита сетевой инфраструктуры: Оцените безопасность сетевой инфраструктуры офисного здания и рекомендуйте необходимые технологии и меры для защиты от сетевых угроз. Включите в свой анализ брандмауэры, системы обнаружения вторжений, шифрование данных и другие технологии обеспечения безопасности сети.

4) Обучение персонала: Разработайте программу обучения для сотрудников офисного здания по правилам информационной безопасности. Обучите их основным принципам безопасности, распознаванию фишинговых атак, защите паролей, безопасному обращению с конфиденциальной информацией и другим аспектам информационной безопасности.

Критерии оценки:

4-8 баллов (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

2 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. Для чего применяется экранирование помещений и дополнительное заземление объектов защиты?

a. для увеличения уровня побочных электромагнитных излучений
b. для уменьшения уровня побочных электромагнитных излучений
c. для обеспечения бесперебойного питания объектов защиты
d. для исключения внедрения злоумышленников во внутренние сегменты сети

2. Какое требование к системе защиты информации предполагает организацию единого управления по обеспечению защиты информации?

a. адекватность
b. непрерывность
c. централизованность
d. универсальность

3. Какое требование к системе защиты информации предполагает то, что методы защиты должны обеспечивать возможность перекрытия канала утечки информации, независимо от его вида и места появления?

a. адекватность
b. непрерывность
c. централизованность
d. универсальность

4. Как называется логическая группа устройств, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам?

a. виртуальная частная сеть
b. виртуальная локальная сеть
c. защищенная магистральная сеть
d. виртуальная канальная сеть

5. Какое название получила технология, позволяющая обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети с применением средств криптографии?

a. виртуальная частная сеть
b. виртуальная локальная сеть
c. защищенная магистральная сеть
d. виртуальная канальная сеть

6. Наиболее общий способ проникновения в систему:

a. слабые пароли
b. дефекты программирования
c. переполнение буфера

7. Наиболее надежный способ аутентификации:

a. парольная защита
b. смарт-карты
c. биометрические методы

8. Какие методы используют хакеры при проведении социального инжиниринга?

a. умение вести телефонную беседу
b. подбор паролей методом перебора
c. скрытое сканирование портов

9. Лучший способ борьбы с социальным инжинирингом:

a. обеспечение физической защиты и контроля доступа
b. информирование служащих
c. использование сертифицированного программного обеспечения

10. Для какой цели применяются виртуальные частные сети?

a. для снижения нагрузки на сеть
b. для обеспечения информационной безопасности
c. для обеспечения отказоустойчивости
d. для уменьшения количества передаваемого служебного трафика

11. Какое название получила технология, позволяющая обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети с применением средств криптографии?

a. виртуальная частная сеть
b. виртуальная локальная сеть
c. защищенная магистральная сеть
d. виртуальная канальная сеть

12. Для какой цели применяются виртуальные частные сети?

a. для снижения нагрузки на сеть
b. для обеспечения информационной безопасности
c. для обеспечения отказоустойчивости
d. для уменьшения количества передаваемого служебного трафика

13. Как называется логическая группа устройств, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам?

a. виртуальная частная сеть
b. виртуальная локальная сеть
c. защищенная магистральная сеть
d. виртуальная канальная сеть

14. Следующее структурное подразделение службы защиты информации отвечает за проведение работ по повышению квалификации персонала

a. Группа режима
b. Группа охраны и сопровождения
c. Техническая группа
d. Детективная группа

15. Следующее структурное подразделение службы защиты информации отвечает за организацию прохода персонала и посетителей в различные зоны безопасности

a. Группа режима
b. Группа охраны и сопровождения
c. Техническая группа
d. Детективная группа

16. Межсетевые экраны прикладного уровня могут

a. Выполнять авторизацию пользователя.
b. Автоматически распознавать новые протоколы.
c. Выполнять аутентификацию пользователя.
d. Шифровать данные пользователя.

17. В обязанности какого сотрудника входит контроль за выполнением планов непрерывной работы

a. Сотрудник группы безопасности
b. Администратор безопасности системы
c. Администратор безопасности данных
d. Руководитель группы

18. В обязанности какого сотрудника входит контроль защиты наборов данных и программ

a. Сотрудник группы безопасности
b. Администратор безопасности системы
c. Администратор безопасности данных
d. Руководитель группы

19. В обязанности какого сотрудника входит организация общей поддержки групп управления защитой и менеджмента в своей зоне ответственности

a. Сотрудник группы безопасности
b. Администратор безопасности системы
c. Администратор безопасности данных
d. Руководитель группы

20. Количественный состав службы безопасности зависит, прежде всего от

a. Типа циркулирующей в ней конфиденциальной информации
b. От возможностей фирмы
c. Нормативных документов регуляторов
d. Численности штата

21. К какому сотруднику предъявляются следующие требования: высшее профессиональное образование и стаж работы в области защиты информации не менее 5 лет, хорошее знание законодательных актов в этой области и принципов планирования защиты

a. Директор
b. Начальник службы защита информации
c. Сотрудник сектора охраны и режима
d. Аналитик
e. Сотрудник сектора технической защиты

22. Кто вырабатывает политику обеспечения защиты информации и обеспечивает ее реализацию?

a. Директор
b. Начальник службы защита информации
c. Аналитик
d. Руководитель группы

e. Юрист
f. Администратор безопасности системы

23. Кто руководит проведением служебных расследований?
a. Директор
b. Начальник службы защиты информации
c. Аналитик
d. Руководитель группы
e. Юрист
f. Администратор безопасности системы

24. Кто несёт персональную ответственность за выполнение службой защиты информации своих функций?
a. Начальник службы защиты информации
b. Сотрудник сектора обеспечения безопасности
c. Аналитик
d. Руководитель группы
e. Юрист

25. Кто разрабатывает руководящие документы и инструкции по вопросам безопасности?
a. Директор
b. Начальник службы защиты информации
c. Сотрудник группы безопасности
d. Аналитик
e. Юрист

26. Кто обеспечивает режим допуска и доступа?
a. Начальник службы защита информации
b. Сотрудник сектора охраны и режима
c. Сотрудник сектора обеспечения безопасности
d. Сотрудник группы безопасности
e. Руководитель группы

27. Какой из перечисленных методов оценки риска основан на расчетах и анализе статистических показателей?
a. Вероятностный метод
b. Метод сценариев
c. Учет рисков при расчете чистой приведенной стоимости
d. Анализ чувствительности

28. Какой из перечисленных методов оценки риска дает представление о наиболее критических факторах инвестиционного проекта?
a. Построение дерева решений
b. Метод сценариев

c. Учет рисков при расчете чистой приведенной стоимости
d. Анализ чувствительности

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

30. Что, из перечисленного, понимается под термином частная виртуальная сеть?
a. Шифрованный туннель внутри обычной сети.
b. Локальная сеть в здании.
c. Программный комплекс для шифрования.

31. Одна из причин, по которой коммутаторы не должны использоваться для предоставления каких-либо возможностей межсетевого экрана
a. Коммутаторы не могут видеть передаваемый трафик.
b. Коммутаторы не могут предотвращать возможные DoS-атаки.
c. Коммутаторы не могут видеть порт, на который ушел пакет.
d. Коммутаторы не могут видеть порт, на который пришел пакет.

32. Основное свойство коммутаторов (выберите самое точное определение, один ответ)
a. Коммутаторы передают пакеты только нужному адресату.
b. Коммутаторы могут фильтровать трафик в зависимости от интерфейса, с которого ушел пакет.
c. Коммутаторы могут фильтровать трафик в зависимости от интерфейса, на который пришел пакет.
d. Коммутаторы могут фильтровать трафик в зависимости от типа трафика.

33. Политика безопасности – это (выберите самое точное определение, один ответ)
a. Совокупность административных мер, которые определяют порядок прохода в компьютерные классы.
b. Межсетевые экраны, используемые в организации.
c. Множество критериев для предоставления сервисов безопасности.
d. Совокупность как административных мер, так и множества критериев для предоставления сервисов безопасности.

34. Основные классы атак на передаваемые по сети данные

a. Удаленная и локальная.
b. Видимая и невидимая.
c. Активная и пассивная.
d. Внешняя и внутренняя.

35. Атака называется пассивной, если
a. Оппонент не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения.
b. Оппонент не предполагает проникновение в систему.
c. Оппонент не использует никаких инструментальных средств для выполнения атаки.
d. Оппонент не анализирует перехваченные сообщения.

36. Риск — это
a. Вероятность того, что в системе остались неизвестные уязвимости.
b. Вероятность того, что конкретная атака будет осуществлена с использованием конкретной уязвимости.
c. Невозможность ликвидировать все уязвимости в информационной системе.
d. Невозможность исправить все ошибки в программном обеспечении.

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

38. Целостность – это
a. Невозможность несанкционированного доступа к информации.
b. Невозможность несанкционированного выполнения программ.
c. Невозможность несанкционированного изменения информации.
d. Невозможность несанкционированного просмотра информации.

39. Сервис, который обеспечивает невозможность несанкционированного изменения данных, называется
a. Конфиденциальностью.
b. Целостностью.
c. Аутентификацией.
d. Доступностью.

40. Многофакторная аутентификация означает
a. Аутентификация не может выполняться с помощью пароля.
b. Аутентификация должна выполняться с использованием смарт-карты.

c. Аутентифицируемой стороне необходимо предоставить несколько параметров, чтобы установить требуемый уровень доверия.

d. Аутентификация должна выполняться третьей доверенной стороной.

41. Основными источниками угроз информационной безопасности являются все указанное в списке:

a. Хищение жестких дисков, подключение к сети, инсайдерство

b. Перехват данных, хищение данных, изменение архитектуры системы

c. Хищение данных, подкуп системных администраторов, нарушение регламента работы

42. Виды информационной безопасности:

a. Персональная, корпоративная, государственная

b. Клиентская, серверная, сетевая

c. Локальная, глобальная, смешанная

43. Цели информационной безопасности – своевременное обнаружение, предупреждение:

a. несанкционированного доступа, воздействия в сети

b. инсайдерства в организации

c. чрезвычайных ситуаций

44. Основные объекты информационной безопасности:

a. Компьютерные сети, базы данных

b. Информационные системы, психологическое состояние пользователей

c. Бизнес-ориентированные, коммерческие системы

45. Основными рисками информационной безопасности являются:

a. Искажение, уменьшение объема, перекодировка информации

b. Техническое вмешательство, выведение из строя оборудования сети

c. Потеря, искажение, утечка информации

46. К основным принципам обеспечения информационной безопасности относится:

a. Экономической эффективности системы безопасности

b. Многоплатформенной реализации системы

c. Усиления защищенности всех звеньев системы

47. Основными субъектами информационной безопасности являются:

a. руководители, менеджеры, администраторы компаний

b. органы права, государства, бизнеса

c. сетевые базы данных, фаерволлы

48. К основным функциям системы безопасности можно отнести все перечисленное:

a. Установление регламента, аудит системы, выявление рисков

b. Установка новых офисных приложений, смена хостинг-компании

c. Внедрение аутентификации, проверки контактных данных пользователей

49. Принципом информационной безопасности является принцип недопущения:

a. Неоправданных ограничений при работе в сети (системе)

b. Рисков безопасности сети, системы

c. Презумпции секретности

50. Принципом политики информационной безопасности является принцип:

a. Невозможности миновать защитные средства сети (системы)

b. Усиления основного звена сети, системы

c. Полного блокирования доступа при риск-ситуациях

51. Принципом политики информационной безопасности является принцип:

a. Усиления защищенности самого незащищенного звена сети (системы)

b. Перехода в безопасное состояние работы сети, системы

c. Полного доступа пользователей ко всем ресурсам сети, системы

52. Принципом политики информационной безопасности является принцип:

a. Разделения доступа (обязанностей, привилегий) клиентам сети (системы)

b. Одноуровневой защиты сети, системы

c. Совместимых, однотипных программно-технических средств сети, системы

53. Наиболее распространены угрозы информационной безопасности корпоративной системы:

a. Покупка нелицензионного ПО

b. Ошибки эксплуатации и неумышленного изменения режима работы системы

c. Сознательного внедрения сетевых вирусов

54. Наиболее распространены угрозы информационной безопасности сети:

a. Распределенный доступ клиент, отказ оборудования

b. Моральный износ сети, инсайдерство
c. Сбой (отказ) оборудования, нелегальное копирование данных

55. Наиболее распространены средства воздействия на сеть офиса:
a. Слабый трафик, информационный обман, вирусы в интернет
b. Вирусы в сети, логические мины (закладки), информационный перехват
c. Компьютерные сбои, изменение администрирования, топологии

56. Утечкой информации в системе называется ситуация, характеризуемая:
a. Потерей данных в системе
b. Изменением формы информации
c. Изменением содержания информации

57. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
a. Целостность
b. Доступность
c. Актуальность

58. Угроза информационной системе (компьютерной сети) – это:
a. Вероятное событие
b. Детерминированное (всегда определенное) событие
c. Событие, происходящее периодически
59. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
a. Регламентированной
b. Правовой
c. Защищаемой

60. Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:
a. Программные, технические, организационные, технологические
b. Серверные, клиентские, спутниковые, наземные
c. Личные, корпоративные, социальные, национальные

61. Окончательно, ответственность за защищенность данных в компьютерной сети несет:
a. Владелец сети
b. Администратор сети
c. Пользователь сети

62. Политика безопасности в системе (сети) – это комплекс:

a. Руководств, требований обеспечения необходимого уровня безопасности

b. Инструкций, алгоритмов поведения пользователя в сети

c. Нормы информационного права, соблюдаемые в сети

63. Наиболее важным при реализации защитных мер политики безопасности является:

a. Аудит, анализ затрат на проведение защитных мер

b. Аудит, анализ безопасности

c. Аудит, анализ уязвимостей, риск-ситуаций

64. Под информационной безопасностью понимается…

a. защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.

b. программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия

c. нет правильного ответа

65. Защита информации – это..

a. комплекс мероприятий, направленных на обеспечение информационной безопасности.

b. процесс разработки структуры базы данных в соответствии с требованиями пользователей

c. небольшая программа для выполнения определенной задачи

66. От чего зависит информационная безопасность?

a. от компьютеров

b. от поддерживающей инфраструктуры

c. от информации

67. Основные составляющие информационной безопасности:

a. Целостность

b. Достоверность

c. Конфиденциальность

68. Доступность – это…

a. возможность за приемлемое время получить требуемую информационную услугу.

b. логическая независимость

c. нет правильного ответа

69. Целостность – это..

a. целостность информации
b. непротиворечивость информации
c. защищенность от разрушения

70. Конфиденциальность – это..
a. защита от несанкционированного доступа к информации
b. программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
c. описание процедур
71. Для чего создаются информационные системы?
a. получения определенных информационных услуг
b. обработки информации
c. все ответы правильные
72. Целостность можно подразделить:
a. Статическую
b. Динамичную
c. структурную
73. Где применяются средства контроля динамической целостности?
a. анализе потока финансовых сообщений
b. обработке данных
c. при выявлении кражи, дублирования отдельных сообщений
74. Какие трудности возникают в информационных системах при конфиденциальности?
a. сведения о технических каналах утечки информации являются закрытыми
b. на пути пользовательской криптографии стоят многочисленные технические проблемы
c. все ответы правильные
75. Угроза – это…
a. потенциальная возможность определенным образом нарушить информационную безопасность
b. система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
c. процесс определения отвечает на текущее состояние разработки требованиям данного этапа
76. Атака – это…
a. попытка реализации угрозы
b. потенциальная возможность определенным образом нарушить информационную безопасность
c. программы, предназначенные для поиска необходимых программ.
77. Источник угрозы – это..
a. потенциальный злоумышленник
b. злоумышленник
c. нет правильного ответа

78. Окно опасности – это…

a. промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.

b. комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области

c. формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

79. Какие события должны произойти за время существования окна опасности?

a. должно стать известно о средствах использования пробелов в защите.

b. должны быть выпущены соответствующие заплаты.

c. заплаты должны быть установлены в защищаемой И.С.

80. Угрозы можно классифицировать по нескольким критериям:

a. по спектру И.Б.

b. по способу осуществления

c. по компонентам И.С.

81. По каким компонентам классифицируется угрозы доступности:

a. отказ пользователей

b. отказ поддерживающей инфраструктуры

c. ошибка в программе

82. Основными источниками внутренних отказов являются:

a. отступление от установленных правил эксплуатации

b. разрушение данных

c. все ответы правильные

83. Основными источниками внутренних отказов являются:

a. ошибки при конфигурировании системы

b. отказы программного или аппаратного обеспечения

c. выход системы из штатного режима эксплуатации

84. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

a. невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности

b. обрабатывать большой объем программной информации

c. нет правильного ответа

85. Какие существуют грани вредоносного П.О.?

a. вредоносная функция

b. внешнее представление

c. способ распространения

86. По механизму распространения П.О. различают:

a. Вирусы

b. Черви

c. все ответы правильные

87. Вирус – это…

a. код обладающий способностью к распространению путем внедрения в другие программы

b. способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов

c. небольшая программа для выполнения определенной задачи

88. Черви – это…

a. код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения

b. код обладающий способностью к распространению путем внедрения в другие программы

c. программа действий над объектом или его свойствами

89. Конфиденциальную информацию можно разделить:

a. Предметную

b. Служебную

c. глобальную

90. Природа происхождения угроз:

a. Случайные

b. Преднамеренные

c. природные

91. Предпосылки появления угроз:

a. Объективные

b. Субъективные

c. преднамеренные

92. К какому виду угроз относится присвоение чужого права?

a. нарушение права собственности

b. нарушение содержания

c. внешняя среда

93. Отказ, ошибки, сбой – это:

a. случайные угрозы

b. преднамеренные угрозы

c. природные угрозы

94. Отказ - это…

a. нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

b. некоторая последовательность действий, необходимых для выполнения конкретного задания

c. структура, определяющая последовательность выполнения и взаимосвязи процессов

95. Ошибка – это…

a. неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния

b. нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

c. негативное воздействие на программу

96. Сбой – это…

a. такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент

b. неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния

c. объект-метод

97. Побочное влияние – это…

a. негативное воздействие на систему в целом или отдельные элементы

b. нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент

c. нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

98. СЗИ (система защиты информации) делится:

a. ресурсы автоматизированных систем

b. организационно-правовое обеспечение

c. человеческий компонент

99. Что относится к человеческому компоненту СЗИ?

a. системные порты

b. администрация

c. программное обеспечение

100. По уровню обеспеченной защиты все системы делят:

a. сильной защиты

b. особой защиты

c. слабой защиты

Задания в открытой форме

1) Система … представляет организованную совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз.

2) … включает в себя анализ возможных угроз и выбор соответствующих мер противодействия, являющихся совокупностью тех норм, правил поведения, которыми пользуется конкретная организация при обработке информации и ее защите.

3) … представляет собой общесистемные и прикладные программы и средства, осуществляющие безопасную обработку данных и безопасно использующие ресурсы системы.

4) … обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств компьютера с целью обеспечения доступности, целостности и конфиденциальности, связанных с ним ресурсов.

5) …– ущерб, который понесет компания от потери ресурса

6) … – степень влияния реализации угрозы на ресурс, т.е. как сильно реализация угрозы повлияет на работу ресурса.

7) В концепции обеспечения информационной безопасности предприятия определяются…

8) … — анализ реализованных мер защиты информации, который позволит определить степень соответствия требованиям основных нормативно-правовых актов, а также оценить реальный уровень защищенности организации от возможных угроз.

9) Под термином … понимается системный процесс получения и оценки объективных данных о текущем состоянии обеспечения безопасности информации.

10) … – любой контейнер, предназначенный для хранения информации, подверженный угрозам информационной безопасности (сервер, рабочая станция, переносной компьютер).

11) … – действие, которое потенциально может привести к нарушению безопасности

12) … критерии предъявляются к возможностям мер и средств защиты информации, определяющим желательный режим работы ИС. Включают в себя требования: организационные, эксплуатационные и к безопасности ИТ.

13) … критерии предъявляются к действиям разработчика системы, документам для оценивания и работе самой организации. Включают требования доверия к мерам к СЗИ в информационных системах, а также к их разработке и эксплуатации.

14) … — положения политик безопасности, затрагивающих ОО и учитывающих его особенности;

15) … — меры физической защиты, персонал и его специфика;

16) … — назначение ОО, предполагаемые области его применения.

17) … — типовой набор требований для некоторой категории ОО.

18) … — документ, содержащий требования безопасности для конкретной разработки, выполнение которых обеспечивает достижение поставленных целей безопасности.

19) … - характеристика средств системы, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню и глубине в зависимости от класса защищенности

20) … - это активный компонент защиты, включающий в себя анализ возможных угроз и рисков, выбор мер противодействия и методологию их применения.

Задание на установление правильной последовательности

1. Установить этапы 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.

2. Установить этапы построения политики безопасности:

1) Выбор и установка средств защиты;

2) Организация обслуживания по вопросам информационной безопасности;

3) Создание системы периодического контроля информационной безопасности

4) Обследование информационной системы на предмет установления организационной и информационной структуры и угроз безопасности информации;

5) Подготовка персонала работе со средствами защиты;

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

1) Реализация аутентификации пользователя;

2) Реализация многозадачности;

3) Создание кольцевой системы защиты процессора;

4) Создание виртуальных контейнеров для запуска приложений;

5) Подготовка аудиторского отчета.

4. Установите последовательность этапов работы по обеспечению информационной безопасности:

1) Определение требований к системе защиты информации;

2) Выбор контрмер, обеспечивающих режим иб, и средств защиты;

3) Разработка, внедрение и организация использования выбранных мер, способов и средств защиты;

4) Осуществление текущего контроля целостности информационных ресурсов и средств защиты и плановый аудит системы управления информационной безопасностью.

5. Установите этапы анализа защищенности:

1) Анализ полученных данных и уязвимостей.

2) Выработка рекомендаций.

3) Подготовка отчетных документов.

4) Инициирование и планирование Определение области и границ аудита.

5) Обследование, документирование и сбор информации.

6. Установите этапы внедрения межсетевого экрана:

1) Планирование
2) Тестирование
3) Развертывание
4) Управление
5) Конфигурирование

7. Установите этапы развития информационных технологий:

1) «электрическая» технология.
2) «электронная» технология.
3) «компьютерная» технология.
4) «ручная» технология.
5) «механическая» технология.

8. Расположите этапы развития информационных технологий в соответствии с проблемами, стоящими на пути информатизации общества.

1) Максимальное удовлетворение потребностей пользователя и создание соответствующего интерфейса работы в компьютерной среде.
2) Обработка больших объемов данных в условиях ограниченных возможностей аппаратных средств.
3) Отставание программного обеспечения от уровня развития аппаратных средств.
4) Выработка соглашений и установление стандартов, протоколов для компьютерной связи; организация доступа к стратегической информации; организация защиты и безопасности информации.

9. Процесс разработки в среде ООП включает в себя следующие этапы:

1) Сопровождение
2) Модификация
3) Программирование
4) Анализ
5) Проектирование

10. 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.

11. Выберите правильную последовательность этапов защиты информации, информационных технологий и автоматизированных систем от атак:

1) Анализ рисков для активов организации, включающий в себя выявление ценных активов и оценку возможных последствий реализации атак с использованием скрытых каналов

2) Реализация защитных мер по противодействию скрытых каналов

3) Организация контроля за противодействием скрытых каналов.

4) Выявление скрытых каналов и оценка их опасности для активов организации

12. Выберите правильную последовательность этапов жизненного цикла информационного сервиса:

1) Сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию.

2) На данном этапе выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение.

3) На данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно закупка.

4) На данном этапе сервис не только работает и администрируется, но и подвергается модификациям.

13. Выберите последовательность приоритетных этапов защиты информации:

1) Защита информации от несанкционированного доступа;

2) Защита информации в системах связи;

3) Защита юридической значимости электронных документов;

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

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

6) Защита от несанкционированного копирования и распространения программ и ценной компьютерной информации.

14. Выберите правильную последовательность этапов работы по обеспечению режима ИБ:

1) Выявление максимально полного множества потенциальных угроз, способов и каналов их осуществления;

2) Определение и выработка политики информационной безопасности;

3) Определение совокупности целей создания системы иб и сферы (границ) ее функционирования;

4) Выявление уязвимостей, проведение оценки рисков, формирование методик управление рисками;

5) Выберите правильную последовательность этапов работы по обеспечению режима ИБ:

15. Установите последовательность этапов работы по обеспечению информационной безопасности:

1) Определение требований к системе защиты информации;
2) Выбор контрмер, обеспечивающих режим иб, и средств защиты;
3) Разработка, внедрение и организация использования выбранных мер, способов и средств защиты;
4) Осуществление текущего контроля целостности информационных ресурсов и средств защиты и плановый аудит системы управления информационной безопасностью.

16. Выберите правильную последовательность этапов процесса управления рисками:

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

17. Выберите правильную последовательность этапов обеспечения информационной:

1) Оценка стоимости;
2) Реализация политики;
3) Квалифицированная подготовка специалистов;
4) Аудит;
5) Разработка политики безопасности;

18. Выберите последовательность уровней безопасности информации:

1) Административный уровень
2) Процедурный уровень
3) Программно-технический уровень
4) Законодательный уровень

19. Выберите правильную последовательность этапов оценки угроз безопасности информации:

7) Определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;

8) Инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;

9) Определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;

10) Оценка способов реализации (возникновения) угроз безопасности информации;

11) Оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;

12) Оценка сценариев реализации угроз безопасности информации в системах и сетях.

20. Выберите правильную последовательность этапов построения политики безопасности:

1) Выбор и установка средств защиты;

2) Организация обслуживания по вопросам информационной безопасности;

3) Создание системы периодического контроля информационной безопасности

4) Обследование информационной системы на предмет установления организационной и информационной структуры и угроз безопасности информации;

5) Подготовка персонала работе со средствами защиты;

Задание на установление соответствия

1. Установить соответствие основных видов подходов при проектировании архитектуры системы ИБ:

1) Объектный	a) В подходе ИС представляется как совокупность объектов, для каждого из которых применен объектный подход, а для совокупности взаимосвязанных объектов - прикладной. Такая методика оказывается более трудоемкой на стадии проектирования, однако часто дает хорошую экономию средств при внедрении, эксплуатации и сопровождении системы защиты информации.
2) Прикладной	b) Подход строит защиту информации на основании физической структуры того

	или иного объекта (здания, подразделения, предприятия). Применение объектного подхода предполагает использование набора универсальных решений для обеспечения механизмов безопасности, поддерживающих однородный набор организационных мер.
3) Смешанный	c) Подход "привязывает" механизмы безопасности к конкретному приложению. Пример такого подхода - защита подсистемы либо отдельных зон автоматизации (бухгалтерия, склад, кадры, проектное бюро, аналитический отдел, отделы маркетинга и продаж и т.д.). При большей полноте защитных мер такого подхода у него имеются и недостатки, а именно: необходимо увязывать различные по функциональным возможностям средства безопасности для минимизации затрат на администрирование и эксплуатацию, а также задействовать уже существующие средства защиты информации для сохранения инвестиций..

2. Установить соответствие нарушителей по уровням знания АСОД:

1) 1 уровень	a) Обладает высоким уровнем знаний и опытом работы с техническими средствами системы и ее обслуживания.
2) 2 уровень	b) Знает функциональные особенности АСОД, основные закономерности формирования в нестандартных массивах данных и потоков запросов к ним. Умеет пользоваться штатными средствами.
3) 3 уровень	c) Знает структуру, функции и механизмы действия средств защиты, их слабые и сильные стороны.

4) 4 уровень	d) Обладает уровнем знаний в области программирования и вычислительных технологий, проектирования и эксплуатации АСОД.

3. Установить соответствие нарушителей по уровням возможностей (используемым методам и вопросам):

1) 1 уровень	a) Применяющие пассивные средства (технические средства перехвата без модификации компонентов системы).
2) 2 уровень	b) Применяющие только агентурные методы получения сведений
3) 3 уровень	c) Использующие только штатные средства и недостатки системы защиты, их сильные и слабые стороны.
4) 4 уровень	d) Применяющие методы и действия активного воздействия (модификация и подключение дополнительных технических устройств).

4. Установить соответствие оценки рисков в зависимости от факторов:

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

5. Установить соответствие:

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

6. Установить соответствие:

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

7. Установить соответствие основных видов систем обнаружения вторжений:

1) Сетевые (NIDS)	a) Для проверки специализированных прикладных протоколов.
2) Основанные на прикладных протоколах СОВ (APIDS)	b) Анализируют журналы приложений, состояние хостов, системные вызовы.
3) Узловые или Host-Based (HIDS)	c) Для проверки сетевого трафика с коммутатора.

8. Установить соответствие:

1) Планирование	a) Отладка программы в соответствии с индивидуальными запросами конкретного предприятия базируется на контроле конфиденциальных сведений в соответствии с признаками особенной документации, принятой в компании
2) Реализация	b) Заключается в точном определении программы защиты данных. Ответ на простой, казалось бы, вопрос: «Что будем защищать?»
3) Корректировка	c) Проанализировав информацию, собранную на этапе тестовой эксплуатации DLP-решения, приступают к перенастройке ресурса.

9. Установить соответствие видов угроз:

1) Аппаратная	a) Когда возможен несанкционированный доступ к данным и их потеря.
2) Вероятность утечки	b) Когда существует вероятность нарушения работоспособности оборудования.
3) Нестабильность ПО	c) Когда есть вероятность некорректной

	работы программного обеспечения.

10. Установить соответствие:

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

11. Установить соответствие:

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

12. Установить соответствие:

1) Основные организационные и организационно-технические мероприятия по созданию и	a) Мероприятия по обеспечению достаточного уровня физической защиты всех компонентов АСОД (противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности средств вычислительной

поддержанию функционирования системы защиты включают:	техники, носителей информации и т.п.).
2) Разовые мероприятия включают:	b) Распределение реквизитов разграничения доступа (пароли, ключи шифрования и т.д.).
3) Периодически проводимые мероприятия включают:	c) Общесистемные мероприятия по созданию научно-технических и методологических основ защиты АСОД.
4) Постоянно проводимые мероприятия включают:	d) Мероприятия проводимые и повторяемые только при полном пересмотре принятых решений.

13. Установить соответствие технических каналов утечки информации:

1) Прямой акустический (окна, двери, щели, проемы)	a) Электронные спетоскопы, установленные в смежном помещении
2) Акусто-вибрационный (через ограждающие кострукции)	b) Направленные микрофоны, установленные за границей КЗ
3) Акусто-электрический (через соединительные линии ВТСС)	c) Специальные низкочастотные усилители, подсоединенные к соединительным линиям ВТСС, обладающие «микрофонным» эффектом
4) Акусто-электромагнитный (параметрический)	d) Защищенность рассматривается как увязка вопросов защиты информации

14. Установить соответствие технических каналов утечки информации:

1) Прямой акустический (окна, двери, щели, проемы)	a) Электронные устройства перехвата речевой информации с датчиками контактного типа, установленными на инженерно-технических коммуникациях
2) Акусто-вибрационный (через	b) Специализированные высокочувствительные микрофоны, установленные в воздуховодах или

ограждающие кострукции)	смежных помещениях
3) Акусто-электрический (через соединительные линии ВТСС)	c) Аппаратура высокочастотного облучения, установленная за пределами КЗ
4) Акусто-электромагнитный (параметрический)	d) Аппаратура «высокочастотного навязывания», подключенная к соединительным линиям ВТСС

15. Установить соответствие технических каналов утечки информации:

1) Прямой акустический (окна, двери, щели, проемы)	a) Электронные устройства перехвата речевой информации с датчиками микрофонного типа при условии неконтролируемого доступа к ним посторонних лиц
2) Акусто-оптический (через оконные стекла)	b) Лазерные акустические локационные системы, находящиеся за пределами КЗ
3) Акусто-электрический (через соединительные линии ВТСС)	c) Специальные низкочастотные усилители, подсоединенные к соединительным линиям ВТСС, обладающие «микрофонным» эффектом
4) Акусто-электромагнитный (параметрический)	d) Прослушивание разговоров, ведущихся в помещении без применения технических средств посторонними лицами

16. Установить соответствие средств информационной защиты:

1) SIEM-системы	a) Виртуально-частная сеть определяет использование собственной частной сети внутри общедоступной. Поэтому ваше приложение, работающее по VPN, будет надежно защищено.
2) CloudAV	b) Они собирают информацию о возможных угрозах из различных источников: файервол, антивирус, межсетевой экран и др., потом проводят анализ и могут среагировать на вероятность возникновения потенциальной угрозы, предупредив о

	ней заранее.
3) Брандмаузер и фаервол	c) Это специальная система шифрования вашей информации. Шифровка происходит таким образом, что для того, чтобы расшифровать нужную информацию, необходимо обладать специальным шифром.
4) Криптографическое преобразование	d) Это специализированные средства, которые контролируют выход во всемирную паутину, при необходимости фильтруют или блокируют сетевой трафик.

17. Установить соответствие средств информационной защиты:

1) Программы-антивирусы	a) Это специальные технологии, которые предотвращают потерю конфиденциальной информации. Как правило, данная технология используется большими предприятиями, так как требует больших финансовых и трудоресурсных затрат.
2) VPN	b) Борются с самыми распространенными вирусами, также способны восстанавливать поврежденные файлы.
3) DLP-решения	c) Это облачные решения для обеспечения антивирусной защиты вашего ресурса.

18. Установить соответствие степеней происхождения угрозы информационной безопасности:

1) Естественная	a) Данные угрозы, в свою очередь, делятся на 2 подкатегории: преднамеренная подкатегория — это действия хакеров, конкурентов, недобросовестных сотрудников и т. д., непреднамеренная — действия происходят из-за людей по их неосторожности.
2) Искусственная	b) Это те угрозы, которые не зависят от деятельности человека: землетрясения, ураганы, смерчи, дожди, молнии и т. д.

3) Внутренняя	c) Все угрозы, которые происходят вне системы.
4) Внешняя	d) Угроза исходит изнутри самой системы.

19. Установить соответствие каналов утечки:

1) Несанкционированное копирование, уничтожение или подделка информации	a) Ошибки персонала и пользователей
2) Перебои электропитания	b) Из-за некорректной работы программ
3) Случайное уничтожение или изменение данных	c) Потери информации, связанная с несанкционированным доступом
4) Потеря или изменение данных при ошибках по	d) Сбои оборудования, при котором теряется информация

20. Установить соответствие:

1) Программно-аппаратные (технические) методы	a) Для обеспечения безопасности используются приемы «перестраховки», с помощью которых исключается возможность ошибочного или несанкционированного проникновения в информационную систему
2) Физическая защита	b) Для осуществления информационной защиты используются специальные компьютерные технологии. С их помощью можно скрыть важные данные, не допустить утечки во время пересылки через интернет
3) Морально-этические методы	c) Профилактические действия, в основном, воспитательного характера
4) Технологические приемы	d) Мероприятия направлены на снижение риска потери данных и выявление лиц, пытающихся проникнуть на охраняемую территорию или в информационную систему

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. Выберите конкретный объект (например, банк, государственную организацию или крупное предприятие) и проведите исследование существующих технологий обеспечения информационной безопасности для данного объекта. Опишите, какие технологии применяются и как они способствуют защите информации.

2. Разработайте план внедрения технологий обеспечения информационной безопасности для выбранного объекта. Учтите особенности объекта, его информационные ресурсы, угрозы и уязвимости. Определите последовательность внедрения технологий и ресурсы, необходимые для успешной реализации.

3. Сравните различные технологии обеспечения информационной безопасности и определите их преимущества и недостатки для конкретного объекта. Ваша задача - выбрать наиболее подходящие технологии, учитывая бюджет, требования безопасности и специфику объекта.

4. Проведите анализ эффективности и эффективности выбранных технологий обеспечения информационной безопасности. Оцените, насколько эти технологии способны предотвратить угрозы и уязвимости, а также как они влияют на работу объекта. Сравните полученные результаты с требованиями безопасности и сформулируйте рекомендации по улучшению.

5. Исследуйте новые технологии обеспечения информационной безопасности и их применимость для объекта. Проведите анализ преимуществ, ограничений и потенциальных рисков использования этих технологий. Определите, насколько они могут улучшить общую защиту информации на объекте и предложите рекомендации по их внедрению.

6. Разработайте план обновления и модернизации технологий обеспечения информационной безопасности для объекта. Учтите текущую ситуацию, новые требования безопасности и доступные ресурсы. Определите этапы обновления, бюджет, роли и ответственности сотрудников, а также ожидаемые результаты.

7. Анализ защищенности сетевой инфраструктуры: Вам предстоит провести анализ защищенности сетевой инфраструктуры компании, идентифицировать уязвимые места и предложить соответствующие технологии и меры для укрепления безопасности сети.

8. Разработка политики управления доступом: Вашей задачей будет разработка политики управления доступом к информационным ресурсам компании. Вы должны определить необходимые технологии (например, аутентификация, авторизация, контроль доступа), которые помогут обеспечить правильное управление доступом и защиту конфиденциальных данных.

9. Построение безопасных архитектурных решений: Вам предстоит разработать безопасные архитектурные решения для информационных систем компании. Задача включает выбор и применение соответствующих технологий, таких как сегментация сети, шифрование данных, защита от DDoS-атак и другие, с целью обеспечения надежности и безопасности системы.

10. Оценка эффективности технологий безопасности: Вам нужно провести оценку эффективности используемых технологий безопасности в компании. Вы должны определить, насколько эффективно они выполняют свои функции и вносят вклад в общую безопасность информационных объектов. При необходимости предложите альтернативные технологии или улучшения существующих.

11. Разработка плана реагирования на инциденты: Вам поручено разработать план реагирования на информационные инциденты в компании. Задача включает определение необходимых технологий (например, мониторинг безопасности, системы обнаружения вторжений), процедур и

ресурсов для своевременного обнаружения и реагирования на инциденты безопасности.

12. Анализ безопасности сети: Ваша компания получила заказ на анализ безопасности сети крупной организации. Задача состоит в том, чтобы провести полный анализ сетевой инфраструктуры и выявить потенциальные уязвимости, рекомендовать соответствующие технологии и меры по обеспечению безопасности сети.

13. Разработка политики доступа: Вам было поручено разработать политику доступа для информационной системы компании. Задача состоит в определении правил доступа к ресурсам информационной системы, включая определение различных уровней доступа, идентификацию пользователей и ролей, а также рекомендацию соответствующих технологий для реализации этой политики.

14. Проведение аудита безопасности: Ваша компания получила заказ на проведение аудита безопасности для организации. Задача состоит в оценке существующих технологий обеспечения безопасности, выявлении слабых мест и рекомендации улучшений. Ваш аудит должен включать анализ защитных механизмов, проверку соответствия нормативным требованиям и обзор политик безопасности.

15. Разработка системы мониторинга безопасности: Вам было поручено разработать систему мониторинга безопасности для крупной компании. Задача состоит в определении соответствующих технологий мониторинга, разработке метрик и индикаторов безопасности, а также создании механизма автоматического обнаружения и оповещения о потенциальных угрозах.

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.