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

Организация и управление службой защиты информации
(наименование учебной дисциплины)

10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий»
(код и наименование ОПОП ВО)

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

Тема 1. Структура службы информационной безопасности.

1. Охарактеризуйте общую структурную схему службы защиты информации.
2. Каковы основные направления деятельности службы информационной безопасности СУИБ?
3. Что входит в понятие «службы информационной безопасности»?
4. Каковы цели создания системы обеспечения информационной безопасности?
5. Каковы функции системы информационной безопасности?
6. Какие принципы построения системы безопасности предприятия?

Тема 2. Функции основных групп службы безопасности

1. Каковы функции сотрудников группы режима?
2. Каковы функции сотрудников группы охраны и сопровождения?
3. Чем занимаются сотрудники технической группы?
4. Что такое детективная группа?
5. Назовите должностные обязанности сотрудников службы безопасности
6. Какой минимальный штатный состав службы безопасности?

Тема 3. Цели и задачи службы информационной безопасности

1. Назовите цели обеспечения безопасности предприятия
2. Каковы основные задачи службы информационной безопасности?
3. Перечислите функции службы информационной безопасности.
4. Какие требования предъявляются к защите информации?
5. Какие существуют методы защиты информации?

Тема 4. Организационные основы и принципы деятельности службы информационной безопасности

1. В чем заключается организация деятельности службы безопасности?
2. Для чего предназначено правовое обеспечение информационной безопасности?
3. Каковы основные принципы организации информационной безопасности?
4. Какие есть гарантии безопасности объектов защиты?
5. Назовите виды пакетов документов для деятельности службы информационной безопасности

6. Что осуществляет служба информационной безопасности для решения текущих задач?

Тема 5. Лицензирование видов деятельности службы безопасности.

1. Какая деятельность различных подразделений службы безопасности предприятия подлежит лицензированию, согласно Федеральному закону «О лицензировании отдельных видов деятельности» от 8.08.2001 года №128-ФЗ?
2. Назовите порядок принятия решения о предоставлении лицензии, которая может быть выдана лицензирующим органом на основании следующих документов
3. Перечень видов деятельности предприятий в области защиты информации, подлежащих лицензированию.
4. Дайте определение термина «лицензирования деятельности предприятий в области защиты информации»
5. Назовите разделы устава службы безопасности предприятий
6. Какие можно дать рекомендации по разработке уставных документов службы безопасности предприятия?

Тема 6. Управление службой защиты информации

1. Какие существуют методы управления службой безопасности предприятия?
2. Какова особенность технологии управления службой безопасности предприятия?
3. Какие существуют функции процесса управления службой безопасности предприятия?
4. Назовите принципы управления службой безопасности предприятия?
5. Какие бывают виды обеспечения деятельности службы безопасности предприятия?
6. Управление безопасностью предприятия в кризисных ситуациях

Тема 7. Организация информационно-аналитической работы.

1. Назовите цели информационно-аналитической работы
2. Каковы задачи информационно-аналитической работы?
3. Какие направления деятельности у информационно-аналитической работы?
4. Охарактеризуйте методы информационно-аналитической работы.
5. Перечислите этапы выполнения информационно-аналитических исследований производственных ситуаций.
6. Каков порядок выполнения аналитических исследований?

Тема 8. Организация работы с персоналом предприятия.

1. Как происходит подбор кадров?
2. Как происходит подготовка кадров?

3. Как проводится проверка персонала на благонадежность?
4. Каков порядок заключение контрактов и соглашений о секретности?
5. Назовите особенности увольнения сотрудников, владеющих конфиденциальной информацией

Критерии оценки:

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

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

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

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

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ПРАКТИЧЕСКИХ РАБОТ

Практическое занятие № 1 «Анализ заданного нормативно-правового акта Российской Федерации»

1. Что представляет собой инструкция по работе с персональными данными в административном подразделении образовательной организации?
2. Какие части документа относятся к вопросам защиты информации?
3. Что показывают комментарии к данному документу?
4. Как менялся текст нормативного акта с момента его создания по настоящее время?
5. Какие Вы знаете федеральные законы о защите информации и информационной безопасности?
6. Какие принципы и рекомендации по обеспечению безопасности государства во всех сферах предусмотренных законом РФ, определяет ФЗ от 28.12.2010 №390-ФЗ «О безопасности»?
7. Дайте определение службы информационной безопасности.

Практическое занятие № 2 «Работа с нормативно-правовыми документами»

1. Какие особенности работы со справочно-информационной правовой системой «Консультант-Плюс»?
2. Как составить план работ по проведению мероприятий защите информации?
3. Охарактеризуйте порядок организационной защиты информации в переговорной комнате предприятия
4. Как формализовать требования по обеспечению безопасности ресурсов КИС в соответствии с действующим законодательством
5. Обоснуйте важность основных положений раздела «Рабочее место». Какие дополнительные требования необходимо ввести для Вашей организации?
6. Опишите как бы Вы ввели процедуру официального получения разрешения на доступ к ресурсам?
7. Укажите законные основания, на основе которых Ваша организация обязана обрабатывать персональные данные.

Практическое занятие № 3 «Система анализа рисков и проверки политики информационной безопасности предприятия»

1. Какие Вы знаете правила расследования инцидентов, связанных с несанкционированным доступом и другими несанкционированными действиями, возникшими в ходе процесса обеспечения безопасности политики информационной безопасности предприятия?

2. Как Вы понимаете понятие «аудит информационной безопасности»?

3. В чем заключается необходимость проведения аудита информационной безопасности?

4. Как Вы считаете, на сколько значимые результаты несет периодический мониторинг действий пользователей и администраторов ресурсов?

5. Как организовать подобную проверку, чтобы она носила результативный, а не формальный характер?

6. Каковы особенности структурных подразделений и категорий сотрудников: Комитет по информационной безопасности, владельцы ИСПДн, распорядители ИСПДн

7. Каковы функции администратор автоматизированных ресурсов обработки политики информационной безопасности предприятия?

Критерии оценки:

5 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.

4-3 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

2-1 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. Организационная структура службы информационной безопасности определяется:

(1) требованиями законодательства

(2) требованиями государственных и международных стандартов

(3) потребностями в защите информационных ресурсах и возможностями в соответствии с оценками руководителей предприятия

2. В состав службы информационной безопасности предприятия могут быть включены:

(1) отдел нормативной документации

(2) отдел технической поддержки пользователей

(3) отдел внутреннего аудита информационной безопасности

(4) отдел персонала

3. Отбор персонала при назначении на должности, связанные с обработкой конфиденциальной информации, включает в себя:

(1) психологическую оценку

(2) проверку знания внутренних регламентов работы с информацией

(3) оценку навыков использования средств обнаружения вторжений

4. В методологии работы с персоналом фигурируют такие понятия как:

(1) социальная инженерия, человеческий фактор, человеко-машинная система

(2) моделирование, анализ

(3) контроль, система обработки данных

5. К задачам обучения и информационной работы с персоналом предприятия относится:

(1) недопущение утечек информации с использованием уязвимостей в сетях и ПО

(2) ознакомление с требованиями законодательства и локальных регламентов

(3) противодействие методам "социальной инженерии"

6. Приемы социотехники основаны на:

(1) особенностях человеческой психологии

(2) недостатках организационных структур

(3) недостатках программных и аппаратных средств защиты информации

7. Обучение персонала, ответственного за обработку информации, включает в себя:

(1) изучение автоматизированных систем обнаружения вторжений

(2) изучение приемов и методов защиты информации, необходимых для выполнения должностных обязанностей

(3) ознакомление с возможными мерами ответственности в случае нарушения требований информационной безопасности

8. Основным противодействием методам "социальной инженерии" является:

(1) повышение надежности криптографических алгоритмов

(2) информационная работа с персоналом предприятия

(3) страхование информационных ресурсов

9. "Социальная инженерия" - это:

(1) метод нарушения информационной безопасности

(2) метод защиты от нарушений информационной безопасности

(3) метод осуществления общественных связей

10. Нарушения информационной безопасности с использованием социотехники предполагают:

(1) социологическое обследование персонала предприятия

(2) использование недостатков в организационной структуре предприятия

(3) обман сотрудников предприятия

11. Регламент реагирования на инциденты должен предусматривать:

(1) регламент круглосуточного дежурства технического персонала

(2) распределение функций персонала в процессе реагирования на инциденты

(3) соглашение с поставщиками ИТ-платформ о срочной поставке компонент, вышедших из строя в результате инцидентов

12. Обнаружение вторжений осуществляется на основе:

(1) косвенных признаков, сигнатур и сообщений пользователей

(2) внутренних признаков и сообщений администратора

(3) внешних признаков

13. К косвенным признакам, по которым могут быть выявлены нарушения информационной безопасности, относятся:

(1) опубликование конфиденциальной информации в открытых источниках

(2) использование баз данных и учетных записей в нехарактерное время

(3) резкое повышение нагрузки на информационные системы предприятия

14. На персонал, отвечающий за обнаружение вторжений, оказывает влияние такой негативный психологический фактор как:

(1) круглосуточный режим дежурства

(2) необходимость постоянно изучать новые методы анализа вирусов

(3) частые ложные сообщения пользователей о предполагаемом заражении вирусами

15. Высокий уровень полномочий необходим для локализации длящихся нарушений в связи с тем что:

(1) Локализация нарушений требует дорогостоящих услуг сторонних аналитиков

(2) для локализации нарушений может потребоваться временное оперативное отключение важных информационных систем предприятия

(3) для локализации нарушений может потребоваться проинформировать о нарушениях большое число пользователей информационных систем

16. Ущерб от нарушения информационной безопасности включает в себя:

(1) уменьшение рыночной капитализации

(2) упущенную выгоду

(3) штрафные санкции за разглашение конфиденциальной информации

17. Расследование нападений, совершенных из корпоративной сети, по сравнению с нападением, совершенным из внешней сети, является:

(1) более легким

(2) более сложным

(3) аналогичным по сложности

18. Выявление вторжения в процессе его совершения по сравнению с выявлением уже завершенного нарушения:

(1) упрощает выявление нарушителя

(2) усложняет выявление нарушителя

(3) никак не влияет на сложность выявления нарушителя

19. Анализ действий нарушителя необходим для:

(1) проверки правильности настроек систем защиты информации

(2) установления сведений, известных нарушителю до нападения

(3) установления круга контактов, которые могли быть у нарушителя до нападения

20. Кто является основным ответственным за определение уровня классификации информации?

(1) руководитель среднего звена

(2) высшее руководство

(3) владелец

(4) пользователь

21. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

(1) сотрудники

(2) хакеры

(3) атакующие

(4) контрагенты (лица, работающие по договору)

22. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

(1) снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования

(2) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

(3) улучшить контроль за безопасностью этой информации

(4) снизить уровень классификации этой информации

23. Что самое главное должно продумать руководство при классификации данных?

(1) типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

(2) необходимый уровень доступности, целостности и конфиденциальности

(3) оценить уровень риска и отменить контрмеры

(4) управление доступом, которое должно защищать данные

24. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

(1) владельцы данных

(2) пользователи

(3) администраторы

(4) руководство

25. Что такое процедура?

(1) правила использования программного и аппаратного обеспечения в компании

(2) пошаговая инструкция по выполнению задачи

(3) руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

(4) обязательные действия

26. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

(1) поддержка высшего руководства

(2) эффективные защитные меры и методы их внедрения

(3) актуальные и адекватные политики и процедуры безопасности

(4) проведение тренингов по безопасности для всех сотрудников

27. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

(1) никогда, для обеспечения хорошей безопасности нужно учитывать и снижать все риски

(2) когда риски не могут быть приняты во внимание по политическим соображениям

(3) когда необходимые защитные меры слишком сложны

(4) когда стоимость контрмер превышает ценность актива и потенциальные потери

28. Что такое политики безопасности?

(1) пошаговые инструкции по выполнению задач безопасности

(2) общие руководящие требования по достижению определенного уровня безопасности

(3) широкие, высокоуровневые заявления руководства

(4) детализированные документы по обработке инцидентов безопасности

29. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

(1) анализ рисков

(2) анализ затрат / выгоды

(3) результаты ALE

(4) выявление уязвимостей и угроз, являющихся причиной риска

30. Что лучше всего описывает цель расчета ALE?

(1) количественно оценить уровень безопасности среды

(2) оценить возможные потери для каждой контрмеры

(3) количественно оценить затраты / выгоды

(4) оценить потенциальные потери от угрозы в год

31. Тактическое планирование – это:

(1) среднесрочное планирование

(2) долгосрочное планирование

(3) ежедневное планирование

(4) планирование на 6 месяцев

32.Что является определением воздействия (exposure) на безопасность?

(1) нечто, приводящее к ущербу от угрозы

(2) любая потенциальная опасность для информации или систем

(3) любой недостаток или отсутствие информационной безопасности

(4) потенциальные потери от угрозы

33. Эффективная программа безопасности требует сбалансированного применения:

(1) технических и нетехнических методов

(2) контрмер и защитных механизмов

(3) физической безопасности и технических средств защиты

(4) процедур безопасности и шифрования

34. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

(1) внедрение управления механизмами безопасности

(2) классификацию данных после внедрения механизмов безопасности

(3) уровень доверия, обеспечиваемый механизмом безопасности

(4) соотношение затрат / выгод

35. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

(1) только военные имеют настоящую безопасность

(2) коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности

(3) военным требуется больший уровень безопасности, т.к. их риски существенно выше

(4) коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

36. Как рассчитать остаточный риск?

(1) угрозы х риски х ценность актива

(2) (угрозы х ценность актива х уязвимости) х риски

(3) SLE х частоту = ALE

(4) (угрозы х уязвимости х ценность актива) х недостаток контроля

37. Что из перечисленного не является целью проведения анализа рисков?

(1) делегирование полномочий

(2) количественная оценка воздействия потенциальных угроз

(3) выявление рисков

(4) определение баланса между воздействием риска и стоимостью необходимых контрмер

38. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

(1) поддержка

(2) выполнение анализа рисков

(3) определение цели и границ

(4) делегирование полномочий

39. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

(1) чтобы убедиться, что проводится справедливая оценка

(2) это не требуется. для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ

(3) поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа

(4) поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

40. Что является наилучшим описанием количественного анализа рисков?

(1) анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности

(2) метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков

(3) метод, сопоставляющий денежное значение с каждым компонентом оценки рисков

(4) метод, основанный на суждениях и интуиции

41. Почему количественный анализ рисков в чистом виде не достижим?

(1) он достижим и используется

(2) он присваивает уровни критичности. их сложно перевести в денежный вид.

(3) это связано с точностью количественных элементов

(4) количественные измерения должны применяться к качественным элементам

42. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

(1) много информации нужно собрать и ввести в программу

(2) руководство должно одобрить создание группы

(3) анализ рисков не может быть автоматизирован, что связано с самой природой оценки

(4) Множество людей должно одобрить данные

43. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?

(1) стандарты

(2) должный процесс (Due process)

(3) должная забота (Due care)

(4) снижение обязательств

44. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

(1) список стандартов, процедур и политик для разработки программы безопасности

(2) текущая версия ISO 17799

(3) структура, которая была разработана для снижения внутреннего мошенничества в компаниях

(4) открытый стандарт, определяющий цели контроля

45. Из каких четырех доменов состоит CobiT?

(1) планирование и организация, приобретение и внедрение, эксплуатация и сопровождение, мониторинг и оценка

(2) планирование и организация, поддержка и внедрение, эксплуатация и сопровождение, мониторинг и оценка

(3) планирование и организация, приобретение и внедрение, сопровождение и покупка, мониторинг и оценка

(4) приобретение и внедрение, эксплуатация и сопровождение, мониторинг и оценка

46. Что представляет собой стандарт ISO/IEC 27799?

(1) стандарт по защите персональных данных о здоровье

(2) новая версия BS 17799

(3) определения для новой серии ISO 27000

(4) новая версия NIST 800-60

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

(1) COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам

(2) COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень

(3) COSO учитывает корпоративную культуру и разработку политик

(4) COSO – это система отказоустойчивости

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

(1) NIST и OCTAVE являются корпоративными

(2) NIST и OCTAVE ориентирован на ИТ

(3) AS/NZS ориентирован на ИТ

(4) NIST и AS/NZS являются корпоративными

49. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?

(1) анализ связующего дерева

(2) AS/NZS

(3) NIST

(4) анализ сбоев и дефектов

50. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?

(1) безопасная OECD

(2) ISOIEC

(3) OECD

(4) CPTED

51. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:

(1) гаммирования

(2) подстановки

(3) кодирования

(4) перестановки

(5) аналитических преобразований

52. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:

(1) гаммирования

(2) подстановки

(3) кодирования

(4) перестановки

(5) аналитических преобразований

53. Защита информации от утечки это деятельность по предотвращению:

(1) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации

(2) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

(3) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений

(4) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа

(5) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

54. Защита информации это:

(1) процесс сбора, накопления, обработки, хранения, распределения и поиска информации

(2) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа

(3) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств

(4) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям

(5) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё

55. Естественные угрозы безопасности информации вызваны:

(1) деятельностью человека

(2) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения

(3) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека

(4) корыстными устремлениями злоумышленников

(5) ошибками при действиях персонала

56. Искусственные угрозы безопасности информации вызваны:

(1) деятельностью человека

(2) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения

(3) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека

(4) корыстными устремлениями злоумышленников

(5) ошибками при действиях персонала

57. К основным непреднамеренным искусственным угрозам АСОИ относится:

(1) физическое разрушение системы путем взрыва, поджога

(2) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи

(3) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех

(4) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств

(5) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы

58. К посторонним лицам нарушителям информационной безопасности относится:

(1) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации

(2) персонал, обслуживающий технические средства

(3) технический персонал, обслуживающий здание

(4) пользователи

(5) сотрудники службы безопасности

(6) представители конкурирующих организаций

(7) лица, нарушившие пропускной режим

59. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата:

(1) черный пиар

(2) фишинг

(3) нигерийские письма

(4) источник слухов

(5) пустые письма

60. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

(1) черный пиар

(2) фишинг

(3) нигерийские письма

(4) источник слухов

(5) пустые письма

61. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:

(1) детектор

(2) доктор

(3) сканер

(4) ревизор

(5) сторож

62. Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:

(1) детектор

(2) доктор

(3) сканер

(4) ревизор

(5) сторож

63. Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:

(1) детектор

(2) доктор

(3) сканер

(4) ревизор

(5) сторож

64. Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:

(1) детектор

(2) доктор

(3) сканер

(4) ревизор

(5) сторож

65. Активный перехват информации это перехват, который:

(1) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации

(2) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций

(3) неправомерно использует технологические отходы информационного процесса

(4) осуществляется путем использования оптической техники

(5) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера

66. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

(1) активный перехват

(2) пассивный перехват

(3) аудиоперехват

(4) видеоперехват

(5) просмотр мусора

67. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:

(1) активный перехват

(2) пассивный перехват

(3) аудиоперехват

(4) видеоперехват

(5) просмотр мусора

68. Перехват, который осуществляется путем использования оптической техники называется:

(1) активный перехват

(2) пассивный перехват

(3) аудиоперехват

(4) видеоперехват

(5) просмотр мусора

69. К внутренним нарушителям информационной безопасности относится:

(1) клиенты

(2) пользователи системы

(3) посетители

(4) любые лица, находящиеся внутри контролируемой территории

(5) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации

(6) персонал, обслуживающий технические средства

(7) сотрудники отделов разработки и сопровождения ПО

(8) технический персонал, обслуживающий здание

70. К правовым методам, обеспечивающим информационную безопасность, относятся:

(1) разработка аппаратных средств обеспечения правовых данных

(2) разработка и установка во всех компьютерных правовых сетях журналов учета действий

(3) разработка и конкретизация правовых нормативных актов обеспечения безопасности

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

(1) хищение жестких дисков, подключение к сети, инсайдерство

(2) перехват данных, хищение данных, изменение архитектуры системы

(3) хищение данных, подкуп системных администраторов, нарушение регламента работы

72. Виды информационной безопасности:

(1) персональная, корпоративная, государственная

(2) клиентская, серверная, сетевая

(3) локальная, глобальная, смешанная

73. Цели информационной безопасности – своевременное обнаружение, предупреждение:

(1) несанкционированного доступа, воздействия в сети

(2) инсайдерства в организации

(3) чрезвычайных ситуаций

74. Основные объекты информационной безопасности:

(1) компьютерные сети, базы данных

(2) информационные системы, психологическое состояние пользователей

(3) бизнес-ориентированные, коммерческие системы

75. Основными рисками информационной безопасности являются:

(1) искажение, уменьшение объема, перекодировка информации

(2) техническое вмешательство, выведение из строя оборудования сети

(3) потеря, искажение, утечка информации

76. К основным принципам обеспечения информационной безопасности относится:

(1) экономической эффективности системы безопасности

(2) многоплатформенной реализации системы

(3) усиления защищенности всех звеньев системы

77. Основными субъектами информационной безопасности являются:

(1) руководители, менеджеры, администраторы компаний

(2) органы права, государства, бизнеса

(3) сетевые базы данных, фаерволлы

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

(1) установление регламента, аудит системы, выявление рисков

(2) установка новых офисных приложений, смена хостинг-компании

(3) внедрение аутентификации, проверки контактных данных пользователей

79. Принципом информационной безопасности является принцип недопущения:

(1) неоправданных ограничений при работе в сети (системе)

(2) рисков безопасности сети, системы

(3) презумпции секретности

80. Принципом политики информационной безопасности является принцип:

(1) невозможности миновать защитные средства сети (системы)

(2) усиления основного звена сети, системы

(3) полного блокирования доступа при риск-ситуациях

81. Принципом политики информационной безопасности является принцип:

(1) усиления защищенности самого незащищенного звена сети (системы)

(2) перехода в безопасное состояние работы сети, системы

(3) полного доступа пользователей ко всем ресурсам сети, системы

82. Принципом политики информационной безопасности является принцип:

(1) разделения доступа (обязанностей, привилегий) клиентам сети (системы)

(2) одноуровневой защиты сети, системы

(3) совместимых, однотипных программно-технических средств сети, системы

83. К основным типам средств воздействия на компьютерную сеть относится:

(1) компьютерный сбой

(2) логические закладки («мины»)

(3) аварийное отключение питания

84. Когда получен спам по e-mail с приложенным файлом, следует:

(1) прочитать приложение, если оно не содержит ничего ценного – удалить

(2) сохранить приложение в парке «спам», выяснить затем ip-адрес генератора спама

(3) удалить письмо с приложением, не раскрывая (не читая) его

85. Принцип Кирхгофа:

(1) секретность ключа определена секретностью открытого сообщения

(2) секретность информации определена скоростью передачи данных

(3) секретность закрытого сообщения определяется секретностью ключа

86. ЭЦП – это:

(1) электронно-цифровой преобразователь

(2) электронно-цифровая подпись

(3) электронно-цифровой процессор

87. Наиболее распространены угрозы информационной безопасности корпоративной системы:

(1) покупка нелицензионного ПО

(2) ошибки эксплуатации и неумышленного изменения режима работы системы

(3) сознательного внедрения сетевых вирусов

88. Наиболее распространены угрозы информационной безопасности сети:

(1) распределенный доступ клиент, отказ оборудования

(2) моральный износ сети, инсайдерство

(3) сбой (отказ) оборудования, нелегальное копирование данных

89. Наиболее распространены средства воздействия на сеть офиса:

(1) слабый трафик, информационный обман, вирусы в интернет

(2) вирусы в сети, логические мины (закладки), информационный перехват

(3) компьютерные сбои, изменение администрирования, топологии

90. Утечкой информации в системе называется ситуация, характеризуемая:

(1) потерей данных в системе

(2) изменением формы информации

(3) изменением содержания информации

91. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

(1) целостность

(2) доступность

(3) актуальность

92. Угроза информационной системе (компьютерной сети) – это:

(1) вероятное событие

(2) детерминированное (всегда определенное) событие

(3) событие, происходящее периодически

93. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

(1) регламентированной

(2) правовой

(3) защищаемой

94. Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:

(1) программные, технические, организационные, технологические

(2) серверные, клиентские, спутниковые, наземные

(3) личные, корпоративные, социальные, национальные

95. Окончательно, ответственность за защищенность данных в компьютерной сети несет:

(1) владелец сети

(2) администратор сети

(3) пользователь сети

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

(1) руководств, требований обеспечения необходимого уровня безопасности

(2) инструкций, алгоритмов поведения пользователя в сети

(3) нормы информационного права, соблюдаемые в сети

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

(1) аудит, анализ затрат на проведение защитных мер

(2) аудит, анализ безопасности

(3) аудит, анализ уязвимостей, риск-ситуаций

98. Основная масса угроз информационной безопасности приходится на:

(1) троянские программы

(2) шпионские программы

(3) черви

99. Какой вид идентификации и аутентификации получил наибольшее распространение:

(1) системы PKI

(2) постоянные пароли

(3) одноразовые пароли

100. Какие угрозы безопасности информации являются преднамеренными:

(1) ошибки персонала

(2) открытие электронного письма, содержащего вирус

(3) не авторизованный доступ

Задания в открытой форме

1. Распределение засекречиваемых данных, согласно уровню секретности, регламентацию и разделение допуска к защищаемым данным ……. .
2. В обязанности …… - сотрудника входит организация общей поддержки групп управления защитой и менеджмента в своей зоне ответственности
3. Количественный состав службы безопасности зависит от ….....
4. …… - разрабатывает руководящие документы и инструкции по вопросам безопасности?
5. …… - Кто обеспечивает режим допуска и доступа?
6. …… - структурное подразделение службы защиты информации отвечает за проведение работ по повышению квалификации персонала
7. …… - структурное подразделение службы защиты информации отвечает за организацию прохода персонала и посетителей в различные зоны безопасности
8. …… - структурное подразделение службы защиты информации отвечает за наблюдение за обстановкой вокруг объекта и на его территории
9. …… - структурное подразделение службы защиты информации отвечает за контроль работоспособности элементов системы защиты и их проверке
10. …… - структурное подразделение службы защиты информации отвечает за обеспечении безопасности деятельности объекта с помощью систем сигнализации, наблюдения, связи

11. …… - структурное подразделение службы защиты информации отвечает за планирование и проведение мероприятий по специальной защите объекта
12. …… - структурное подразделение службы защиты информации отвечает за приобретение и установку различных технических средств для службы безопасности
13. …… - структурное подразделение службы защиты информации отвечает за техническое обеспечение мероприятий детективной группы
14. …… - структурное подразделение службы защиты информации отвечает за проверку кандидатов для приема на работу на объекте
15. …… - структурное подразделение службы защиты информации отвечает за проведение специальных мероприятий в отношении фирм-конкурентов
16. …… - структурное подразделение службы защиты информации отвечает за контакты с правоохранительными органами по всем вопросам обеспечения безопасности деятельности объекта
17. …… - вырабатывает политику обеспечения защиты информации и обеспечивает ее реализацию?
18. …… - несёт персональную ответственность за выполнение службой защиты информации своих функций?
19. …… - в сфере информационной безопасности принято считать риском?
20. 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
21. На …… ресуры может быть направлена угроза?

Задания на установление соответствия

1. Установить соответствие

1) режимно-секретное подразделение	a) отвечает за выполнение комплекса мероприятий по пропускному режиму и осуществляют постоянный контроль над их выполнением
2) бюро пропусков	b) служат для непрерывного осуществления пропускного режима на территорию и объекты предприятия, контролируют вход и выход лиц с территории предприятия
3) контрольно-пропускной пункт (КПП)	c) решает непосредственно задачи по учету, хранению, уничтожению и выдаче пропусков сотрудникам предприятия, а также другим лицам, имеющим на это право

2. Установить соответствие

1) Политика безопасности	a) Для предотвращения несанкционированного доступа к ресурсам КИС используются пароли и/или аппаратные средства аутентификации
2) Цель политики информационной безопасности	b) Совокупность документированных правил, процедур, практических приёмов или руководящих принципов в области безопасности информации (БИ), которыми руководствуется организация в своей деятельности
3) Парольная политика	c) Общее описание правил работы с информацией компании, наличие сформулированных и закрепленных на бумаге правил обеспечения информационной безопасности позволит достичь: стабильности защиты, независимости защиты от личных и профессиональных качеств исполняющего персонала и возможности контроля как защиты, так и процедур обработки информации

3. Установить соответствие

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

4. Установить соответствие

1) Угроза анализа криптографических алгоритмов и их реализации	a) сетевое программное обеспечение
2) Угроза воздействия на программы с высокими привилегиями	b) прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение
3) Угроза доступа к локальным файлам сервера при помощи URL	c) виртуальная машина, информационная система, сетевое программное обеспечение, сетевой трафик

4) Угроза изменения системных и глобальных переменных	d) Метаданные, системное программное обеспечение

5. Установить соответствие

1) Модель угроз	a) совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных
2) Угрозы безопасности персональных данных	b) совокупность предположений о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности
3) Модель нарушителя	c) Документ, тем или иным способом описывающий возможные угрозы безопасности персональных данных.

6. Установить соответствие

1) Внешние нарушители	a) это субъект, который случайно или преднамеренно совершает действие, в результате чего возникают и/или могут быть реализованы угрозы нарушения безопасности информации.
2) Внутренние нарушители	b) лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы
3) Нарушитель безопасности информации	c) лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам

7. Установить соответствие:

1) Оптический канал	a) видовая информация — документы, изображения на мониторе, оборудование, новые модные коллекции, все, что можно увидеть или сфотографировать
2) Модифицированный оптический канал	b) оптико-электронный канал утечки речевой информации. Перехват ведется при помощи лазерного луча, испускаемого от лазерных

	акустических систем разведки (ЛАСР), а также триппель-призм (промежуточных элементов конструкции систем разведки, отражающих лазерный луч под определенным углом) на расстоянии до 500 метров
3) Акустический канал	c) Речь в помещении или из телефонного разговора. Мощный направленный микрофон перехватит сигнал на расстоянии до 100—150 м
4) Виброакустический	d) перехватываются и преобразуются в данные колебания твердых сред — стекол, труб, строительных конструкций, вызываемые механическим воздействием звуковых волн

8. Установить соответствие:

1) Заявителями на осуществление сертификации являются изготовители	a) а также на материально-технических базах заявителя и (или) изготовителя, расположенных на территории Российской Федерации.
2) Заявители должны обеспечивать соответствие сертифицированных средств защиты информации требованиям по безопасности информации	b) а также осуществлять устранение недостатков и дефектов средств защиты информации, в том числе устранение уязвимостей и недекларированных возможностей программного обеспечения средств защиты информации, информирование потребителей об обновлении программного обеспечения средств защиты информации, доведение до потребителей обновлений программного обеспечения средств защиты информации, а также изменений в эксплуатационную документацию (далее - техническая поддержка средств защиты информации)
3) Сертификационные испытания средств защиты информации проводятся на материально-технической базе испытательной лаборатории	c) а также федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления и организации, планирующие применять средства защиты информации

9. Установить соответствие

1) Требования ФСТЭК по защите	подбираются с учетом структуры СЗИ, состава и мест размещения ее элементов. Если защищаемая ИС

конфиденциальной информации	проектируется в составе центра обработки данных (ЦОД) рекомендуется использовать уже имеющиеся в ЦОД средства, меры защиты данных.
2) Методы и средства технической защиты информации	направлены на исключение неправомерного доступа, копирования, передачи или распространения сведений. Для обеспечения требований по безопасности конфиденциальной информации проводится оценка возможных уязвимостей ИС для внешних и внутренних нарушителей, возможных средств реализации этих уязвимостей.
3) Меры защиты информации в информационных системах	согласно требованиям ФСТЭК должны обеспечивать необходимый уровень безопасности при взаимодействии защищаемых ИС с другими ИС, при обработке и хранении информации. При этом предлагаемые на этапе проектирования меры должны быть реализуемы в конкретной ИС.

10. Установить соответствие

1) Клиент-сервер	a) Подключенная к сети, достаточно мощную вычислительную машину, обладающую определёнными ресурсами общего пользования, а также, как правило, возможностью объединять некоторое количество компьютеров как в локальной, так и в глобальной информационных сетях.
2) Сервер	b) Задача, рабочая станция, пользователь. Он может сформировать запрос для сервера: считать файл, осуществить поиск записи и т.п. Клиентский процесс в архитектуре клиент-сервер – процесс, который выполняется на стороне клиента и посылает запрос серверному процессу на выполнение некоторой задачи
3) Клиент	c) Вычислительная или сетевая архитектура, в которой задания или сетевая нагрузка распределены между поставщиками услуг (сервисов), называемыми серверами, и заказчиками услуг, называемыми клиентами

11. Установить соответствие

1) Объект защиты	a) информация, носители информации, технические средства и технология их обработки, а также средства защиты информации
2) Объект информатизации	b) совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения

	объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены
3) Защищаемые помещения	c) помещения (служебные кабинеты, актовые, конференц-залы), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров)
Утечка информации по техническому каналу	d) неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации

12. Установить соответствие

1) Состояние источника угрозы	a) 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	b) 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	c) 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	d) применение нестандартного канала пути к ресурсам, что включает в себя несанкционированное использование возможностей операционной системы, использование стандартного канала для открытия доступа к ресурсам, например, незаконное получение паролей и других параметров с дальнейшей маскировкой под зарегистрированного в системе пользователя

13. Установить соответствие

1) Автоматизированная система	a) система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая

	информационную технологию выполнения установленных функции
2) Контролируемая зона	b) пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных, технических и иных материальных средств
3) Специальные исследования	c) выявление с использованием контрольно-измерительной аппаратуры возможных каналов утечки защищаемой информации от основных и вспомогательных технических средств и систем
4) Специальная проверка	d) проверка технических средств и систем объекта защиты с целью выявления возможно внедренных электронных устройств съема информации (закладочных устройств)

14. Установить соответствие:

1) Перехват паролей	a) 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»	b) 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	c) название разновидности хищения информации и подрыва безопасности информационной системы говорит само за себя

15. Установить соответствие:

1) Принцип законности	a) необходимо нормативно- правовое регулирование этой области общественных отношений. Законодательно должны быть обозначены права различных субъектов в области защиты информации

2) Принцип защиты информации	b) сновополагающие идеи, важнейшие рекомендации по организации и осуществлению этой деятельности на различных этапах решения задач сохранения секретов
3) Принцип приоритета	c) бъектом засекречивания не могут быть сведения, которые государство обнародует или сообщает согласно конвенциям или соглашениям
4) Принцип собственности и экономической целесообразности	d) право собственникам информации принимать меры к защите этой информации, а также оценивать ее потребительские свойства

16. Установить соответствие

1) Случайные антенны	a) вспомогательные технические средства, их соединительные линии, а также линии электропитания, посторонние проводники и цепи заземления, при непосредственном подключении к которым средств разведки ПЭМИН возможен перехват информационных сигналов
2) Сосредоточенные	b) телефонный аппарат, громкоговоритель радиотрансляционной сети, датчик пожарной сигнализации и т. д., подключенные к линии, выходящей за пределы КЗ
3) Распределенные	c) кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы КЗ

17. Установить соответствие

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

18.Установить соответствие

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

19.Установите соответствие

1) однослойный перцептрон	a) представляет собой полностью связанный класс искусственных нейронных сетей прямой связи (ANN).
2) Многослойный персептрон	b) Математическая или компьютерная модель восприятия информации мозгом (кибернетическая *модель мозга*), предложенная Фрэнком Розенблаттом в 1958 году
3) Перцептрон,	c) это искусственный нейрон, который на вход принимает только 0 и 1.

20.Установите соответствие

1) Нелинейная функция	a) Дифференцируема на всей оси абсцисс, что используется в некоторых алгоритмах обучения, обладает свойством усиливать слабые сигналы лучше, чем большие, и предотвращает насыщение от больших сигналов, так как они соответствуют областям аргументов, где сигмоид имеет пологий наклон.
2) Сигмоидная функция	b) Функции, которые не реализуются однослойной сетью, называются линейно неразделимыми[2]. Решение задач, подпадающих под это ограничение, заключается в применении 2-х и более слойных се
3) Линейно неразделимая функция	c) Называется активационной и может иметь различный вид. Одной из наиболее

	распространеных является нелинейная функция с насыщением, так называемая логистическая функция или сигмоид (т.е. функция S-образного вида)

21.Установить соответствие

1) Мажоритарным элементом	называется пороговая схема с нечетным числом входов n, выходной сигнал которой равен 1 только при поступлении на ее входы не менее К=(n+1)/2 входных сигналов равных 1
2) Триггеры	электронные схемы, имеющие два устойчивых состояния, которые устанавливаются при подаче соответствующей комбинации сигналов на управляющие входы триггера и сохраняются после окончания действия этих сигналов.
3) Нейрокомпьютер "Эмбрион"	Система, основанная на коллективном спиновом резонансе.

Задания на установление правильной последовательности

1. Установить 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

12. Установите последовательность функций применительно к рассматриваемому объекту управления СПБ, по мнению В.П. Мак-Мака:
1. Организация
2. Контроль
3. Планирование
4. Мотивация
5. Регулирование.
6. Прогнозирование

13. Расположите в правильной последовательности этапы работ по построению (модернизации) системы защиты информации и поддержанию на требуемом уровне ее защиты в организации:
1. Определение мер по защите информации, вызванных изменениями целей и задач защиты, перечня защищаемых сведений, угроз безопасности информации
2. Уточнение перечня защищаемых сведений в организации, определение источников и носителей информации, выявление и оценка угроз ее безопасности;
3. Контроль эффективности мер по инженерно-технической защите информации в организации

14. Выберите правильную последовательность этапов проектирования (модернизации) системы защиты:

1. Моделирование угроз информации
2. Выбор мер защиты
3. Моделирование объектов защиты

15. Расположите в логической последовательности принципы управления службой безопасности, определяющих требования к системе, структуре и организации процесса управления:
1. Принцип системности и комплексности
2. Принцип оптимального сочетания централизации и децентрализации
3. Принцип сочетания прав, обязанностей и ответственности
4. Принцип плановости.
6. Научность
5. Единоначалие и коллегиальность

16. Расположите в правильной последовательности документы, которые представляет предприятие-учредитель в органы внутренних дел (по месту своего нахождения):
1. Лицензии на руководителя и персонал службы безопасности
2. Сведения о характере и направлениях деятельности службы безопасности, составе и предполагаемой численности персонала, наличии специальных средств, технических и иных средств, а также потребности в них и оружии
3. Устав службы безопасности
4. Заявление о согласовании Устава службы безопасности

17. Расположите в правильной последовательности этапы проектирования содержания функциональной управленческой деятельности:
1.Нормативное проектирование функциональной управленческой деятельности
2.Проектирование информационного обеспечения системы управления Макеты рабочих форм документов Проект технического обеспечения системы управления
3.Определение состава специфических функций и задач управления, осуществляемых в организации Классификатор функциональной управленческой деятельности
4.Формирование предварительного перечня документов, обеспечивающих выполнение специфических функций управления
5.Определение стадий «жизненных циклов» элементов организации, осуществляемых внутри организации
6.Определение нормативной трудоемкости документальных операций
7.Определение операционального содержания функциональной управленческой деятельности
8.Определение состава общих функций управления, осуществляемых в организации

9.Определение нормативной численности функционального управленческого персонала

18. Расположите в правильной последовательности этапы принципа плановости, состоящего в установлении основных направлений и пропорций
1. Сотрудник
2. Службы безопасности
3. Подразделения

19. Установить последовательность этапов построения программы обеспечения безопасности:
1. Установление уровня безопасности
2. Регулярный контроль пошаговой реализации плана безопасности
3. Проведение разъяснительных мероприятий и обучения персонала для поддержки требуемых мер безопасности
4. Определение ценности технологических и информационных активов организации
5. Формирование политики безопасности организации

20. Установить действия этапа анализа рисков:
1. Анализ угроз
2. Идентификация и оценка стоимости технологических и информационных активов
3. Оценка вероятности того, что угроза будет реализована на практике
4. Оценка рисков технологических и информационных активов

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
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
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.

Компетентностно-ориентированная задача № 2
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 2) Поликлиника
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.

Компетентностно-ориентированная задача № 3
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 3) Колледж
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.

Компетентностно-ориентированная задача № 4
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 4) Офис страховой компании
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.

Компетентностно-ориентированная задача № 5
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 5) Рекрутинговое агентство
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.

Компетентностно-ориентированная задача № 6
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 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.

Компетентностно-ориентированная задача № 7
Из Приложения D ГОСТа Р ИСО/МЭК ТО 13335-3-2007 «Методы и средства обеспечения безопасности» Часть 3 «Методы менеджмента безопасности информационных технологий» подберите три конкретных уязвимости системы защиты указанных информационных активов.

Компетентностно-ориентированная задача № 8
Пользуясь Приложением С ГОСТа Р ИСО/МЭК ТО 13335-3-2007 «Методы и средства обеспечения безопасности» Часть 3 «Методы менеджмента безопасности информационных технологий» напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

Компетентностно-ориентированная задача № 9
Пользуясь одним из методов предложенных в Приложении Е ГОСТа Р ИСО/МЭК ТО 13335-3-2007 произведите оценку рисков информационной безопасности.

Компетентностно-ориентированная задача № 10
Пользуясь ГОСТом Р ИСО/МЭК ТО 13335-3-2007 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.