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

Теоретические основы компьютерной безопасности
(наименование учебной дисциплины)

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

Курск – 2023

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

Тема 1. Основные аспекты построения системы информационной безопасности.

1. Основные объекты информационной безопасности
2. Что является основными рисками информационной безопасности
3. Что относят к основным принципам обеспечения информационной безопасности
4. Что является принципом политики информационной безопасности
5. Какие основные цели должна преследовать система информационной безопасности организации?
6. Какие основные компоненты должны входить в систему информационной безопасности и как они взаимодействуют между собой?
7. Каким образом должны быть определены роли и полномочия людей, ответственных за обеспечение информационной безопасности в организации?
8. Как происходит процесс идентификации и классификации информационных активов, а также определение уровней их защиты?
9. Каким образом организация обеспечивает непрерывность бизнес-процессов и восстановление после сбоев или инцидентов в системе информационной безопасности?
10. Как проводится аудит и мониторинг системы информационной безопасности для выявления уязвимостей и своевременного реагирования на потенциальные угрозы?

Тема 2. Угрозы информационной безопасности, оценка риска их возникновения.

1. Что относят к правовым методам обеспечения информационной безопасности
2. Перечислите виды информационной безопасности
3. Цели информационной безопасности
4. Что является угрозой информационной системы
5. Какие основные типы угроз информационной безопасности существуют и как они могут нанести вред организации?
6. Как проводится оценка риска возникновения угроз информационной безопасности и какие факторы учитываются при этом?

7. Каким образом определяется вероятность возникновения угрозы информационной безопасности и какие критерии применяются для оценки её воздействия?

8. Какие меры безопасности могут быть предприняты для сокращения вероятности возникновения угроз информационной безопасности?

9. Как осуществляется мониторинг и обновление оценки риска, чтобы быть в курсе изменений угроз и принимать соответствующие меры?

10. Какие процедуры и планы чрезвычайных ситуаций разрабатываются для реагирования на угрозы информационной безопасности и смягчения их последствий?

Тема 3. Персональные данные, защита авторских прав.

1. В каком нормативном правовом акте закреплены все виды конфиденциальной информации?

2. Что такое персональные данные в соответствии с ФЗ-152?

3. Какую информацию запрещено относить к конфиденциальной в соответствии с законом РФ?

4. Раскройте понятие "конфиденциальный документ"

5. Перечислите 4 вида тайн относящихся к персональным данным. В случае если Вам известно больше видов тайн относящихся к ПД их следует перечислить.

6. Какие данные считаются персональными и почему их защита является важной составляющей информационной безопасности?

7. Какие принципы и нормы регулируют обработку и хранение персональных данных в соответствии с требованиями конфиденциальности?

8. Каким образом организация может обеспечить безопасность персональных данных в процессе их сбора, хранения и передачи?

9. Какие меры и политики защиты авторских прав должны быть включены в систему информационной безопасности организации?

10. Как осуществляется мониторинг и контроль доступа к персональным данным и материалам с авторскими правами?

11. Каким образом происходит уничтожение или анонимизация персональных данных после их использования или устранения необходимости их хранения?

Тема 4. Выявление контрафактной продукции.

1. Какие преимущества и недостатки объективных и эвристических методов экспертизы?

2. Что понимается под сенсорным анализом и сенсорной чувствительностью?

3. Что такое порог чувствительности, распознавания?

4. Причины фальсификации продовольственных товаров в современных условиях
5. Место и роль идентификации при оценке степени соответствия товара
6. Какие методы и технологии могут быть использованы для выявления контрафактной продукции в информационной среде?
7. Как происходит мониторинг и идентификация поддельных или нелицензионных программных продуктов?
8. Каким образом проводится анализ и проверка подлинности цифровых документов и электронной печати для предотвращения контрафакции?
9. Какие методы могут быть применены для обнаружения плагиата или незаконного использования интеллектуальной собственности?
10. Как осуществляется сотрудничество с органами правопорядка и другими организациями в борьбе с контрафактной продукцией?
11. Какие проведены регулярные проверки и ревизии в организации, чтобы обнаруживать и предотвращать случаи контрафакции?

Тема 5. Криптографические методы защиты.

1. Что такое шифрование?
2. Что такое кодирование?
3. Для восстановления защитного текста требуется
4. Сколько лет назад появилось шифрование?
5. Как работают криптографические методы защиты и как они могут обеспечить конфиденциальность и целостность информации?
6. Какие алгоритмы шифрования и протоколы могут быть применены для защиты данных и обмена информацией?
7. Как осуществляется генерация и хранение криптографических ключей, и какие меры обеспечивают их конфиденциальность и защиту от несанкционированного использования?
8. Каким образом осуществляется аутентификация и проверка подлинности сообщений и данных с использованием криптографических методов?
9. Какие меры безопасности применяются для защиты криптографических систем от взлома или компрометации?
10. Как осуществляется управление и обновление криптографических протоколов и алгоритмов для обеспечения их актуальности и надежности?

Тема 6. Методы выбора системы защиты информации.

1. Какую длину имеет IP-адрес
2. Какую длину блока использует алгоритм DES
3. Какую длину ключа использует алгоритм DES
4. Для чего используется алгоритм Диффи-Хеллмана

5. Какие факторы следует учитывать при выборе системы защиты информации для организации?

6. Как происходит анализ требований и потребностей организации для определения необходимых функций и возможностей системы защиты информации?

7. Какие критерии принятия решения используются при выборе системы защиты информации, такие как совместимость, надежность, цена и поддержка?

8. Каким образом проводится сравнительный анализ различных вендоров и поставщиков систем защиты информации?

9. Как осуществляется тестирование и оценка производительности выбранной системы защиты информации перед ее внедрением?

10. Как осуществляется обучение и подготовка сотрудников организации для работы с выбранной системой защиты информации?

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.

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа № 1 «Оценка рисков информационной безопасности»

1. Какие основные шаги необходимо выполнить при проведении оценки рисков информационной безопасности?
2. Какие факторы необходимо учитывать при оценке рисков информационной безопасности?
3. Какие методы и инструменты могут быть использованы для оценки рисков информационной безопасности?
4. Как идентифицировать потенциальные угрозы безопасности информации в организации?
5. Какие преимущества имеют качественные и количественные методы оценки рисков информационной безопасности?
6. Какие документы и информацию требуется собрать для проведения оценки рисков информационной безопасности?
7. Каким образом определить уязвимости в информационной системе и их ранг по степени угрозы?
8. Какие факторы могут повлиять на возникновение и воздействие угроз информационной безопасности?
9. Как определить вероятность возникновения и последствий угроз для информационных активов организации?
10. Каким образом оценить финансовые, репутационные и операционные риски в области информационной безопасности?

Практическая работа № 2 «Оценка эффективности организации информационной безопасности»

1. Какие основные компоненты оценки эффективности информационной безопасности включает в себя?
2. Какими методами можно оценить уровень защищенности информации в организации?
3. Какие факторы и угрозы следует учитывать при оценке эффективности информационной безопасности?
4. Какие показатели и метрики могут быть использованы для измерения эффективности организации информационной безопасности?
5. Какие шаги необходимо предпринять, чтобы провести успешную оценку эффективности информационной безопасности?
6. Какие рекомендации можно дать для улучшения эффективности организации информационной безопасности на основе результатов оценки?
7. Как влияют политики безопасности на эффективность информационной безопасности организации?
8. Какую роль играет обучение и осведомленность персонала в оценке эффективности информационной безопасности?

9. Как оценить уровень соответствия организации нормативным требованиям и стандартам в области информационной безопасности?

10. Какие типичные уязвимости информационной безопасности могут быть выявлены при оценке эффективности организации?

Практическая работа № 3 «Реализация модели информационной безопасности»

1. Каковы основные шаги при реализации модели информационной безопасности в организации?
2. Какие факторы необходимо учесть при выборе подхода к реализации модели информационной безопасности?
3. Какие преимущества можно получить, используя стандартные подходы к реализации модели информационной безопасности?
4. Какую роль играют политики безопасности в успешной реализации модели информационной безопасности?
5. Какие технические меры могут быть приняты в рамках модели информационной безопасности?
6. Каким образом обучение персонала и повышение осведомленности способствуют реализации модели информационной безопасности?
7. Как организационные структуры и роли связаны с реализацией модели информационной безопасности?
8. Какие компоненты модели информационной безопасности требуют аудита и управления рисками?
9. Какие инструменты и технологии можно использовать для реализации модели информационной безопасности?
10. Каковы главные вызовы или проблемы, с которыми можно столкнуться при реализации модели информационной безопасности?

Практическая работа № 4 «Изучение парольных систем защиты»

1. Какие основные принципы лежат в основе парольных систем защиты?
2. Какие проблемы возникают при использовании слабых паролей?
3. Какие методы аутентификации используются в парольных системах защиты?
4. Что такое хеширование паролей и почему оно важно?
5. Какие меры безопасности рекомендуется применять при хранении паролей?
6. Что такое "политика паролей" и какие принципы она должна включать?
7. Какие средства доступны для обнаружения и предотвращения атак на парольные системы?
8. Какие методы можно использовать для создания сильных паролей?

9. Какие рекомендации по безопасности паролей при общем использовании компьютера?

10. Как можно защититься от перехвата паролей при использовании открытых Wi-Fi сетей?

Практическая работа № 5 «Изучение характеристик защищенности паролей»

1. Каковы основные критерии стойкости паролей?
2. Какова рекомендуемая минимальная длина пароля для обеспечения безопасности?
3. Какие типы символов следует использовать в паролях для повышения их стойкости?
4. Почему важно избегать использования обычных слов и фраз в паролях?
5. Какие риски связаны с использованием персональной информации (например, даты рождения или имен) в паролях?
6. Какой роль длины пароля в защите от метода перебора?
7. Почему генерация паролей случайным образом способствует их стойкости?
8. Какие типы алгоритмов можно использовать для генерации непредсказуемых паролей?
9. Какие шаблоны паролей следует избегать?
10. Какой инструмент можно использовать для оценки стойкости сгенерированных паролей?

Практическая работа № 6 «Целостность данных. Модель Кларка-Вилсона.»

1. Что такое целостность данных и почему она является важным аспектом информационной безопасности?
2. Какая роль у модели Кларка-Вилсона в обеспечении целостности данных?
3. Какие основные принципы лежат в основе модели Кларка-Вилсона?
4. Каковы основные компоненты модели Кларка-Вилсона?
5. Что означает понятие "целостность данных в широком смысле" в контексте модели Кларка-Вилсона?
6. Как модель Кларка-Вилсона помогает в предотвращении несанкционированного доступа к данным?
7. Как организации могут выполнять аутентификацию данных с использованием модели Кларка-Вилсона?
8. Какие виды угроз могут негативно повлиять на целостность данных?
9. Какая роль у криптографических хэш-функций в обеспечении целостности данных по модели Кларка-Вилсона?

10. Какие техники используются для обнаружения и восстановления поврежденных данных согласно модели Кларка-Вилсона?

Критерии оценки:

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.

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

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

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

1.3 ПРОИЗВОДСТВЕННЫЕ ЗАДАЧИ

1. Задача разработки политики доступа к информации: Ваша компания хочет установить строгую политику доступа к информации с целью обеспечения безопасности данных. Ваша задача - разработать политику, определяющую различные уровни доступа к информации в зависимости от роли и обязанностей сотрудников. Вам нужно учесть требования безопасности и обеспечить соответствие политики законодательству и стандартам безопасности.

2. Задача анализа уязвимостей системы: Вам предоставлены компьютерные системы вашей компании, и вам необходимо провести анализ уязвимостей. Ваша задача - использовать соответствующие инструменты и методы для обнаружения уязвимостей в сетевой инфраструктуре, операционных системах и приложениях. После обнаружения уязвимостей вы

должны предложить меры по их устранению и улучшению безопасности системы.

3. Задача разработки системы мониторинга безопасности: Ваша компания нуждается в непрерывном мониторинге безопасности системы. Ваша задача - разработать систему мониторинга, которая будет отслеживать активность в сети и на компьютерах, обнаруживать подозрительные действия и инциденты безопасности. Вам нужно выбрать соответствующие инструменты и настроить их для автоматического оповещения о потенциальных угрозах.

4. Задача разработки плана реагирования на инциденты: Ваша компания нуждается в эффективном плане реагирования на компьютерные инциденты. Ваша задача - разработать план, который определит шаги, которые должны быть предприняты при обнаружении инцидента безопасности, включая уведомление, изоляцию и восстановление системы. Вам нужно учесть различные сценарии инцидентов и предложить соответствующие процедуры реагирования.

5. Задача аудита информационной безопасности: Ваша компания хочет провести аудит информационной безопасности своих систем и сетей. Ваша задача - разработать методологию аудита, определить области, которые следует проверить (например, аутентификация, авторизация, защита данных) и провести полный аудит с последующим представлением отчета о найденных уязвимостях и рекомендациях по их устранению.

6. Задача разработки политики паролей: Ваша компания столкнулась с частыми случаями несанкционированного доступа к системе из-за слабых паролей пользователей. Ваша задача - разработать строгую политику паролей, которая будет определять требования к паролям (например, длина, сложность) и обязательное их изменение с определенной периодичностью.

7. Задача обучения сотрудников о компьютерной безопасности: Ваша компания хочет провести обучающую программу по компьютерной безопасности для всех сотрудников. Ваша задача - разработать образовательную программу, которая будет покрывать основные аспекты компьютерной безопасности, такие как управление паролями, обнаружение фишинговых атак, защита от вредоносного программного обеспечения и т. д.

8. Задача разработки политики управления доступом: Ваша компания хочет улучшить контроль над доступом к информационным ресурсам. Ваша задача - разработать политику управления доступом, определить роли и привилегии пользователей, определить процедуры запроса доступа и разработать систему контроля доступа для обеспечения безопасности информационных ресурсов.

9. Задача разработки плана реагирования на инциденты: Ваша компания хочет быть готовой к возможным инцидентам информационной безопасности, таким как взлом или утечка данных. Ваша задача - разработать план реагирования на инциденты, который определит шаги, которые должны быть предприняты в случае инцидента, включая оповещение, изоляцию системы, восстановление и анализ инцидента.

10. Задача разработки политики паролей: Вам предоставлена компания, которая хочет улучшить безопасность своих учетных записей. Ваша задача - разработать политику паролей, определяющую требования к созданию и использованию паролей сотрудниками. Обоснуйте выбранные критерии и определите периодичность смены паролей.

Критерии оценки:

7-12 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.

2-6 баллов (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. Что называется систематизацией информации:
   а) обработка документа с целью получения новых данных
   б) разделение информации по определенному признаку
   в) кодирование данных
2. Выберите изменение формы представления информации:
   а) собака — dog
   б) домашний питомец — попугай
   в) собака — домашний питомец
3. Связанная с получением нового содержания, новой информации обработка:
   а) запись воспоминаний
   б) набор текста в текстовом редакторе и форматирование
   в) решение математической или логической задачи
4. Необходимо преобразовать текстовую информацию в математическую запись и найти ответ на вопрос задачи:
   «У одного мужика 23 овцы, а у другого на 7 больше. Сколько у них овец вместе? »
   а) 23 + (23 + 7) = 53
   б) 23 — (23 + 7) = 53
   в) 23 + (23 — 7) = 53
5. «Символ — … — строка — фрагмент текста», что в этом ряду пропущено:
   а) абзац
   б) слово
   в) предложение
6. Необходимо указать основную позицию пальцев на клавиатуре:
   а) ФЫВА — ОЛДЖ
   б) ОЛДЖ — ФЫВА
   в) АБВГ — ДЕЁЖ
7. Где указывается информация о местоположении курсора:
   а) в окне текстового редактора
   б) в строке состояния текстового редактора
   в) на панели задач
8. Сергей набирал на компьютере текст. Вдруг все буквы, вводимые им, стали прописными, что случилось:
   а) случайно нажал клавишу Caps Lock

б) случайно нажал клавишу Num Lock
в) сломался компьютер

9. Выберите предложение, где все пробелы стоят правильно:
а) «Пора, что железо:куй, поколе кипит!»
б) «Пора, что железо : куй , поколе кипит!»
в) «Пора, что железо: куй, поколе кипит!»
10. Нина набирает очень длинное предложение, курсор «подошёл» к концу строки, а ей ещё нужно написать пару слов. Что она должна сделать, чтобы продолжить ввод предложения на следующей строке:
а) перевести курсор в начало следующей строки с помощью мыши
б) продолжать набор текста, не обращая внимания на конец строки, на новую строку курсор перейдёт автоматически
в) перевести курсор в начало следующей строки
11. Если курсор находится внутри абзаца, что произойдет если нажать клавишу Enter:
а) абзац разобьётся на два отдельных абзаца
б) курсор переместится в конец текущей строки
в) курсор останется на прежнем месте
12. Что представляет из себя редактирование текста:
а) процесс передачи текстовой информации по компьютерной сети
б) процесс внесения изменений в имеющийся текст
в) процедуру считывания с внешнего запоминающего устройства ранее созданного текста
13. Положение курсора в слове с ошибкой отмечено чёрточкой: МО|АНИТОР. Какую клавишу нужно нажать, для исправления ошибки:
а) Backspace
б) Delete и Backspace
в) Delete
14. Положение курсора в слове с ошибкой отмечено чёрточкой: ДИАГРАММ|МА. Какую клавишу нужно нажать, для исправления ошибки:
а) Delete или Backspace
б) только Delete
в) только Backspace
15. Для чего служит клавиша Insert при работе с текстом:
а) удаления символа слева от курсора
б) переключения раскладки клавиатуры русская/латинская
в) переключения режима вставка/замена
16. Что нужно нажать, чтобы переместить курсор в начало текста:
а) Caps Lock
б) Ctrl + Home
в) Esc
17. Что называется фрагментом текста:
а) предложение

б) абзац
в) непрерывная часть текста

18. Что в первую очередь предусматривает копирование текстового фрагмента в текстовом редакторе:
а) выделение копируемого фрагмента
б) открытие нового текстового окна
в) выбор соответствующего пункта меню

19. Сколько раз фрагмент можно вставить в текст, если он был помещён в буфер обмена:
а) это зависит от количества строк в данном фрагменте
б) один
в) столько раз, сколько требуется

20. Что называется буфером обмена:
а) раздел жёсткого магнитного диска
б) раздел оперативной памяти
в) часть устройства ввода

21. Буфер обмена предназначается для:
а) временного хранения копий фрагментов или удалённых фрагментов
б) передачи текста на печать
в) исправления ошибок при вводе команд

22. «Далеко за отмелью, в ельнике, раздалась птичья трель.» Сколько слов будет найдено в процессе автоматического поиска в этом предложении, если в качестве образца задать слово «ель»:
а) 2
б) 3
в) 1

23. Что необходимо указать для того, чтобы считать текстовый файл с диска:
а) имя файла
б) размеры файла
в) дату создания файла

24. В каком — то текстовом процессоре можно использовать только один шрифт и два варианта начертания — полужирное начертание и курсив. Сколько различных начертаний символов можно получить:
а) 3
б) 2
в) 4

25. Необходимо выбрать лишнее:
а) вставка
б) выравнивание
в) изменение цвета
г) изменение начертания

26. Если считать, что символ кодируется одним байтом, определите, чему равен информационный объём представленного высказывания:

«Тысячи путей ведут к заблуждению, к истине — только один.»
а) 280 битов
б) 456 битов
в) 518 битов

27. Как называется этап подготовки текстового документа, на котором он заносится во внешнюю память:
а) форматированием
б) вводом
в) сохранением

28. В виде чего хранится на внешнем запоминающем устройстве текст, который был набран в текстовом редакторе:
а) файла
б) папки
в) каталога

29. В состав персонального компьютера входит?
А) Сканер, принтер, монитор
Б) Видеокарта, системная шина, устройство бесперебойного питания
В) Монитор, системный блок, клавиатура, мышь
Г) Винчестер, мышь, монитор, клавиатура

30. Все файлы компьютера записываются на?
А) Винчестер
Б) Модулятор
В) Флоппи-диск
Г) Генератор

31. Как включить на клавиатуре все заглавные буквы?
А) Alt + Ctrl
Б) Caps Lock
В) Shift + Ctrl
Г) Shift + Ctrl + Alt

32. Как называется основное окно Windows, которое появляется на экране после полной загрузки операционной среды?
А) Окно загрузки
Б) Стол с ярлыками
В) Рабочий стол
Г) Изображение монитора

33. Какую последовательность действий надо выполнить для запуска калькулятора в Windows?

А) Стандартные → Калькулятор
Б) Пуск → Программы → Стандартные → Калькулятор
В) Пуск → Стандартные → Калькулятор

Г) Пуск → Калькулятор

34. Как называется программа файловый менеджер, входящая в состав операционной среды Windows?
А) Проводник
Б) Сопровождающий
В) Менеджер файлов
Г) Windows commander

35. Для создания новой папки в программе Windows commander надо нажать на клавиатуре кнопку?
А) F5
Б) F6
В) F7
Г) F8

36. Для удаления файла в программе Windows commander следует нажать на клавиатуре кнопку?
А) F5
Б) F6
В) F7
Г) F8

37. Для запуска любой программы надо на рабочем столе Windows нажать на?
А) Ссылку на программу
Б) Ярлык программы
В) Кнопку запуска программы
Г) Рабочий стол

38.Для того, чтобы найти файл в компьютере надо нажать?
А) Пуск → Найти → Файлы и папки
Б) Пуск → Файлы и папки
В) Найти → Файл
Г) Пуск → Файл → Найти

39.Для настройки параметров работы мыши надо нажать?
А) Настройка → панель управления → мышь
Б) Пуск → панель управления → мышь
В) Пуск → настройка → мышь
Г) Пуск → настройка → панель управления → мышь

40.Как установить время, через которое будет появляться заставка на рабочем столе Windows?
А) Свойства: экран → Заставка → Интервал
Б) Заставка → Период времени
В) Свойства: экран → Заставка → Время

Г) Свойства: Интервал

41.Какие функции выполняет пункт Документы Главного меню Windows?
А) Пункт Документы Главного меню выводит список открытых в данный момент документов и позволяет переключаться между ними
Б) Пункт Документы Главного меню отображает список документов, с которыми работали последние 15 дней. Щелчок по названию или значку документа запускает приложение, с помощью которого он был создан и открывает документ
В) Пункт Документы Главного меню отображает список всех созданных документов и позволяет открыть любой из них
Г) Пункт Документы Главного меню выводит список последних открывавшихся документов. Щелчок по названию или значку документа запускает приложение, с помощью которого он был создан и открывает документ

42. С какой целью производится выделение объектов?
А) С целью группировки и создания тематической группы
Б) С целью последующего изменения их внешнего вида (изменения размера, вида значка и др.
В) С целью их сортировки
Г) С тем, чтобы произвести с ними какие-либо действия (открыть, скопировать, переместить и др.)

43. Как вызвать на экран контекстное меню?
А) Щелкнуть левой кнопкой мыши на объекте и в открывшемся списке выбрать команду "Контекстное меню"
Б) Открыть команду меню "СЕРВИС" и в ней выбрать команду "Контекстное меню"
В) Щелкнуть на объекте правой кнопкой мыши
Г) Дважды щелкнуть левой кнопкой мыши на объекте

44. В какой программе можно создать текстовый документ (отчет по научной работе)?
А) Windows Word
Б) Microsoft Word
В) Microsoft Excel
Г) Microsoft Power Point

45.Сколько документов можно одновременно открыть в редакторе Word?
А) Только один
Б) Не более трех
В) Сколько необходимо
Г) Зависит от задач пользователя и ресурсов компьютера

46. Открыть или создать новый документ в редакторе Microsoft Word можно используя панель?
А) Стандартная
Б) Форматирование
В) Структура
Г) Элементы управления

47. Для включения или выключения панелей инструментов в Microsoft Word следует нажать?
А) Вид → панели инструментов
Б) Сервис → настройка → панели инструментов
В) Щелкнув правой копкой мыши по любой из панелей
Г) Подходят все пункты а, б и в

48. Как создать новый документ "Стандартный отчет" из шаблонов Microsoft Word?
А) Файл → создать → общие шаблоны → отчеты → стандартный отчет
Б) Общие шаблоны → отчеты → стандартный отчет
В) Файл → отчеты → стандартный отчет
Г) Файл → создать → стандартный отчет

49. Для настройки параметров страницы Word надо нажать последовательность?
А) Файл → параметры страницы
Б) Файл → свойства → параметры страницы
В) Параметры страницы → свойства
Г) Правка → параметры страницы

50. Какие вирусы активизируются в самом начале работы с операционной системой:
а) загрузочные вирусы
б) троянцы
в) черви

51. Stuxnet — это:
а) троянская программа
б) макровирус
в) промышленный вирус

52. Таргетированная атака — это:
а) атака на сетевое оборудование

б) атака на компьютерную систему крупного предприятия
в) атака на конкретный компьютер пользователя

53. Под информационной безопасностью понимается:
а) 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
б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
в) нет верного ответа

54. Защита информации:
а) небольшая программа для выполнения определенной задачи
б) комплекс мероприятий, направленных на обеспечение информационной безопасности
в) процесс разработки структуры базы данных в соответствии с требованиями пользователей

55. Информационная безопасность зависит от:
а) компьютеров, поддерживающей инфраструктуры
б) пользователей
в) информации

56. Конфиденциальностью называется:
а) защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
б) описание процедур
в) защита от несанкционированного доступа к информации

57. Для чего создаются информационные системы:
а) получения определенных информационных услуг
б) обработки информации
в) оба варианта верны

58. Кто является основным ответственным за определение уровня классификации информации:
а) руководитель среднего звена
б) владелец
в) высшее руководство

59. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:
а) хакеры
б) контрагенты
в) сотрудники

60. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству:
а) снизить уровень классификации этой информации
б) улучшить контроль за безопасностью этой информации
в) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

61. Что самое главное должно продумать руководство при классификации данных:
а) управление доступом, которое должно защищать данные
б) оценить уровень риска и отменить контрмеры
в) необходимый уровень доступности, целостности и конфиденциальности

62. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены:
а) владельцы данных
б) руководство
в) администраторы

Задания в открытой форме

1. К правовым методам относят…
2. Назовите виды информационной безопасности….
3. Назовите цели информационной безопасности….
4. К основным принципам обеспечения информационной безопасности относится…
5. Основными субъектами информационной безопасности являются:
6. К основным функциям системы безопасности можно отнести
7. Принципом информационной безопасности является принцип недопущения
8. Принципом политики информационной безопасности является принцип:
9. К основным типам средств воздействия на компьютерную сеть относится:
10. Когда получен спам по e-mail с приложенным файлом, следует:
11. ЭЦП – это:

12. Наиболее распространены угрозы информационной безопасности корпоративной системы:
13. Наиболее распространены средства воздействия на сеть офиса:
14. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
15. Угроза информационной системе (компьютерной сети) – это:
16. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
17. Окончательно, ответственность за защищенность данных в компьютерной сети несет:
18. Политика безопасности в системе (сети) – это комплекс:
19. Наиболее важным при реализации защитных мер политики безопасности является:
20. Что такое тактическое планирование?

Задания на установление соответствия

1. Установите взаимно однозначное соответствие

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

2. Установите взаимно однозначное соответствие функции памяти

1	Proximity	А	Чтение/Запись

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

3. Установите взаимно однозначное соответствие

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

4. Установите взаимно однозначное соответствие методы реализации систем одноразовых паролей

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

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

5. Установите взаимно однозначное соответствие

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

6. Установите взаимно однозначное соответствие

1	Замкнутая программная среда	А	Предназначен для обеспечения гарантии того, что к моменту завершения загрузки ОС все ключевые компоненты СЗИ загружены и функционируют.

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

7. Установите взаимно однозначное соответствие

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

			дисков реализована в некоторых утилитах компрессии, например Stacker или Microsoft DriveSpace

8. Установите взаимно однозначное соответствие

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

9. Установите взаимно однозначное соответствие

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

10. Установите взаимно однозначное соответствие

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

11. Установить соответствие между терминами и определениями

1	Объект защиты	А	информация, носители информации, технические

			средства и технология их обработки, а также средства защиты информации
2	Объект информатизации	Б	совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены
3	Защищаемые помещения (ЗП)	В	помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.)
4	Утечка информации по техническому каналу	Г	неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации

12. Установить соответствие классификации угроз

1	Состояние источника угрозы	А	в самой системе, что приводит к ошибкам в работе и сбоям при реализации ресурсов АС; в пределах видимости АС, например, применение подслушивающей аппаратуры, похищение информации в распечатанном виде или кража записей с носителей данных
2	Степень влияния	Б	активная угроза безопасности, которая вносит коррективы в структуру системы и ее сущность,

			например, использование вредоносных вирусов или троянов; пассивная угроза – та разновидность, которая просто ворует информацию способом копирования, иногда скрытая. Она не вносит своих изменений в информационную систему.
3	Возможность доступа сотрудников к системе программ или ресурсов		вредоносное влияние, то есть угроза информационным данным может реализоваться на шаге доступа к системе (несанкционированного); вред наносится после согласия доступа к ресурсам системы.
4	Способ доступа к основным ресурсам системы	Г	применение нестандартного канала пути к ресурсам, что включает в себя несанкционированное использование возможностей операционной системы; использование стандартного канала для открытия доступа к ресурсам, например, незаконное получение паролей и других параметров с дальнейшей маскировкой под зарегистрированного в системе пользователя.

13. Установить соответствие угроз безопасности информации в локальных размерах

1	Компьютерные вирусы	А	нарушающие информационную безопасность. Они оказывают воздействие на информационную систему одного компьютера или сети ПК после попадания в программу и самостоятельного размножения. Вирусы способны остановить действие системы, но в основном они действуют локально;
2	«Черви»	Б	модификация вирусных программ, приводящая информационную систему в состояние блокировки и

			перегрузки. ПО активируется и размножается самостоятельно, во время каждой загрузки компьютера. Происходит перегрузка каналов памяти и связи
3	«Троянские кони»	В	программы, которые внедряются на компьютер под видом полезного обеспечения. Но на самом деле они копируют персональные файлы, передают их злоумышленнику, разрушают полезную информацию

14. Установить соответствие между терминами и определениями

1	Автоматизированная система (АС)	А	система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функции
2	Контролируемая зона (КЗ)	Б	пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных, технических и иных материальных средств
3	Специальные исследования (СИ)	В	выявление с использованием контрольно-измерительной аппаратуры возможных каналов утечки защищаемой информации от основных и вспомогательных технических средств и систем
4	Специальная проверка (СП)	Г	проверка технических средств и систем объекта защиты с целью выявления возможно внедренных электронных устройств съема информации (закладочных устройств)

15. Установить соответствие между

1	Перехват паролей	А	мошенничество возможно с

			участием специальных программ, которые имитируют на экране монитора окошко для ввода имени и пароля. Введенные данные попадают в руки злоумышленника, и далее на дисплее появляется сообщение о неправильной работе системы.
2	«Маскарад»	Б	действия в информационной системе от лица другого человека в сети компании. Существуют такие возможности реализации планов злоумышленников в системе -передача ложных данных в системе от имени другого человека
3	Незаконное использование привилегий	В	название разновидности хищения информации и подрыва безопасности информационной системы говорит само за себя

16. Установить соответствие между излучениями каналов

1	Побочные электромагнитные излучения и наводки (ПЭМИН)	А	паразитные и побочные электромагнитные излучения радиоэлектронного оборудования и средств вычислительной техники. В зависимости от среды распространения различают
2	Побочные электромагнитные излучения (ПЭМИ)	Б	нежелательные (паразитные) электромагнитные излучения, возникающие при функционировании технических средств обработки информации, и приводящие к утечке обрабатываемой информации
3	Информативными ПЭМИ	В	сигналы, представляющие собой ВЧ несущую, модулированную информацией обрабатываемой на СВТ (например, изображением, выводимым на экран монитора, данными, обрабатываемыми на устройствах ввода-вывода и т.д.)

4	Неинформативными ПЭМИ	Г	сигналы, анализ которых может дать представление только о режиме работы СВТ и никак не раскрывает характер информации, обрабатываемой на СВТ

17. Установить соответствие между основными принципы защиты информации

1	Принцип законности	А	необходимо нормативно- правовое регулирование этой области общественных отношений. Законодательно должны быть обозначены права различных субъектов в области защиты информации
2	Принцип защиты информации	Б	основополагающие идеи, важнейшие рекомендации по организации и осуществлению этой деятельности на различных этапах решения задач сохранения секретов
3	Принцип приоритета	В	объектом засекречивания не могут быть сведения, которые государство обнародует или сообщает согласно конвенциям или соглашениям
4	Принцип собственности и экономической целесообразности	Г	право собственникам информации принимать меры к защите этой информации, а также оценивать ее потребительские свойства

18. Установить соответствие между терминами и определениями

1	Специальные обследования помещений	А	комплекс мер в области защиты информации в части проведения работ по выявлению электронных устройств, предназначенных для негласного получения сведений в помещениях, где циркулирует информация ограниченного пользования

2	Аттестация объекта защиты	Б	официальное подтверждение наличия на объекте защиты необходимых и достаточных условий, обеспечивающих выполнение установленных требований РД по ЗИ
3	Основные технические средства и системы	В	технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации
4	Нормирование показателей защищенности	Г	установление нормативными документами численных значений показателей защищенности информации

19. Установить соответствие между элементами и функциями

1	Дробление	А	знание какой-то одной части информации не позволяет восстановить всю технологию в целом
2	Кодирование	Б	метод защиты информации, преследующий цель скрыть от соперника содержание защищаемой информации и заключающийся в преобразовании с помощью кодов открытого текста в условный при передаче информации по каналам связи
3	Шифрование	В	метод защиты информации, используемый при передаче сообщений с помощью различной радиоаппаратуры, направлении письменных сообщений и в других случаях, когда есть опасность перехвата этих сообщений соперником

20. Установить соответствие между элементами и функциями

1	Случайные антенны	А	вспомогательные технические средства, их соединительные линии, а также линии

			электропитания, посторонние проводники и цепи заземления, при непосредственном подключении к которым средств разведки ПЭМИН возможен перехват информационных сигналов
2	Сосредоточенные	Б	телефонный аппарат, громкоговоритель радиотрансляционной сети, датчик пожарной сигнализации и т. д., подключенные к линии, выходящей за пределы КЗ
3	Распределенные	В	кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы КЗ

Задания на установление правильной последовательности

1. Установить этапы защиты от угроз безопасности:

1. Предоставление персоналу защищенный удаленный доступ к информационным ресурсам

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

3. Защита внешних каналов передачи информации

4. Разработка политики информационной безопасности

5. Анализ угрозы безопасности

2. Установить этапы стадии исполнения компьютерных вирусов:

1. Выполнение деструктивных функций

2. Передача управления программе-носителю вируса

3. Поиск жертвы

4. Заражение найденной жертвы

5. Загрузка вируса в память

3. Установить этапы построения системы антивирусной защиты сети:

1. Реализация плана антивирусной безопасности

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

3. Разработка политики антивирусной безопасности

4. Разработка плана обеспечения антивирусной безопасности

4. Установить этапы построения программы обеспечения безопасности:

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

2. Регулярный контроль пошаговой реализации плана безопасности

3. Установление уровня безопасности

4. Формирование политики безопасности организации

5. Определение ценности технологических и информационных активов организации

5. Установить действия этапа анализа рисков:

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

2. Оценка рисков технологических и информационных активов

3. Идентификация и оценка стоимости технологических и информационных активов

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

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

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

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

3. Совокупность событий должна сравниваться с заранее установленной пороговой величиной

4. Каждое нарушение безопасности должно генерировать системное событие

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

1. Дата, время

2. Протокол

3. Порт получателя

4. Номер агента

5. IP-адрес атакующего

6. Тип атаки

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

1. ISO 27001:2005

2. ISO/IEC 17799

3. ISO/IEC 15408

4. «Критерии оценки доверенных компьютерных систем»

9. Расположить этапы процесса управления рисками информационной безопасности:

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

10. Расположить этапы проведения аудита информационной безопасности:
1. Разработка рекомендаций по повышению уровня защиты автоматизированной системы
2. Анализ полученных данных
3. Сбор исходных данных
4. Разработка регламента проведения аудита

11. Расположить этапы процесса управления рисками информационной безопасности:
1. Классификация рисков, выбор методологии оценки рисков и проведение оценки
2. Анализ угроз и их последствий, определение слабостей в защите
3. Выбор, реализация и проверка защитных мер
4. Оценка остаточного риска
5. Идентификация активов и ценности ресурсов, нуждающихся в защите
6. Выбор анализируемых объектов и степени детальности их рассмотрения

12. Расположить этапы проведения аудита информационной безопасности:
1. Разработка рекомендаций по повышению уровня защиты автоматизированной системы
2. Анализ полученных данных
3. Сбор исходных данных
4. Разработка регламента проведения аудита

13. Расположите в правильном порядке объекты защиты

1. __класс. Ценность данных определяется их собственником (коммерческая тайна)
2. __класс. Данные имеют ограниченный доступ на основании федеральных законов (персональные данные, банковская тайна)
3. __класс — государственная тайна.

Информационные объекты, имеющие ценность, присутствуют в жизни организации в виде

14. Расположить этапы процесса комплекса превентивных мер

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

15. Восстановите алгоритм испытаний

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

16. Расположите этапы применения фреймворка управления рисками (NIST SP 800-37)
1. оценка внедренных мер защиты для определения корректности их применения, работоспособности и продуцирования ими результатов, удовлетворяющих требованиям безопасности и конфиденциальности
2. подготовка, т.е. определение целей и их приоритизация с точки зрения организации и ИТ-систем
3. внедрение мер защиты и описание того, как именно применяются меры защиты
4. категоризация систем и информации на основе анализа возможного негативного влияния от потери информации
5. выбор базового набора мер защиты и их уточнение (адаптация) для снижения риска до приемлемого уровня на основе оценки риска
6. непрерывный мониторинг систем и примененных мер защиты для оценки эффективности примененных мер, документирования изменений, проведения

оценки рисков и анализа негативного влияния, создания отчетности по состоянию безопасности и конфиденциальности.
7. формальное согласование/утверждение использования систем или мер защиты на основе заключения о приемлемости рисков

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

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

18. Выберите правильную последовательность этапов по созданию системы защиты персональных данных:

1. Опытная и промышленная эксплуатация
2. Проектный этап
3. Аттестация или декларирование
4. Предпроектный этап

19. 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.

20.Последовательность слов для понятия Компьютерная сеть – это

1. Обеспечивающего передачу
2. Устройства связи
3. Связанных с помощью
4. Данных между ними
5. Группа компьютеров

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. Объясните принципы конфиденциальности, целостности и доступности информации в контексте компьютерной безопасности. Приведите примеры ситуаций, когда каждый из этих принципов может быть нарушен, и опишите возможные последствия.

2. Исследуйте различные виды атак на информационные системы, такие как атаки на основе уязвимостей, социальная инженерия, фишинг и др. Опишите каждый вид атаки, объясните, как они работают и какие меры предосторожности можно принять для защиты от них.

3. Рассмотрите модели угроз и рисков в компьютерной безопасности, такие как модель STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege). Поясните каждый аспект модели и приведите примеры ситуаций, когда каждый из них может быть применен.

4. Исследуйте различные методы шифрования и их применение в компьютерной безопасности. Объясните основные принципы симметричного и асимметричного шифрования, а также использование хэш-функций. Приведите примеры практического применения каждого метода.

5. Изучите понятие аутентификации и методы проверки подлинности в компьютерной безопасности. Объясните различные факторы аутентификации, такие как пароль, биометрические данные, аппаратные токены и др. Рассмотрите преимущества и ограничения каждого метода.

6. Обсудите понятие политики безопасности и ее роль в компьютерной безопасности. Опишите основные компоненты политики безопасности, такие

как правила доступа, аудит и мониторинг, обучение пользователей и др. Приведите примеры эффективных политик безопасности.

7. Задача о криптографических алгоритмах: Рассмотрите различные криптографические алгоритмы, такие как шифр Цезаря, асимметричное шифрование RSA или симметричное шифрование AES. Опишите их основные принципы работы и применение. Задача состоит в том, чтобы выбрать наиболее подходящий криптографический алгоритм для защиты конкретной информации и объяснить причины выбора.

8. Задача о безопасности сетей: Рассмотрите основные аспекты безопасности сетей, включая сетевые протоколы, аутентификацию и авторизацию, защиту от атак типа DDoS и многое другое. Представьте себя в роли сетевого администратора и определите меры, которые следует принять для обеспечения безопасности компьютерной сети. Объясните, какие технологии и методы могут быть использованы для защиты сети от угроз.

9. Задача о уязвимостях веб-приложений: Изучите типичные уязвимости веб-приложений, такие как инъекции SQL, уязвимости XSS и CSRF, утечки информации и др. Возьмите в рассмотрение конкретное веб-приложение и определите его уязвимости. Задача состоит в том, чтобы предложить рекомендации по устранению этих уязвимостей и улучшению общей безопасности веб-приложения.

10. Задача о социальной инженерии: Исследуйте методы социальной инженерии, используемые злоумышленниками для получения несанкционированного доступа к системам. Рассмотрите примеры фишинговых атак, атак через социальные сети и другие формы манипуляции людьми. Задача заключается в том, чтобы разработать программу обучения для сотрудников, чтобы они могли распознавать и предотвращать атаки со стороны социальных инженеров.

11. Задача идентификации уязвимостей: Изучите различные типы уязвимостей в компьютерных системах, такие как буферное переполнение, инъекции SQL и кросс-сайтовый скриптинг. Ваша задача - проанализировать код программы и идентифицировать возможные уязвимости, а затем предложить соответствующие меры для их устранения.

12. Задача построения безопасной сетевой инфраструктуры: Вам предоставлено предприятие, которое хочет построить безопасную сетевую инфраструктуру. Ваша задача - разработать план сети, определить необходимые сетевые устройства (маршрутизаторы, брандмауэры и т. д.) и настроить правила безопасности для защиты сети от внешних угроз.

13. Задача анализа безопасности данных: Вам предоставлен набор данных, содержащий персональную информацию пользователей. Ваша задача - провести анализ данных и выявить потенциальные угрозы безопасности, такие как утечка конфиденциальных данных или нарушение

приватности. Затем предложите меры по обеспечению безопасности данных и защите личной информации.

14. Задача разработки политики безопасности: Вам предоставлена компания, которая хочет разработать политику безопасности для своих сотрудников. Ваша задача - определить ключевые аспекты безопасности, такие как пароли, доступ к информации, использование сети и т. д., и разработать подходящую политику безопасности, которая будет учитывать специфические потребности компании.

15. Задача анализа угроз и рисков: Вам предоставлен список потенциальных угроз и рисков в компьютерной системе. Ваша задача - оценить каждую угрозу по их вероятности и влиянию на систему, а затем определить необходимые меры по предотвращению и снижению рисков.

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.