МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности

(наименование ф-та полностью)

М.О. Таныгин

(подпись, инициалы, фамилия)

« *29* » *августа* 2022 г.

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

Информационная безопасность

(наименование дисциплины)

38.05.01 Экономическая безопасность, направленность (специализация)
«Экономико-правовое обеспечение экономической безопасности»

(код и наименование ОПОП ВО)

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

Тема 1. Основные понятия и анализ угроз информационной безопасности.

1. Становление индустрии информации.
2. Назовите основные элементы системы защиты информации.
3. Экономика защиты информации как наука, задачи экономики защиты информации.
4. Назовите экономические проблемы защиты информации.
5. Организация как объект защиты информации.
6. Информация как товар.
7. Рынок информации.

Тема 2. Проблемы информационной безопасности сетей.

1. Производственные ресурсы предприятия и служб защиты информации.
2. Информационные технологии.
3. Финансовые ресурсы организации.
4. Результаты деятельности фирмы. Бизнес-план.
5. Инновационная деятельность организации.
6. Классификация инноваций.
7. Инфраструктура инновационной деятельности.
8. Инновационный проект.
9. Эффективность инноваций.

Тема 3. Политика безопасности.

1. Назовите основные понятия политики безопасности.
2. Верхний, средний и нижний уровни политики безопасности.
3. Структура политики безопасности организации.
4. Базовая политика безопасности.
5. Специализированные политики безопасности.
6. Процедуры безопасности.
7. Основные этапы разработки политики безопасности организации.
8. Опишите компоненты архитектуры безопасности сети: физическая безопасность, логическая безопасность, защита ресурсов, определение административных полномочий, аудит и оповещение.

Тема 4. Криптографическая защита информации

1. Назовите основные понятия криптографической защиты информации.
2. Требования к криптографическим системам.
3. Симметричные и ассиметричные криптосистемы шифрования.
4. Блочные и потоковые шифры.
5. Шифры простой замены.

6. Шифры Виженера.
7. Стандарт шифрования AES.
8. Алгоритм шифрования RSA.
9. Функция хэширования.
10. Электронная цифровая подпись (ЭЦП).
11. Защита электронного документооборота с использованием ЭЦП.
12. Обзор программных и программно-аппаратных средств криптографической защиты.

Тема 5. Технологии аутентификации

1. Аутентификация, авторизация и администрирование действий пользователей.
2. Аутентификация на основе многоразовых паролей.
3. Аутентификация на основе одноразовых паролей.
4. Аутентификация на основе PIN-кода.
5. Строгая аутентификация, основанная на симметричных алгоритмах.
6. Биометрическая аутентификация пользователя.
7. Аппаратно-программные системы идентификации и аутентификации.

Тема 6. Технологии межсетевых экранов

1. Классификация межсетевых экранов.
2. Функции межсетевых экранов: фильтрация трафика, выполнение функций посредничества.
3. Дополнительные возможности межсетевых экранов: идентификация и аутентификация пользователей, трансляция сетевых адресов, регистрация и анализ событий.
4. Варианты исполнения межсетевых экранов.
5. Особенности функционирования межсетевых экранов на различных уровнях модели OSI.

Тема 7. Технологии защиты от вирусов

1. Классификация компьютерных вирусов.
2. Загрузочные вирусы.
3. Файловые вирусы.
4. Вирусы-сценарии.
5. Макровирусы.
6. Троянские программы.
7. Черви.
8. Жизненный цикл вирусов.
9. Основные каналы распространения вредоносных программ.
10. Методы обнаружения компьютерных вирусов

Тема 8. Требования к системам защиты информации

1. Показатели защищенности средств вычислительной техники от несанкционированного доступа.
2. Классы защищенности автоматизированных систем.
3. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных.

4. Требования к защите информации в автоматизированных системах, локальных вычислительных сетях, на рабочих местах пользователей ПК.

Тема 9. Основы правового обеспечения защиты информации

1. Правовое обеспечение информационной собственности и его место в системе информационного права.
2. Информация как объект юридической защиты.
3. Формирование государственной системы правового обеспечения информационной безопасности.
4. Правовое обеспечение защиты государственной тайны.
5. Законодательство Российской Федерации в области информационной безопасности.

Критерии оценки:

3-4 балла (или оценка «отлично») выставляется обучающемуся, если ондемонстрирует глубокое знание содержания вопроса; дает точные определения основныхпонятий; аргументированно и логически стройно излагает учебный материал; иллюстрируетсвой ответ актуальными примерами (типовыми и нестандартными), в том числесамостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросахпреподавателя.

2 балла (или оценка «хорошо») выставляется обучающемуся, если он владеетсодержанием вопроса, но допускает некоторые недочеты при ответе; допускаетнезначительные неточности при определении основных понятий; недостаточноаргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свойответ типовыми примерами.

1 балл (или оценка «удовлетворительно») выставляется обучающемуся, если оносвоил основные положения контролируемой темы, но недостаточно четко дает определениеосновных 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 онне владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основныеопределения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе наних грубые ошибки.

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ПРАКТИЧЕСКИХ РАБОТ

Контрольные вопросы для защиты практической работы №1:

1. Какова роль информации в проведении конкурентной борьбы?

2. Почему информация также является товаром?
3. Какими основными свойствами обладает информация как товар?

Контрольные вопросы для защиты практической работы №2:
1. Как выбрать базы для наблюдения?
2. Откуда брать необходимую для работы предприятия информацию?
3. Как классифицировать информацию, поступающую из внешней среды в организацию?

Контрольные вопросы для защиты практической работы №3:
1. Что такое коммерческая тайна организации (фирмы)?
2. Кто определяет состав и объем сведений, составляющих КТ?
3. Перечень сведений, которые не могут составлять КТ.
4. Какие сведения могут быть отнесены к КТ?

Контрольные вопросы для защиты практической работы №4:
1. Какая информация используется для стратегического планирования?
2. Что такое бизнес-план? Основные разделы бизнес-плана.
3. Зачем проводится технико-экономическое обоснование проекта и для кого предназначен этот документ?
4. Откуда исходит угроза риска при реализации проекта?

Контрольные вопросы для защиты практической работы №5:
1. Каков порядок проведения секретных переговоров и совещаний?
2. Чем достигается соответствие помещений требованиям стандартов по безопасности информации?
3. Какие действия необходимо предпринять при выборе коммерческой организации - делового партнера?
4. Как осуществляется проверка достоверности информации о партнере?
5. Назовите виды рисков в предпринимательской деятельности.

Контрольные вопросы для защиты практической работы №6:
1. Какие существуют виды угроз информационным ресурсам?
2. С какой целью проводится психологический профотбор?
3. Что включает в себя профессиограмма?
4. Какие структуры используются для сбора сведений о кандидатах?

Контрольные вопросы для защиты практической работы №7:
1. Какие методы используются для сбора сведений о кандидатах?
2. Назовите тестовые приемы и другие научные методики проверки кандидатов.
3. Особенности проведения итоговой беседы с кандидатами.
4. Какие меры целесообразно предпринять до беседы с увольняемым сотрудником?

Контрольные вопросы для защиты практической работы №8:
1. Какие формы может принимать беседа с увольняемым сотрудником, и каким образом должен быть построен разговор?
2. Какие существуют варианты сохранения в тайне коммерческих сведений при увольнении сотрудников?
3. Как рекомендуется действовать в тех случаях, когда увольнения сотрудников происходят по инициативе самих коммерческих структур?

Контрольные вопросы для защиты практической работы №9:
1. Как оценить уровень затрат предприятия на проведение мер предосторожности?
2. Первоочередные действия службы безопасности при возникновении ЧС.
3. Какая информация для правоохранительных органов готовится службой безопасности после нападения на организацию?

Критерии оценки:

6-8 баллов (или оценка «отлично») выставляется обучающемуся, если ондемонстрирует глубокое знание содержания вопроса; дает точные определения основныхпонятий; аргументированно и логически стройно излагает учебный материал; иллюстрируетсвой ответ актуальными примерами (типовыми и нестандартными), в том числесамостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросахпреподавателя.

4-5 балла (или оценка «хорошо») выставляется обучающемуся, если он владеетсодержанием вопроса, но допускает некоторые недочеты при ответе; допускаетнезначительные неточности при определении основных понятий; недостаточноаргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свойответ типовыми примерами.

1-3 балла (или оценка «удовлетворительно») выставляется обучающемуся, если оносвоил основные положения контролируемой темы, но недостаточно четко дает определениеосновных 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 онне владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основныеопределения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе наних грубые ошибки.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1. Важнейшие виды экономической безопасности:
А) Финансовая, энергетическая, информационная, обороннопромышленная, продовольственная;
Б) Финансовая, энергетическая, военная (оборонная), инновационно-промышленная, продовольственная;
В) Финансовая, энергетическая, военная (оборонная), оборонно-промышленная, продовольственная.

2. В структуре национальной безопасности экономическая безопасность занимает особое место. Это обусловлено тем, что:
А) Все виды безопасности зависят от состояния сельского хозяйства;
Б) Ни один вид безопасности не может быть реализован без экономического обеспечения;
В) Все виды безопасности зависят от банковской сферы.

3. Анализ информационных рисков предназначен для:
а) оценки существующего уровня защищенности информационной системы и формирования оптимального бюджета на информационную безопасность;
б) оценки технического уровня защищенности информационной системы
в) получения стоимостной оценки вероятного финансового ущерба от реализации угроз, направленных на информационную систему компании и для оценки возможности реализации угроз;
г) убеждения руководства компании в необходимости вложений в систему обеспечения информационной безопасности и для инструментальной проверки защищенности информационной системы

4. Политика информационной безопасности, прежде всего, необходима для:
а) успешного прохождения компанией регулярного аудита по ИБ;
б) обеспечения реального уровня защищенности информационной системы компании;
в) понимания персоналом важности требований по ИБ;
г) обеспечения адекватной защиты наиболее важных ресурсов компании

5. Политика информационной безопасности в общем случае является
а) руководящим документом для администраторов безопасности и системных администраторов
б) руководящим документом для ограниченного использования руководящим документом для руководства компании, менеджеров, администраторов безопасности и системных администраторов
в) руководящим документом для всех сотрудников компании

6. Предположим, информационная система компании надежно защищена комплексом средств информационной защиты (межсетевые экраны, антивирусы, системы защиты от НСД, системы обнаружения атак и т.д.). Выберите, как на существующий уровень рисков влияет реализация требований политики безопасности:
а) информационная система сама по себе надежно защищена комплексом средств защиты, поэтому реализация требований политики безопасности не оказывает существенного влияния на уровень рисков;

б) политика безопасности, как документ для непосредственного использования, отсутствует, что не оказывает существенного влияния на уровень рисков из-за высокого <технологического> уровня защищенности информационной системы;
в) политика безопасности является формальным, не используемым на практике документом, и это не оказывает серьезного влияния на существующий уровень рисков реализация требований политики безопасности
г) существенно влияет на уровень рисков, так как <технологический> фактор защищенности информационной системы является лишь необходимым, но не достаточным условием обеспечения безопасности

7. Выберите, невыполнение, какого из следующих требований политики безопасности, на Ваш взгляд, может наибольшим образом повысить существующие в системе информационные риски:
а) регулярное обновление антивирусных баз создание и поддержание форума по информационной безопасности для всех специалистов, вовлеченных в процесс обеспечения ИБ
б) классификация ресурсов по степени важности с точки зрения ИБ завершение активной сессии пользователя по окончании работы

8. Международный стандарт управления информационной безопасностью ISO 17799 предъявляет:
а) требования, предъявляемые только для узкого круга крупнейших мировых компаний
б) базовые требования по обеспечению ИБ повышенные требования по обеспечению безопасности информационной системы
в) требования, которые не соответствуют законам стран СНГ в области информационной безопасности

9. Одной из рекомендаций ISO 17799 является :
а) четкая регламентация настроек межсетевых экранов
б) применение антивирусных продуктов ведущих производителей
в) проведение анализа рисков и регулярных тестов на проникновение сторонней компанией
г) необходимость прохождения руководством компании регулярных тренингов по ИБ

10. Для проведения анализа информационных рисков, прежде всего, необходимо:
а) градация информационных рисков
б) построение полной модели информационной системы с точки зрения информационной безопасности
в) модель нарушителя вероятностные оценки угроз безопасности

11. Основной задачей теста на проникновение, прежде всего, является:
а) оценка возможности обнаружения атаки службой ИБ компании

б) проверка времени реакции службы обеспечения информационной безопасности
в) оценка возможности осуществления атаки из Интернет на информационную систему компании
г) оценка возможных потерь при реализации атаки из Интернет

12. Тест на проникновение позволяет (выберите наиболее полное и точное определение)
а) убедить руководство компании в реальной опасности вторжения из Интернет и обосновать необходимость инвестиций в ИБ
б) снизить вероятные риски вирусной атаки на корпоративную сеть
в) обеспечить должный уровень отношения руководства компании к проблеме

обеспечения ИБ
г) убедиться в способности службы ИБ противостоять возможным атакам злоумышленников из Интернет

13. Укажите в общем случае возможные типовые пути воздействия при получении удаленного доступа пользователя к информации на сервере
а) атака на канал передачи, атака на сервер, атака на пользовательскую группу
б) вирусная атака на корпоративную сеть атака на станцию пользователя, атака на канал передачи
в) атака на сервер, проникновение злоумышленника в сеть компании из Интернет

14. Какой метод обычно используется профессиональными взломщиками при информационной атаке?
а) атака на наиболее защищенную цель
б) атака на промежуточную цель
в) атака на наименее защищенную цель
г) атака осуществляется без целенаправленного выбора цели

15. Выберите наиболее оптимальную стратегию управления рисками в следующем случае: Веб-сервер компании находится внутри корпоративной сети и его программное обеспечение, возможно, содержит уязвимости
а) уменьшение риска и уклонение от риска
б) принятие риска
в) изменение характера риска и уклонение от риска
г) изменение характера риска и уменьшение риска

16. Для оценки ущерба по угрозе <целостность> необходимо:
а) оценить полную стоимость информации оценить какой ущерб понесет компания в случае изменения информации
б) оценить какой ущерб понесет компания в случае осуществления несанкционированного доступа к информации
в) оценить возможность осуществления атаки на ресурс, на котором хранится информация

17. Выберите наиболее полное описание методов, которые применяются при оценке ущерба в случае нарушения конфиденциальности информации
а) оценка стоимости затрат на реабилитацию подмоченной репутации, престижа, имени компании стоимость упущенной выгоды (потерянный контракт) стоимость затрат на поиск новых клиентов, взамен более не доверяющих компании

б) оценка стоимости контрмер по уменьшению ущерба от нарушения конфиденциальности информации;
в) оценка прямого ущерба от нарушения конфиденциальности информации

18. В случае анализа рисков базового уровня необходимо:
а) провести тесты на проникновение проверить выполнение требований соответствующего стандарта, например ISO 17799
б) провести полный аудит информационной безопасности, включая тесты на проникновение построить полную модель информационной системы с точки зрения информационной безопасности

20. Восстановите алгоритм оценки рисков информационной безопасности:
а) идентификация активов;

б) разработка модели угроз;
в) определение допустимого уровня риска;
г) определение риска несоответствия требований законодательства;
д) процедура количественного определения рисков;

21. Восстановите алгоритм количественного оценивая риска ИБ:
а) определение ценности актива
б) выбор актуальных угроз ИБ частной модели угроз
в) вычисления значения риска
г) определение ценности актива
д) определение возможности использования организационных и технических уязвимостей

22. Выделите основные элементы системы
- рабочие места, на которых операторы вводят информацию, поступающую из внешнего мира;
- почтовый сервер, на который информация поступает с удаленных узлов сети через Интернет;
- сервер обработки, на котором установлена СУБД;
- сервер резервного копирования;
- рабочие места группы оперативного реагирования;
- рабочее место администратора безопасности;
- рабочее место администратора БД.

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

24. Какой из перечисленных методов оценки риска дает представление о наиболее критических факторах инвестиционного проекта?
- Построение дерева решений
- Метод сценариев
- Учет рисков при расчете чистой приведенной стоимости
- Анализ чувствительности

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

26. Каким образом при расчете чистой приведенной стоимости можно учитывать риск?
- В знаменателе формулы NPV посредством корректировки ставки дисконта
- Комбинация формул NPV посредством корректировки чистых денежных потоков
- В числителе формулы NPV посредством корректировки чистых денежных поток
- все варианты верны

27. Какой из перечисленных методов оценки риска используется в ситуациях, когда принимаемые решения сильно зависят от принятых ранее и определяют сценарии дальнейшего развития событий?

- Имитационное моделирование
- Вероятностный метод
- Учет рисков при расчете чистой приведенной стоимости
- Анализ чувствительности
- Построение дерева решений

28. Следующее структурное подразделение службы защиты информации отвечает за контакты с правоохранительными органами по всем вопросам обеспечения безопасности деятельности объекта
- Группарежима
- Группа охраны исопровождения
- Техническаягруппа
- Детективная группа

29. В обязанности какого сотрудника входит разработка и поддержка эффективных мер защиты по обработке информации для обеспечения сохранное данных
- Сотрудник группы безопасности
- Администратор безопасности системы
- Администратор безопасности данных
- Руководитель группы

30. В обязанности какого сотрудника входит контроль за выполнением плана восстановления после инцидента информационной безопасности
- Сотрудник группы безопасности
- Администратор безопасности системы
- Администратор безопасности данных
- Руководитель группы

31. В обязанности какого сотрудника входит реализация и изменение средств защиты данных
- Сотрудник группы безопасности
- Администратор безопасности системы
- Администратор безопасности данных
- Руководитель группы

32. В обязанности какого сотрудника входит контроль состояния защиты наборов данных
- Сотрудник группы безопасности
- Администратор безопасности системы
- Администратор безопасности данных
- Руководитель группы

33. В обязанности какого сотрудника входит опубликование нововведений в области защиты
- Сотрудник группы безопасности
- Администратор безопасности системы
- Администратор безопасности данных
- Руководитель группы

34. В обязанности какого сотрудника входит хранение резервных копий данных
- Сотрудник группы безопасности
- Администратор безопасности системы
- Администратор безопасности данных
- Руководитель группы

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

- Сотрудник группы безопасности
- Администратор безопасности системы
- Администратор безопасности данных
- Руководитель группы

36. В обязанности какого сотрудника входит контроль защиты наборов данных и программ
- Сотрудник группы безопасности
- Администратор безопасности системы
- Администратор безопасности данных
- Руководитель группы

37. В обязанности какого сотрудника входит организация общей поддержки групп управления защитой и менеджмента в своей зоне ответственности
- Сотрудник группы безопасности
- Администратор безопасности системы
- Администратор безопасности данных
- Руководитель группы

38. Количественный состав службы безопасности зависит, прежде всего от
- Типа циркулирующей в ней конфиденциальной информации
- От возможностей фирмы
- Нормативных документов регуляторов
- Численности штата

39. 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
- Директор
- Начальник службы защита информации
- Сотрудник сектора охраны и режима
- Аналитик
- Сотрудник сектора технической защиты

40. Кто вырабатывает политику обеспечения защиты информации и обеспечивает ее реализацию?
- Директор
- Начальник службы защита информации
- Аналитик
- Руководитель группы
- Юрист
- Администратор безопасности системы

41. Кто руководит проведением служебных расследований?
- Директор
- Начальник службы защиты информации
- Аналитик
- Руководитель группы
- Юрист
- Администратор безопасности системы

42. Кто несёт персональную ответственность за выполнение службой защиты информации своих функций?
- Начальник службы защиты информации
- Сотрудник сектора обеспечения безопасности
- Аналитик

- Руководитель группы
- Юрист

43. Кто разрабатывает руководящие документы и инструкции по вопросам безопасности?

- Директор
- Начальник службы защиты информации
- Сотрудник группы безопасности
- Аналитик
- Юрист

44. Кто обеспечивает режим допуска и доступа?

- Начальник службы защита информации
- Сотрудник сектора охраны и режима
- Сотрудник сектора обеспечения безопасности
- Сотрудник группы безопасности
- Руководитель группы

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

- Группарежима
- Группа охраны исопровождения
- Техническаягруппа
- Детективнаягруппа

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

- Группарежима
- Группа охраны исопровождения
- Техническаягруппа
- Детективнаягруппа

47. Следующее структурное подразделение службы защиты информации отвечает за наблюдение за обстановкой вокруг объекта и на его территории

- Группарежима
- Группа охраны исопровождения
- Техническаягруппа
- Детективнаягруппа

48. Следующее структурное подразделение службы защиты информации отвечает за контроль работоспособности элементов системы защиты и их проверке

- Группарежима
- Группа охраны исопровождения
- Техническаягруппа
- Детективнаягруппа

49. Следующее структурное подразделение службы защиты информации отвечает за обеспечении безопасности деятельности объекта с помощью систем сигнализации, наблюдения, связи

- Группарежима
- Техническаягруппа
- Детективнаягруппа

50. Следующее структурное подразделение службы защиты информации отвечает за планирование и проведение мероприятий по специальной защите объекта

- Группарежима
- Группа охраны исопровождения
- Техническаягруппа

- Детективнаягруппа

51. Следующее структурное подразделение службы защиты информации отвечает за приобретение и установку различных технических средств для службы безопасности
- Группарежима
- Группа охраны исопровождения
- Техническаягруппа
- Детективнаягруппа

52. Следующее структурное подразделение службы защиты информации отвечает за техническое обеспечение мероприятий детективной группы
- Группарежима
- Группа охраны исопровождения
- Техническаягруппа

53. Следующее структурное подразделение службы защиты информации отвечает за проверку кандидатов для приема на работу на объекте
- Группарежима
- Группа охраны исопровождения
- Техническаягруппа
- Детективная группа

54. Следующее структурное подразделение службы защиты информации отвечает за проведение специальных мероприятий в отношении фирм-конкурентов
- Группарежима
- Группа охраны исопровождения
- Техническаягруппа
- Детективная группа

55. Следующее структурное подразделение службы защиты информации отвечает за контакты с правоохранительными органами по всем вопросам обеспечения безопасности деятельности объекта
- Группарежима
- Группа охраны исопровождения
- Техническаягруппа

56. Что представляет собой стандарт ISO/IEC 27799?
- Стандарт по защите персональных данных о здоровье
- Новая версия BS 17799C.
- Определения для новой серии ISO 27000
- Новая версия NIST 800-60

57. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?
- Список стандартов, процедур и политик для разработки программы безопасности
- Текущая версия ISO 17799
- Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
- Открытый стандарт, определяющий цели контроля

55. Из каких четырех доменов состоит CobiT?
- Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
- Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
- Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
- Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

58. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?

- COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам
- COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень
- COSO учитывает корпоративную культуру и разработку политик
- COSO – это система отказоустойчивости

59. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?

- NIST и OCTAVE являются корпоративными
- NIST и OCTAVE ориентирован на ИТ
- AS/NZS ориентирован на ИТ
- NIST и AS/NZS являются корпоративными

60. Методы анализа риска:

- Хаотический.
- Единичный.
- Статистический.
- Периодический.

61. Что в сфере информационной безопасности принято считать риском?

(1) потенциальную возможность понести убытки из-за нарушения безопасности информационной системы

(2) потенциально возможное происшествие неважно, преднамеренное или нет, которое может оказать нежелательное воздействие на компьютерную систему, а также информацию, хранящуюся и обрабатывающуюся в ней

(3) характеристику, которая делает возможным возникновение угрозы

60. Что принято считать ресурсом или активом информационной системы?

(1) модель информационной системы

(2) все элементы, имеющие материальную ценность независимо от того подлежат они защите или нет

(3) именованный элемент информационной системы, имеющий (материальную) ценность и подлежащий защите

61. Что отличает риск от угрозы?

(1) объем вероятных потерь

(2) наличие количественной оценки возможных потерь и (возможно) оценки вероятности реализации угрозы

(3) угроза и риск - понятия идентичные

62. Почему аналитический метод определения минимальных затрат при расчетах защиты информационной системы неприменим?

(1) потому, что расчеты ресурсов подвержены флуктуациям, связанными с колебаниями на рынке услуг в сфере безопасности ИС

(2) потому, что на практике точные зависимости между затратами и уровнем защищенности определить не представляется возможным

(3) потому, что уровень защищенности информационной системы неадекватен затратам на ее защиту

63. Идентифицируется ли риск уязвимостью, через которую может быть реализована некая угроза в отношении определенного ресурса?

(1) да

(2) нет

(3) да, но только в случае отсутствия угрозы

64. На какие ресуры может быть направлена угроза?
(1) только на информационные ресурсы
(2) только на аппаратные ресурсы
65. Что представляет собой система с полным перекрытием?
(1) система, в которой ведется учет всех вторжений, блокируются только вредоносные проникновения
(2) система, в которой имеются средства защиты на каждый возможный путь проникновения
(3) система, в которой обеспечивается селективная безопасность
66. Что происходит с размером ожидаемых потерь при увеличении затрат на защиту?
(1) падает
(2) находится в зависимости от других факторов
(3) не изменяется
67. Каким параметром принято определять степень разрушительности?
(1) коэффициентом разрушительности
(2) стоимостью ресурса
(3) коэффициентом риска
68. Какие из перечисленных вариантов решений в отношении рисков являются неуместными:
(1) принят, устранен
(2) принят, дезавуирован
(3) дезавуирован, отклонен
69. Какие из перечисленных характеристик не входят в систему обеспечения безопасности Клементса: O - набор защищаемых объектов; T - набор угроз; M - набор средств обеспечения безопасности; P- набор креативных функций; Z - набор виндикативных инструментов?
(1) O - набор защищаемых объектов; T - набор угроз; M - набор средств обеспечения безопасности; P- набор креативных функций
(2) O - набор защищаемых объектов; T - набор угроз; M - набор средств обеспечения безопасности; P- набор креативных функций; Z - набор виндикативных инструментов
70. В каком отечественном документе впервые в России выделено понятие риска в отношении ИБ?
(1) ГОСТ Р ИСО/МЭК 15408-2002
(2) КЗОТ
(3) УК РФ
71. Какое из перечисленных требований доверия к безопасности не является справедливым?
(1) к технологии разработки и тестированию
(2) к анализу уязвимостей
(3) верификации контента
72. На основании каких из перечисленных документов разрабатываются задания по безопасности?
(1) каталог сертифицированных профилей защиты и продуктов
(2) технический регламент
(3) профиль защиты
73. Какой термин определяет характеристику функции безопасности объекта оценки, выражающую минимальные усилия, которых теоретически может быть достаточно для нарушения работоспособности при прямой атаке на информационную систему?
(1) "потенциал падения"
(2) "стойкость функции безопасности (СФБ)"
(3) "резистивность системы" (РС)
74. Что из перечисленного характеризует потенциал нападения?

(1) показатели компетентности
(2) ресурсы
(3) мотивация
75. Каким образом мотивация связана с нарушителем и активами, которые его интересуют?
(1) мотивация может косвенно выражать вероятность нападения
(2) мотивация может быть связана с ценностью актива
(3) мотивация может быть связана с ресурсами нарушителя
76. Какой из перечисленных классов функциональных требований включает требования кодирования информации?
(1) класс приватности (конфиденциальности)"
(2) класс защиты функций безопасности объекта
(3) класс криптографической поддержки (криптографической защиты)
77. Что определяет ресурсы или активы ИС?
(1) модель ИС
(2) все элементы, имеющие материальную ценность независимо от того подлежат они защите или нет
(3) именованный элемент ИС, имеющий (материальную) ценность и подлежащий защите
78. Что представляет собой событие - триггер?
(1) событие, повлекшее реализацию или дальнейшее развитие рисков и являющееся идентификатором риска
(2) событие, увеличивающее время отклика web - сервера
(3) это одна из разновидностей атак на сервер
79. Каковы цели анализа и тестирования прикладных систем в аспектах информационной безопасности?
(1) оперативное внесение изменений в операционные системы
(2) обеспечение целостности программного обеспечения
(3) обеспечение более эффективного использования готовых пакетов программ
80. Какие из перечисленных мер способствуют предотвращению утечки?
(1) использование программного обеспечения, полученного от доверенных поставщиков
(2) применение аморфных схем контроля
(3) контроль целостности системы
81. Какие из перечисленных рекомендаций уместны в случае, когда для проведения работ по разработке программного обеспечения привлекается сторонняя организация?
(1) необходимо предусмотреть антиифильтрационные меры
(2) необходимо предусмотреть меры по контролю правильности выполненных работ
(3) необходимо предусмотреть меры по контролю качества выполненных работ
82. Какой из перечисленных вариантов последовательности действий предписан стандартом ГОСТ Р ИСО/МЭК 17799:2005 "Информационная технология. Практические правила управления информационной безопасностью" в аспектах управления непрерывностью бизнеса?
(1) идентифицировать события, которые могут быть причиной прерывания бизнес-процессов, провести оценку последствий, после чего разработать планы восстановления
(2) произвести экспертную оценку контента информации на сервере на предмет возможных схем утечки критически важной информации, после чего разработать планы восстановления системы
(3) произвести контроль плана восстановления и его тестирование на предмет реализуемости, затем идентифицировать события, которые могут быть причиной прерывания бизнес-процессов (отказ оборудования, пожар и т.п.)
83. Что формируют потенциальные злоумышленные действия по отношению к объектам?
(1) вероятностный набор действий по подавлению угроз
(2) шаблоны мер потенциального противодействия

(3) набор угроз ИБ
84. Что в аспектах информационной безопасности связывается с каждым объектом, требующим защиты?
(1) множество действий, к которым может прибегнуть нарушитель для получения несанкционированного доступа к объекту
(2) множество вариантов развития ситуации, при которых санкционированный доступ ведет к нарушению целостности системы объекту
(3) множество вариантов действий, к которым может прибегнуть нарушитель для валидации ID пользователя
85. Чем характеризуются угрозы?
(1) нежелательностью их появления
(2) невероятностью их появления
(3) вероятностью их появления
86. Содержит ли модель системы безопасности с полным перекрытием требования к составу подсистемы защиты ИС?
(1) да
(2) нет
(3) да, но лишь в имплицитной форме

87. Что из перечисленного предписывается выполнить при проектировании системы с полным перекрытием?
(1) выверить остаточную стоимость активов
(2) детально прописать пути потенциального проникновения
(3) согласовать порядок применения альтернативных инструментов защиты
88. Рассматривается ли в системе с полным перекрытием вопрос соотношения затрат на защиту и получаемого эффекта?
(1) да
(2) нет
(3) в системе с полным перекрытием эта величина не является критической
89.С какой целью предпринимаются контрмеры в аспектах защиты активов от угроз?
(1) в целях уменьшения уязвимостей
(2) в целях политики безопасности владельцев активов
(3) в целях получения дополнительной прибыли
90.Способствуют контрмеры в аспектах достижения информационной безопасности эффективному снижению уязвимостей?
(1) да
(2) нет
(3) лишь отчасти
91. Может ли анализ угроз каким-то образом помочь при выборе контрмер для противостояния угрозам и уменьшения рисков до приемлемого уровня?
(1) нет
(2) да
(3) спорно
92. Что обеспечивает базовая стойкость?
(1) защиту от тщательно спланированного и организованного нарушения безопасности объекта оценки нарушителем с высоким потенциалом нападения
(2) защиту от целенаправленного нарушения безопасности объекта оценки нарушителем с умеренным потенциалом нападения
(3) адекватную защиту от случайного нарушения безопасности объекта оценки нарушителем с низким потенциалом нападения
93. Что обеспечивает средняя стойкость системы?

(1) защиту от целенаправленного нарушения безопасности объекта оценки нарушителем с умеренным потенциалом нападения
(2) защиту от тщательно спланированного и организованного нарушения безопасности объекта оценки нарушителем с высоким потенциалом нападения
(3) адекватную защиту от случайного нарушения безопасности объекта оценки нарушителем с низким потенциалом нападения

94. Чем определяется высокая стойкость системы?
(1) уровнем стойкости функции безопасности объекта оценки, на котором она обеспечивает защиту от тщательно спланированного и организованного нарушения безопасности ОО нарушителем с высоким потенциалом нападения
(2) уровнем стойкости, при котором обеспечивается защита от целенаправленного нарушения безопасности объекта оценки нарушителем с умеренным потенциалом нападения
(3) уровнем стойкости функции безопасности объекта оценки, на котором обеспечивается адекватная защита от случайного нарушения безопасности ОО нарушителем с низким потенциалом нападения

Задания в открытой форме

1. Экономическая безопасность предприятия характеризуется_____

2. В процессе функционирования предприятие подвергается следующим угрозам_____

3. При построении эффективной системы информационного обеспечения необходимо решать задачи_____

4. Создание системы защиты информации на предприятии обеспечивает_____

5. Пользователь осуществляет удаленный доступ к информации на сервере. Пусть условный уровень защищенности информации на сервере - 24 единицы; условный уровень защищенности рабочего места пользователя - 10 единиц. Оцените условный уровень защищенности удаленного доступа пользователя к информации на сервере_____

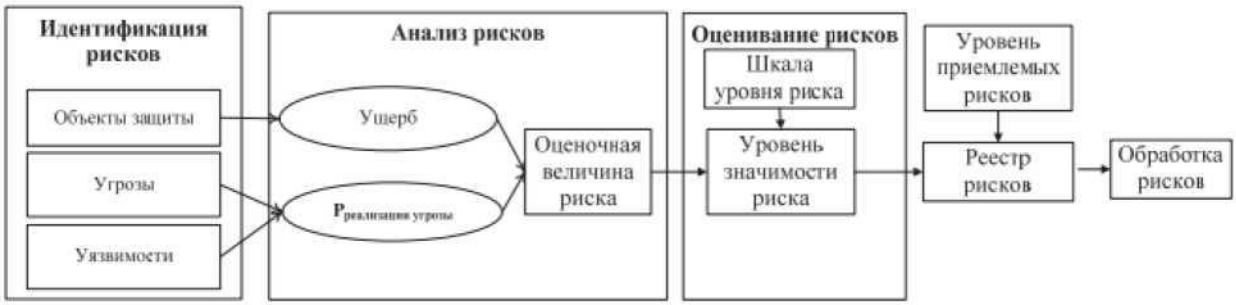
6. Методика и одноименное инструментальное средство RA SoftwareTool основаны на требованиях международных стандартов и _____

7. Раскройте значение каждого элемента формулы $R = P_{угр} R_n C \frac{K_o + K_i}{2} 100\%$ _____

8. Дайте развернутую характеристику информационному активу - программно-аппаратные средства_____

9. Раскройте методику управления рисками CRAMM_____

10. Дайте развернутую характеристику процессу оценки информационных рисков педставленному на рисунке_____



11. Информация как товар характеризуется таким показателем как_____

12. Жизненный цикл товара (ЖЦТ) представляет собой_____

13. Защита и поддержание информационной инфраструктуры на современном уровне заключается в _____

14. Раскройте значение каждого элемента формулы $Z - V * q - U * p = W$

_____

15. Перечислите основные методы определения затрат на информационную безопасность_____

16. Объектами интеллектуальной собственности (ОИС) принято называть_____

17. Перечислите прямые и косвенные виды ущерба, наносимые информации_____

18. Опишите процесс оценки эффективности криптографической защиты_____

19. Угрозой информации называют_____

20. Перечислите методы оценки эффективности защиты и страхования информации_____

Задания на установление соответствия

1. между элементами затрат и функциями затрат

1	Затраты на обслуживание системы информационной безопасности	А	Затраты на идентификацию угроз безопасности
2	Затраты на контроль работы системы безопасности	Б	Затраты на доставку и обмен конфиденциальной информации
3	Затраты на обеспечение должного качества информационных технологий и их соответствия требованиям стандартов	В	Затраты на обслуживание и настройку программно-технических средств защиты
4	Затраты, связанные с пересмотром политики информационной безопасности предприятия	Г	Затраты на контроль за действиями персонала

2.Установите соответствие между сведениями, содержащими коммерческую тайну

1	Сведения о финансовой деятельности	А	прибыль, кредиты, товарооборот, финансовые отчеты и прогнозы, коммерческие замыслы, фонд заработной платы, стоимость основн тежа, банковские счета, плановые и отчетные калькуляции;
2	Информация о рынке	Б	цены, скидки, условия договоров, спецификация продукции, объем, история, тенденции производства и прогноз для конкретного продукта, рыночная политика и планирование, мар тегия цен, отношения с потребителем и репутация, численность и размещения торговых агентов, каналы и методы сбыта, политика сбыта, программа рекламы;
3	Сведения о производстве продукции	В	сведения о техническом уровне, технико-экономических характеристиках разрабатываемых изделий, сведения о планируем о применяемых и перспективных технологиях, технологических процессах, приемах и оборудовании, сведения о модификации и модернизации ранее известных технологий, процессов;
4	Сведения о научных разработках	Г	новые технологические методы, новые технические, технологические и физические принципы, программы НИР, новые алгоритмы, оригинальные программы;

3. Установить соответствие между элементами и функциями

1	Доступность	А	это критерий, который учитывает, насколько удобно источнику угроз использовать определенный вид уязвимости, чтобы нарушить информационную безопасность
2	Фатальность	Б	характеристика, которая оценивает глубину влияния уязвимости на

			возможности программистов справиться с последствиями созданной угрозы для информационных систем
3	Количество	В	характеристика подсчета деталей системы хранения и реализации информации, которым присущ любой вид уязвимости в системе.

4.Установите соответствие между методологиями риск-менеджмента

1	NIST SP 800-39	А	предлагает для обеспечения безопасности и конфиденциальности использовать подход управления жизненным циклом систем
2	NIST SP 800-37	Б	предлагает трехуровневый подход к управлению рисками: организация, бизнес-процессы, информационные системы. Данный стандарт описывает методологию процесса управления рисками: определение, оценка, реагирование и мониторинг рисков
3	NIST SP 800-30	В	описывает подход к процессу мониторинга информационных систем и ИТ-сред в целях контроля примененных мер обработки рисков ИБ и необходимости их пересмотра
4	NIST SP 800-137	Г	сфокусирован на ИТ, ИБ и операционных рисках, описывает подход к процессам подготовки и проведения оценки рисков, коммуницирования результатов оценки, а также дальнейшей поддержки процесса оценки

5. Установите соответствие технического построения оборудования

1	Связанные с техническими средствами излучения	А	электромагнитные методики
2	Активизируемые	Б	вредоносные ПО, нелегальные программы, технологические выходы из программ, что

			объединяется термином «программные закладки»
3	создаются особенностями объекта, находящегося под защитой	В	расположение объекта, организация каналов обмена информацией
4	зависят от особенностей элементов-носителей	Г	детали, обладающие электроакустическими модификациями

6. Установите соответствие между международной организации по стандартизации ISO

1	ISO/IEC 27005:2018	А	предлагает подходы к оценке необходимости приобретения киберстраховки как меры обработки рисков, а также к оценке и взаимодействию со страховщиком
2	ISO/IEC 27102:2019	Б	входит в серию стандартов ISO 27000 и является логически взаимосвязанным с другими стандартами по ИБ из этой серии. Данный стандарт отличается фокусом на ИБ при рассмотрении процессов управления рисками
3	ISO/IEC 31000:2018	В	описывает подход к риск-менеджменту без привязки к ИТ/ИБ. Методы оценки риска» ссылается 607-П ЦБ РФ «О требованиях к порядку обеспечения бесперебойности функционирования платежной системы, показателям бесперебойности функционирования платежной системы и методикам анализа рисков в платежной системе, включая профили рисков»

7. Установить соответствие между принципами информационной безопасности

1	Целостность	А	информационных данных означает способность информации сохранять изначальный вид и

			структуру как в процессе хранения, как и после неоднократной передачи. Вносить изменения, удалять или дополнять информацию вправе только владелец или пользователь с легальным доступом к данным.
2	Конфиденциальность	Б	характеристика, которая указывает на необходимость ограничить доступа к информационным ресурсам для определенного круга лиц. В процессе действий и операций информация становится доступной только пользователям, который включены в информационные системы и успешно прошли идентификацию
3	Доступность	В	информация, которая находится в свободном доступе, должна предоставляться полноправным пользователям ресурсов своевременно и беспрепятственно
4	Достоверность	Г	принадлежность информации доверенному лицу или владельцу, который одновременно выступает в роли источника информации

8.Установить соответствие между элементами и функциями

1	программный риск	А	риск, связанный с вероятностью потерь финансовых ресурсов
2	финансовый риск	Б	Финансовые или репутационные потери, которые могут возникнуть в результате недостаточной осведомленности или непонимания, двусмысленности или безрассудного безразличия
3	юридический риск	В	текущий или будущий риск потери дохода, капитала или возникновения убытков в связи с нарушениями или несоответствием внутренним и внешним правовым нормам, таким как законы, подзаконные

			акты регуляторов, правила, регламенты, предписания, учредительные документы
4	риск несоответствия законодательству	Г	причины, из-за которых проект может быть неуспешным. Это могут быть технические риски, проектные риски, экономические риски.

9. 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.

10.Установить соответствие между элементами и функциями

1	Идентификация рисков	А	Сравнение уровней рисков с критериями сравнения рисков и критериями принятия рисков
2	Оценка опасности рисков	Б	Формируется и утверждается руководством список принимаемых рисков
3	Принятие рисков	В	выявление последствий реализации угроз нарушения конфиденциальности / целостности / доступности ИТ-активов
4	Поддержка и улучшение процесса управления рисками ИБ	Г	Контекст, оценка и план обработки рисков должны оставаться релевантными текущей ситуации и обстоятельствам

11. 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

12. Установить соответствие

1	Информация как предмет труда	А	это первичные исходные данные, сведения в конкретной сфере деятельности и смежных с нею областях
2	Информация как средство труда	Б	это совокупность знаний, данных и приемов, при помощи которых исходная информация (предмет труда) может быть наиболее эффективным образом обработана в целях получения запланированного результата
3	Информация как результат	В	должна обладать потребительскими свойствами, то есть снижать неопределенность ситуации или риск, в которой оказался субъект
4	Продукция индустрии информации	Г	в укрупненном виде может быть подразделена на продукты (вычислительная техника, офисное оборудование, коммуникационное оборудование, программное обеспечение, информационный продукт) и услуги (техническое обслуживание, сопровождение программного обеспечения, обучение и консультации, услуги связи, услуги по обработке данных).

13. 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

14.Установить соответствие между процедурами управления оперрисками

1	Идентификация риска	А	Информирование СУОР о реализации событий , Регистрацию событий ОР
2	Операционный риск	Б	систематическое использование информации для установления опасностей относительно аспекта риска или для описания проблемы
3	Сбор и регистрация событий и потерь	В	риск, связанный с выполнением компанией бизнес-функций, включая риски мошенничества и внешних событий

15. 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

16. Установить соответствие между

1	Процедуры управления операционным риском	А	анализ базы событий самооценка анализ динамики количественных показателей (ключевых индикаторов риска) анализ результатов регуляторных проверок анализ результатов внешнего аудита анализ поступающих сигналов от сотрудников.
2	Сбор и регистрация информации о событиях операционного риска:	Б	автоматизированное (из информационных систем), неавтоматизированное (экспертным методом), алгоритмизированное выявление информации о рисках классификация рисковых событий

			оценка потерь, стоимости возмещения потерь регистрация рисковых событий в базе событий обновление информации, актуализация источников информации.
3	Мониторинг рисков:	В	анализ индикаторов риска и статистики контроль выполнения мероприятий мониторинг входящей информации.

17. Установить соответствие между элементами и функциями

1	Скрытие	А	метод защиты информации является в основе своей реализации на практике одним из основных организационных принципов защиты ин- формации - максимального ограничения числа лиц, допускаемых к секретам
2	Ранжирование	Б	метод защиты информации является частным случаем метода скрытия и включает в себя, во-первых, деление засекречиваемой ин- формации по степени секретности, и, во-вторых, регламентацию допуска и разграничение доступа к защищаемой информации
3	Дезинформация	В	распространении заведомо ложных сведений относительно истинного назначения каких-либо объектов и изделий, действительного состояния какой-то области государственной деятельности

18. Установить соответствие между элементами и функциями

1	В основные задачи управления	А	периметр безопасности сети

	ИБ входят		
2	Компоненты архитектуры безопасности включают	Б	распределять административные роли по типам и группам устройств
3	Подсистемы управления обновлениями позволяют автоматизировать следующие задачи	В	управление доступом к базе данных
4	Использование централизованного управления рабочими станциями и серверами позволяет	Г	контроль времени обновления ПО

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
4	Страхование	Г	метод защиты информации сводится к тому, чтобы защитить права и интересы собственника информации или средства информации как от традиционных угроз

20.Установить соответствие между этапами алгоритма проведения экспертизы ИС предприятия и их описанием

1	Формулирование цели экспертизы и определение ее объектов	А	Проверка соответствия предъявляемым к ней требованиям безопасности
2	Формирование аналитической группы	Б	Подготовка экспертизы, оказание помощи в проведении оценки, обработке и анализе ее результатов
3	Утверждение состава экспертной группы	В	Определение области компетенций
4	Подготовка необходимой информации об объектах экспертизы	Г	Получение информации от персонала, изучение документации

Задания на установление правильной последовательности

1. Установить в этапы построения комплексной системы защиты информации в порядке их реализации:

1. Выявление потенциально возможных угроз
2. Анализ состояния подсистем обеспечения безопасности
3. Обоснование структуры и технологии функционирования комплексной системы защиты информации
4. Предварительное обследование состояния объекта и уровня организации защиты информации

2. 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

3. 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

4. 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

5. Установить этапы разработки модели:
1. Построение модели
2. Объект
3. Корректировка модели
4. Анализ результатов
5. Исследование модели на компьютере

6. 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

7. 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 активыявляются целевым объектом

8. 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

9. 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»

10. 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

11. 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

12. 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

13. Расположить параметры для группировки данных в журнале брандмауэра информации об атаке:

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

6. Тип атаки

14. Расположить этапы процесса управления рисками информационной безопасности:

1. Описание методов YCL к ресурсам ОС
2. Формирование атрибутов безопасности и прав доступа субъектов
3. Выбор, реализация и проверка защитных мер
4. Анализ журналов безопасности ОС
5. Идентификация активов и ценности ресурсов, нуждающихся в защите

15. 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

16. 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.

17. 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

18. Выберите последовательность уровней защищенности персональных данных

1. специальные категории ПДн
2. биометрические ПДн
3. общедоступные ПДн
4. иные категории ПДн

19. Выберите последовательность уровней безопасности информации:

1. Административный уровень
2. Процедурный уровень
3. Программно-технический уровень

4. Законодательный уровень

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;

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

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

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

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

Соответствие 100-балльной и 5-балльной шкал

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

2.2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

Компетентностно-ориентированная задача № 1

Основные производственные фонды предприятия на начало года составили 470 млн. руб. В августе того же года приобретен комплекс технических средств защиты стоимостью 100 млн. руб., а 1 октября продано устаревшее оборудование по остаточной стоимости 186 млн. рублей. Найдите среднегодовую стоимость основных производственных фондов.

Компетентностно-ориентированная задача № 2-7

Выбрать средства и методы для проведения полного анализа и управления рисками на примере:

Вариант 1) Отделение коммерческого банка

Вариант 2) Поликлиника

Вариант 3) Колледж

Вариант 4) Офис страховой компании

Вариант 5) Рекрутинговое агентство

Вариант 6) Интернет-магазин

Какие сложные проблемы необходимо решить при выполнении полного анализа рисков страховой компании?

Компетентностно-ориентированная задача № 8

Предприятие производит 4000 изделий в год, ежеквартально приобретая материал для производства (в год предприятию требуется 360 тонн материала для производства); технологический запас 5 дней, среднее отклонение между поставками материала – 4 дня. Надо рассчитать величину производственного запаса материала для обеспечения производственной программы.

Компетентностно-ориентированная задача № 9

Оцените величину нанесенного организации ущерба и уровень защиты предприятия по частному функциональному критерию эффективности принимаемыхмер.

Компетентностно-ориентированная задача № 10

Фирма реализовала в 1 квартале года 5000 изделий, покрыв свои расходы, но не получив прибыли. Общие постоянные расходы составили 70 тыс рублей, удельные переменные 60 рублей. Во втором квартале было изготовлено 6000 изделий. Какова прибыль и рентабельность?

Компетентностно-ориентированная задача № 11

Фирма после внедрения СЗИ стоимостью 900 тыс рублей положительный эффект (снижение потерь) оценено в 1325 тыс. Оцените рентабельность затрат (в процентах).

Компетентностно-ориентированная задача № 12-15

Надо на основе исходных оценок найти показатель ALE (Annual Loss Expectancy) уменьшения среднегодовых потерь фирмы из-за инцидентов безопасности. ALE найдите как разницу между среднегодовым ущербом ДО – и ПОСЛЕ внедрения защитных мер (ALE=Ущ1-Ущ2, где Ущ1 – ущерб от инцидентов безопасности вУщ1-Ущ2, где Ущ1 – ущерб от инцидентов безопасности в текущем году, Ущ2 – в предыдущем).

Данные для оценки ущерба за 2 года:

Вариант 1) в прошлом году было 8 успешных для злоумышленников попыток взлома базы данных, в этом году – 1; оценка финансовых потерь от взлома в прошлом году 120000, в этом 15000. Число уязвимостей и сократилось в 4 раза (после применения мер защиты).

Вариант 2) в прошлом году было 8 успешных для злоумышленников попыток взлома базы данных, в этом году – 1; оценка финансовых потерь от взлома в прошлом году 2540000, в этом 35000. Число уязвимостей и сократилось в 4 раза (после применения мер защиты).

Вариант 3) в прошлом году было 8 успешных для злоумышленников попыток взлома базы данных, в этом году – 1; оценка финансовых потерь от взлома в прошлом году 140000, в этом 115000. Число уязвимостей и сократилось в 4 раза (после применения мер защиты).

Вариант 4) в прошлом году было 8 успешных для злоумышленников попыток взлома базы данных, в этом году – 1; оценка финансовых потерь от взлома в прошлом году 150000, в этом 10000. Число уязвимостей и сократилось в 4 раза (после применения мер защиты).

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.