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
Оценка рисков и угроз
(наименование дисциплины)

10.03.01Информационная безопасность, профиль «Безопасность автоматизированных систем»
(код и наименование ОПОП ВО)

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

Тема 1. Основные понятия дисциплины «Оценка рисков информационной безопасности».

1. Основные риски информационной безопасности?
2. Методы анализа рисков информационной безопасности?
3. Методы оценки рисков информационной безопасности?
4. Основные понятия менеджмента рисков информационной безопасности?
5. Стандарты управления рисками ИБ?
6. Методы снижения рисков ИБ?

Тема 2. Оценка информационных рисков.

1. В чём заключается положение о применимости системы управления рисками?
2. Как происходит документирование процедуры обеспечения ИБ?
3. Какие существуют способы снижения рисков?
4. В чём заключается управление ИБ?
5. Опишите этапы внедрения процедур системы управления ИБ

Тема 3. Управление рисками. Основные понятия.

1. Что такое система управления рисками, её назначение?
2. Опишите этапы процесса управления риском.
3. Какие существуют методики оценивания рисков?
4. В чём отличие между качественными и количественными методиками оценки рисков?
5. В чём преимущества и недостатки количественной модели управления рисками?
6. Как формируется модель угроз?
7. Как формируется модель уязвимостей?
8. Опишите модель оценки рисков на основе модели информационных потоков

Тема 4. Методики и технологии управления рисками.

1. В чём заключаются преимущества и недостатки качественных методик управления рисками?
2. Опишите метод COBRA.
3. Опишите метод RA Software Tool
4. Возможно ли применение метода RA Software Tool для описание рисков в системах, обрабатывающих гостайну и почему?
5. Опишите метод CRAMM.
6. Какой из методов управления рисками наиболее предпочтителен в национальной системе стандартов информационной безопасности и почему?

7. Как использовать метод CRAMM в аудите информационной безопасности?

Тема 5. Разработка корпоративной методики анализа рисков.

1. Кто ставит задачи разработки корпоративной методики анализа рисков?
2. Структура сценария анализа информационных рисков компании.
3. Преимущества и недостатки табличных методов оценки рисков.
4. Как происходит оценка рисков по двум факторам.
5. Приведите пример, когда возможна оценка риска по трём факторам
6. Какие критерии позволяют отнести риск к неприемлемым?

Тема 6. Современные методы и средства анализа и управление рисками информационных систем компаний

1. Назовите критерии, по которым какая-либопроцедура обеспечения ИБ может быть названа необходимой в бизнес-процессах компании.
2. Кто выполняет оценку риска?
3. В чём заключается методика FRAP.
4. Как формируется матрица рисков.
5. Недостатки матричного представления рисков
6. Что такое профиль угрозы?
7. Сопоставьте преимущества и недостатки методик Risk Watch и OCTAVE.
8. Как происходит определение категорий защищаемых ресурсов?

Критерии оценки:

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

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

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

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может

привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ПРАКТИЧЕСКИХ РАБОТ

Контрольные вопросы для защиты практической работы №1:

1. Назовите критерии, по которым какая-либо процедура обеспечения ИБ может быть названа необходимой в бизнес-процессах компании.
2. Кто выполняет оценку риска?
3. В чём заключается методика FRAP.
4. Как формируется матрица рисков.
5. Недостатки матричного представления рисков
6. Что такое профиль угрозы?
7. Сопоставьте преимущества и недостатки методик Risk Watch и OCTAVE.

Контрольные вопросы для защиты практической работы №2:

1. Назовите количественные показатели информационных ресурсов.
2. Как производится оценивание показателей и степени критичности информационных ресурсов для наихудшего варианта развития событий?
3. Назовите потенциальные воздействия на бизнес-деятельность компании при возможном несанкционированном ознакомлении с конфиденциальной информацией.
4. Назовите типы нарушений безопасности конфиденциальной информации.
5. Какие критерии входят в методику оценивания критически важных ресурсов компании?

Контрольные вопросы для защиты практической работы №3:

1. Какие существуют табличные методы оценки информационных рисков компании?
2. Как оценивается уровень угрозы по трем факторам?
3. Чем метод трех факторов отличается от метода двух факторов?
4. Назовите уровни угроз, уязвимостей, тяжести последствий и рисков.
5. Перечислите показатели негативного воздействия.

Контрольные вопросы для защиты практической работы №4:

1. Какие задачи решаются в ходе количественной оценки рисков безопасности?

2. Как проводится сопоставление денежной стоимости классам активов?
3. Какие категории используются при оценивании общей стоимости влияния для каждого актива?
4. Опишите подход к определению стоимости активов на основе сотрудничества с группой управления финансовыми рисками.
5. Какой документ регламентирует правила ссылок в государственном бухгалтерском учете для упрощения поиска существенных искажений?

Контрольные вопросы для защиты практической работы №5:

1. Опишите подход к определению степени ожидаемого разового ущерба.
2. Опишите подход к определению ежегодной частоты возникновения (ЕЧВ).
3. Опишите подход к определению ожидаемого годового ущерба (ОГУ).
4. Что характеризует величина ОГУ?

Критерии оценки:

6-8 баллов (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

4-5 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.

1-3 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.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1. В каких единицах измеряется риск?

а) в стоимостном выражении

б) во временном выражении

в) в процентах в уровнях

2. 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

3. 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

4. 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

5. 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

6. 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

7. 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

8. 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

9. 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

10. 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

11. 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

12. 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

13. 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

14. 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

15. 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

16. 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

17. 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

18. 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;

19. 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

20. 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.

21. 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

22. 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

23. 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

24. 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

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
- Анализ чувствительности
- Построение дерева решений

26. Следующее структурное подразделение службы защиты информации отвечает за контакты с правоохранительными органами по всем вопросам обеспечения безопасности деятельности объекта

- Группа режима
- Группа охраны и сопровождения
- Техническая группа
- Детективная группа

27. 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

28. 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

29. В обязанности какого сотрудника входит реализация и изменение средств защиты данных

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

30. В обязанности какого сотрудника входит контроль состояния защиты наборов данных

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

31. В обязанности какого сотрудника входит опубликование нововведений в области защиты

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

32. В обязанности какого сотрудника входит хранение резервных копий данных

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

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

- Сотрудник группы безопасности

- Администратор безопасности системы
- Администратор безопасности данных
- Руководитель группы

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

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

35. 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

36. Количественный состав службы безопасности зависит, прежде всего от

- Типа циркулирующей в ней конфиденциальной информации
- От возможностей фирмы
- Нормативных документов регуляторов
- Численности штата

37. 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

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

- Директор
- Начальник службы защита информации
- Аналитик
- Руководитель группы
- Юрист
- Администратор безопасности системы

39. Кто руководит проведением служебных расследований?

- Директор
- Начальник службы защиты информации
- Аналитик
- Руководитель группы
- Юрист
- Администратор безопасности системы

40. Кто несёт персональную ответственность за выполнение службой защиты информации своих функций?

- Начальник службы защиты информации
- Сотрудник сектора обеспечения безопасности
- Аналитик
- Руководитель группы

- Юрист

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

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

42. Кто обеспечивает режим допуска и доступа?

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

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

- Группа режима
- Группа охраны и сопровождения
- Техническая группа
- Детективная группа

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

- Группа режима
- Группа охраны и сопровождения
- Техническая группа
- Детективная группа

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

- Группа режима
- Группа охраны и сопровождения
- Техническая группа
- Детективная группа

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

- Группа режима
- Группа охраны и сопровождения
- Техническая группа
- Детективная группа

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

- Группа режима
- Техническая группа
- Детективная группа

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

- Группа режима
- Группа охраны и сопровождения
- Техническая группа

- Детективная группа

49. Следующее структурное подразделение службы защиты информации отвечает за приобретение и установку различных технических средств для службы безопасности

- Группа режима
- Группа охраны и сопровождения
- Техническая группа
- Детективная группа

50. Следующее структурное подразделение службы защиты информации отвечает за техническое обеспечение мероприятий детективной группы

- Группа режима
- Группа охраны и сопровождения
- Техническая группа

51. Следующее структурное подразделение службы защиты информации отвечает за проверку кандидатов для приема на работу на объекте

- Группа режима
- Группа охраны и сопровождения
- Техническая группа
- Детективная группа

52. Следующее структурное подразделение службы защиты информации отвечает за проведение специальных мероприятий в отношении фирм-конкурентов

- Группа режима
- Группа охраны и сопровождения
- Техническая группа
- Детективная группа

53. Следующее структурное подразделение службы защиты информации отвечает за контакты с правоохранительными органами по всем вопросам обеспечения безопасности деятельности объекта

- Группа режима
- Группа охраны и сопровождения
- Техническая группа

54. 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

55. 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

56. 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

57. 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

58. Методы анализа риска:

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

59. 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?

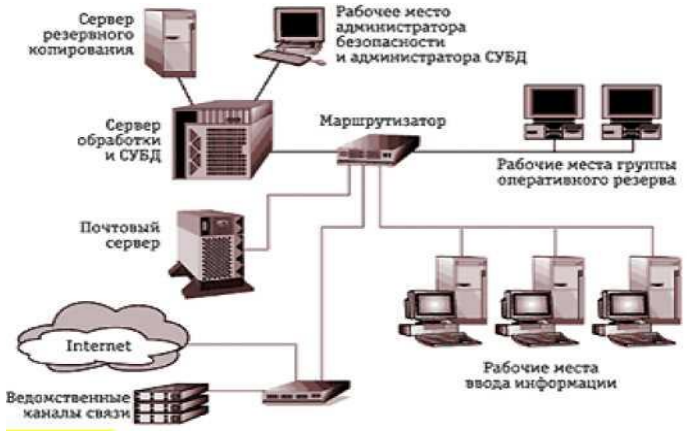
(1) уровнем стойкости функции безопасности объекта оценки, на котором она обеспечивает защиту от тщательно спланированного и организованного нарушения безопасности ОО нарушителем с высоким потенциалом нападения

(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. Видами рисков в предпринимательской деятельности являются……..
2. В процессе функционирования предприятие подвергается следующим угрозам……..
3. К методам анализа риска относятся…….
4. Способами минимизации рисков являются……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_____
5. Выделите основные элементы системы



Ответ_____

6. COBRA это методика позволяющая выполнить в _____ режиме простейший вариант _____информационных рисков любой компании. Для этого предлагается _____

7. Методика и одноименное инструментальное средство RA Software Tool основаны на требованиях международных стандартов и _____

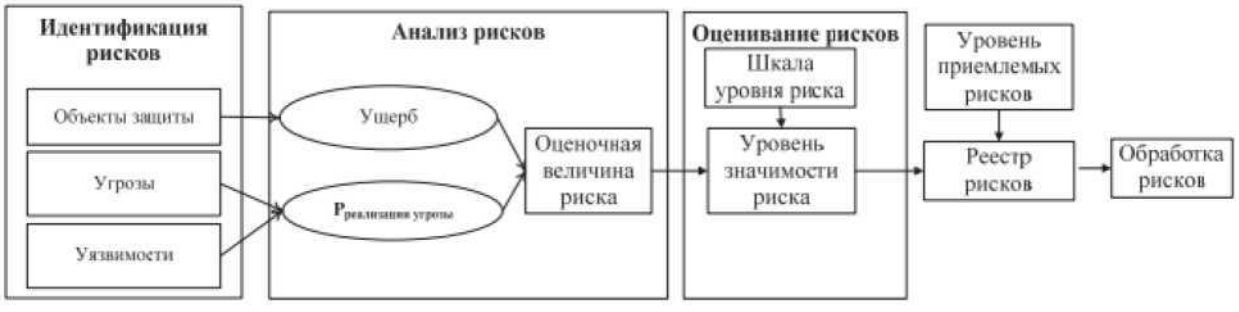
8. Раскройте значение каждого элемента формулы

$$R = P_{\text{угр}} R_{\text{л}} C \frac{K_o + K_i}{2} 100\%$$

9. Дайте развернутую характеристику информационному активу - программно-аппаратные средства.

10. Раскройте методику управления рисками CRAMM

11. Дайте развернутую характеристику процессу оценки информационных рисков педставленному на рисунке



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. Установить соответствие топологии сети её характеристике

1	Общая шина	А	Каждая рабочая станция сети соединяется с несколькими другими рабочими станциями этой же сети
2	Звезда	Б	В данной топологии все рабочие станции соединены друг с другом с помощью центрального концентратора
3	Кольцо	В	В основе топологии лежит общий кабель (магистраль), к которому подсоединяются все рабочие станции
4	Комбинированные решения	Г	Топология, в которой каждая рабочая станция соединяется только с двумя соседними

3. способов и видов информации

1	По способу кодирования	А	Цифровая, аналоговая
2	По способу представления	Б	Визуальная, звуковая, документ
3	По способу обработки	В	Текстовая, графическая, числовая
4	По способу восприятия	Г	Непрерывная, дискретная

4. Установить соответствие названия ОС её назначению

1	NetWare	А	Серверная операционная система для поддержки виртуальных машин, включая виртуальные машины на Linux.
2	LANtastic	Б	Серверная операционная система с объектно-ориентированный интерфейсом OS/2 для создания мощного набора графических средств администратора.
3	Windows Server 2019	В	Сетевая операционная система и набор сетевых протоколов для взаимодействия с компьютерами-клиентами, подключёнными к сети
4	LAN server	Г	Сетевая операционная система для DOS, Windows,OS/2 с поддержкой технологии Ethernet, ARCNET и Token Ring

5. Установить соответствие между способами и видами информации

1	По способу кодирования	А	Цифровая, аналоговая
2	По способу представления	Б	Визуальная, звуковая, документ
3	По способу обработки	В	Текстовая, графическая, числовая
4	По способу восприятия	Г	Непрерывная, дискретная

6. Установить соответствие названия протокола его назначению

1	FTP	А	Протокол передачи данных
2	SMTP	Б	Протокол передачи файлов
3	TCP/IP	В	Протокол передачи гипертекста
4	HTTP	Г	Протокол передачи почты

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 активы являются 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. 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

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

Изучив предложенную схему подготовить информацию, ответить на следующие вопросы:

1. Прочитать схему, объяснив принцип действия.
2. Определить область применения.
3. Отметить наиболее важные аспекты и их влияние на безопасность информационной системыВыводы о целесообразности и месте применения данного механизма.

Компетентностно-ориентированная задача № 2

Выбрать средства и методы для проведения полного анализа и

управления рисками на примере страховой компании.

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

Компетентностно-ориентированная задача № 3

Представить основные этапы полного анализа рисков министерства социальной защиты, при работе его сотрудников с системой обработки персональных данных.

Компетентностно-ориентированная задача № 4

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

Компетентностно-ориентированная задача № 5-10

Используя требования ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Методы и средства обеспечения безопасности.» Часть 3 «Методы менеджмента безопасности информационных технологий» Выберите один из различных информационных актива организации представленных ниже:

Вариант 1) Отделение коммерческого банка

Вариант 2) Поликлиника

Вариант 3) Колледж

Вариант 4) Офис страховой компании

Вариант 5) Рекрутинговое агентство

Вариант 6) Интернет-магазин

1. Из **Приложения D** ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.
2. Пользуясь **Приложением С** ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.
3. Пользуясь одним из методов (см. вариант) предложенных в **Приложении Е** ГОСТа произведите оценку рисков информационной безопасности.
4. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

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.