МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование кафедры полностью)

М.О. Таныгин
(подпись, инициалы, фамилия)

«30» августа 2022 г.

ОЦЕНОЧНЫЕ СРЕДСТВА
для текущего контроля успеваемости
и промежуточной аттестации обучающихся
по дисциплине
Основы информационной безопасности
(наименование дисциплины)

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

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

Тема №1 «Базовые понятия»

1. Какой смысл несёт в себе словосочетание «информационная безопасность»?
2. Что такое информационная безопасность?
3. Что такое защита информации?
4. Какой смысл отражает в себе понятие – угрозы информационной безопасности?
5. От чего зависит информационная безопасность?
6. Что такое ущерб и в каком значении это слово употребляется в определении информационной безопасности?
7. Компьютерная безопасность, это информационная безопасность? Ответ объясните
8. Что такое доступность?
9. Что такое целостность?
10. Что такое конфиденциальность?
11. На какие два направления можно разделить понятие целостности?
12. О чем говориться в Доктрине информационной безопасности Российской федерации?
13. Что из себя представляет жизненный цикл ИС?

Тема №2 «Конфиденциальность. Классификация угроз»

1. Что такое угроза?
2. Как называют людей, предпринимающих попытки реализации угрозы?
3. Какой промежуток времени называют окном опасности?
4. По каким критериям производится классификация угроз?
5. Можно ли использовать несколько критериев для классификации одной угрозы? Ответ объясните
6. Перечислите основные источники внутренних отказов.
7. Приведите пример угрозы доступности.
8. Является ли удаленное потребление ресурсов угрозой?
9. Что понимается под конфиденциальной информацией?
10. Что такое вирус?
11. Что такое червь?
12. Перечислите основные угрозы целостности
13. Перечислите основные угрозы конфиденциальности
14. Какое назначение имеет перечень конфиденциальных сведений предприятия?
15. Какие угрозы наносят наибольший ущерб субъектам информационных отношений?

Тема №3 «Угрозы ИБ. Классы нарушителей. Оценка риска»

1. Определите перечень основных угроз для АС, состоящей из автономно работающего компьютера без выхода в сеть, расположенной в одной из лабораторий университета.
2. Постройте неформальную модель нарушителя для учебной компьютерной лаборатории.
3. Выведите формулу для расчета прочности трехуровневой защитной оболочки.
4. Охарактеризуйте защитные оболочки и перечень преград, применяемые в учебной компьютерной лаборатории.
5. Каким образом классифицируются каналы утечки информации?
6. Какие основные методы контроля доступа используются в известных вам информационных системах? В чем их достоинства и недостатки?
7. Что такое скрытые каналы утечки информации и как их обнаружить?

Тема №4 «Персональные данные. Защита авторских прав»

1. Что такое персональные данные?
2. Что из себя представляют авторские права?
3. Что такое обработка персональных данных?
4. Что включает в себя обработка персональных данных?
5. Перечислите основные принципы обработки персональных данных
6. Какая глава Гражданского кодекса описывает основные составляющие такого понятия как авторское право

Тема №5 «Выявление контрафактной продукции»

1. Что такое контрафактная продукция?
2. Перечислите оптимальные методы контроля и защиты информационных систем?
3. На основе каких критериев оценки следует выбирать средства защиты?
4. Что такое лицензирование программных продуктов и для чего оно производится?
5. Перечислите основные этапы лицензирования

Тема №6 «Криптографические методы защиты»

1. Приведите пример сервисов безопасности
2. Что такое криптография?
3. Что включает в себя понятие криптографическая защита информации?
4. Какие виды преобразования информации вы знаете?
5. Перечислите основные способы преобразования информации
6. Шифры каких видов вам знакомы?
7. Что из себя представляют потоковые шифры?
8. Что такое скремблирование?

9. Чем отличаются симметричные и ассиметричные шифры?
10. Что такое клеточный автомат и какое отношение это понятие имеет к шифрованию?

Критерии оценки:

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

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

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

1.2 ВОПРОСЫ И ЗАДАНИЯ В ТЕСТОВОЙ ФОРМЕ

Тема 1

1 Общими требованиями к системе защиты информации являются:
1. Целостность
2. Безопасность
3. Прозрачность
4. Все перечисленные

2 Режим защиты информации не устанавливается в отношении сведений, относящихся к:
1. государственной тайне
2. конфиденциальной информации
3. персональным данным
4. деятельности государственных деятелей

3 Засекречиванию подлежат сведения о:
1. состоянии демографии
2. состоянии преступности
3. силах и средствах гражданской обороны
4. фактах нарушения прав и свобод человека и гражданина

4 Режим документированной информации – это :
1. выделенная информация по определенной цели
2. выделенная информация в любой знаковой форме
3. электронная информация, позволяющая ее идентифицировать
4. электронный документ с электронно-цифровой подписью

5 Сколько видов электронной подписи существует согласно Российскому законодательству?
1. 1
2. 2
3. 3
4. 4

6 С точки зрения информационного права информация – это …:
1. форма выражения объективных знаний
2. сведения о законодательстве, правовых явлениях, правоприменительной деятельности
3. сведения независимо от формы их представления
4. данные о развитии конкретной правовой науки и ее практическом применении

Тема 2

7 К государственной тайне не относятся сведения, защищаемые государством …, распространение которых может нанести ущерб государству.

1. в экономической области
2. в оперативно-разыскной деятельности
3. в контрразведывательной деятельности
4. о частной жизни политических деятелей

8 Субъектами информационных отношений могут (может) быть …:

1. трансграничные информационно-телекоммуникационные сети
2. муниципальные образования
3. Российская Федерация
4. трудовой коллектив

9 С какого этапа начинается практически любой процесс по защите информации?

1. Обучение сотрудников
2. Обследование
3. Составление технического задания
4. Моделирование угроз

10 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

11 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

12 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

Тема 3

13 Признак, не относящийся к охраноспособной информации – это …:
1. доступ к охраноспособной информации ограничен только законом
2. защита охраноспособной информации устанавливается Законом
3. доступ к охраноспособной информации ограничен владельцем информационных ресурсов
4. охране подлежит только документированная информация

14 Какие три основные свойства информации достигаются с помощью защиты информации?
1. Актуальность, достоверность, защищенность
2. Отчуждаемость, правильность, упругость
3. Конфиденциальность, целостность, доступность
4. Нет правильного ответа

15 Когда применяются алгоритмы шифрования информации?
1. Когда мы не доверяем месту, где храним информацию
2. Когда мы не доверяем каналам связи, по которым передаем информацию
3. Когда нам требуется подтверждения подлинности отправителя
4. Во всех перечисленных случаях

16 Признак, не относящийся к коммерческой тайне:
1. отсутствует свободный доступ к информации
2. обладатель информации принимает меры к охране ее конфиденциальности
3. информация имеет действительную или потенциальную коммерческую ценность
4. сведения, содержащие коммерческую тайну, устанавливаются учредительными
5. документами

17 К служебной тайне не относится …:
1. тайна деятельности соответствующего органа
2. профессиональная тайна
3. вред, причиненный здоровью работника в связи с производственной травмой

18 Симметричное шифрование – это шифрование, в котором для зашифрования и расшифрования используется...:
1. Один ключ
2. Два ключа

Тема 4

19 Каким законом в Российской Федерации регламентируется процесс обработки и защиты персональных данных?

1. 97-ФЗ
2. 1-ФЗ
3. 137-ФЗ
4. 152-ФЗ

20 Кто имеет право выдавать сертификаты усиленной квалифицированной электронной подписи?

1. Аккредитованный удостоверяющий центр
2. Любой удостоверяющий центр
3. Организация, имеющая лицензию на деятельность по технической защите конфиденциальной информации
4. Организация, имеющая лицензию на деятельность по техническому обслуживанию, модернизации и распространению шифровальных средств

21 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

22 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

23 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.

24 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; ошибками при действиях персонала.

25 К основным непреднамеренным искусственным угрозам АСОИ относится:

1. физическое разрушение системы путем взрыва, поджога и т.п.;
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 и т.п.;
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.

Тема 5

26 Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

27 Как называется совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация?

1. несанкционированный канал утечки информации
2. технический канал утечки информации
3. параметрический канал утечки информации
4. физический канал утечки информации

28 Как называется бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена:

1. угроза
2. утечка
3. уязвимость
4. атака

29 Что является носителем информации в оптическом канале утечки информации?

1. акустическая волна
2. электрическое поле
3. электромагнитное поле
4. световая волна

30 К какому техническому каналу утечки информации относится несанкционированное распространение за пределы контролируемой зоны вещественных носителей с защищаемой информацией?

1. оптический
2. акустический
3. материально-вещественный
4. радиоэлектронный

31 Как называется пространство, в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств?

1. ограниченная зона
2. пограничная зона
3. контролируемая зона
4. зона 1

32 Как называется технический канал утечки информации, при котором производится съем информации с линии связи контактного подключения аппаратуры злоумышленника?

1. электромагнитный
2. электрический
3. индукционный

Тема 6

33 Как называется технический канал утечки информации, при котором производится бесконтактный съем информации с кабельных линий связи?

1. электромагнитный
2. электрический
3. индукционный

34 В каких технических каналах утечки акустической информации основным средством съема информации является микрофон?

1. воздушные
2. вибрационные
3. электроакустические

4. параметрические

35 В каких технических каналах утечки акустической информации основным средством съема информации является лазер?
   1. воздушные
   2. вибрационные
   3. электроакустические
   4. оптико-электронные

36 Возникновение каких каналов утечки акустической информации обусловлено тем, что в ВТСС и ОТСС есть элементы, обладающие "микрофонным эффектом"?
   1. воздушные
   2. вибрационные
   3. электроакустические
   4. параметрические

37 Как называются электромагнитные излучения технических средств, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях?
   1. вспомогательные электромагнитные излучения
   2. вторичные электромагнитные излучения
   3. побочные электромагнитные излучения
   4. недекларированные электромагнитные излучения

38 Какой тип технических каналов утечки образуется за счет просачивания информационных сигналов в цепи заземления и электропитания ОТСС?
   1. электромагнитные
   2. параметрические
   3. электрические

Критерии оценки:

2 балла по шкале БРС выставляется обучающемуся, если даны правильные ответы на 2 вопроса из 2;

1 балл по шкале БРС выставляется обучающемуся, если дан правильный ответ на 1 вопрос из 2;

0 баллов по шкале БРС выставляется обучающемуся, если дан правильный ответы на 0 вопросов из 2.

1.3 КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРАКТИЧЕСКИМ РАБОТАМ

Контрольные вопросы для защиты практической работы №1.

1 Какой состав и организационная структура системы обеспечения информационной безопасности?

2 В чем заключается стандарт ISO 17799?

3 Опишите методику анализа рисков.

4 Перечислите основные обязанности администратора безопасности

5 Какие программные и аппаратные средства позволяют идентифицировать и оценивать возможные риски в сети?

6 Проанализируйте как GFI LANguard защищает против червей.

7 При каких обстоятельствах GFI LANguard вывод диалог во время патча.

8 Вы можете изменить сообщение, выведенное на экран, когда GFI LANguard выполняет административные задачи? Если да, то как?

Контрольные вопросы для защиты практической работы №2.

1. Основы алгоритма шифрования AES?
2. Что такое раунд шифрования?
3. Что такое ключ шифрования? Как он используется?
4. В чем заключается атака «Квадрат»?
5. Что такое положение ECB?
6. 6 Как изменяется работа шифрования в зависимости от
7. режима шифрования?
8. Что из себя представляет полиалфавитное шифрование?
9. Чьи труды были взяты за основу Шифра Виженера?
10. Опишите процесс шифрования
11. Опишите процесс дешифрования
12. В данный момент, шифр уязвим к криптоанализу?
13. Какой вклад внёс Гилберт Вернам по отношению к шифру?

Контрольные вопросы для защиты практической работы №3.

1. Дайте определение шифрованию?
2. Для чего применяется программа PGP?
3. Перечислите основные функции программы?
4. Что такое RSA?
5. Что такое открытые ключи? В каком случае их используют?
6. Как проверяется достоверность источника?
7. Что такое скремблирование?
8. Каким требованиям должен удовлетворять двоичный сигнал для синхронной передачи?
9. Назовите один из способов обработки двоичных посылок

10.В каких видах систем применяется скремблирование?
11.Перечислите основные типы скремблеров и дескремблеров

Контрольные вопросы для защиты практической работы №4.

1. Что представляет собой алгоритм RSA?
2. Почему шифр RSA называется ассиметричным?
3. По какой формуле производится шифрование
4. По какой формуле производится дешифрование
5. В чем заключается криптостойкость алгоритма?
6. Что из себя представляют открытый и закрытый ключ?

Контрольные вопросы для защиты практической работы №5.

1. Что такое клеточный автомат?
2. В каких сферах деятельности принимаются клеточные автоматы?
3. Какое отношение имеют клеточные автоматы к информационной безопасности?
4. Кем была разработана игра «Жизнь»?
5. Какие алгоритмы применяются в функциях?

Контрольные вопросы для защиты практической работы №6.

1. Что в себя включает понятие защита программного обеспечения?
2. Какими инструментами пользуются злоумышленники для исследования программ?
3. Что такое отладчик?
4. Что такое дизассемблер?
5. Для чего используют шифрование исполняемого файла?
6. Какие методы используются для обнаружения модифицированного кода?

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.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1. К правовым методам, обеспечивающим информационную безопасность, относятся:
   a. Разработка аппаратных средств обеспечения правовых данных
   b. Разработка и установка во всех компьютерных правовых сетях журналов учета действий
   c. Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2. Основными источниками угроз информационной безопасности являются все указанное в списке:
   a. Хищение жестких дисков, подключение к сети, инсайдерство
   b. Перехват данных, хищение данных, изменение архитектуры системы
   c. Хищение данных, подкуп системных администраторов, нарушение регламента работы

3. Виды информационной безопасности:
   a. Персональная, корпоративная, государственная
   b. Клиентская, серверная, сетевая
   c. Локальная, глобальная, смешанная

4. Цели информационной безопасности – своевременное обнаружение, предупреждение:
   a. несанкционированного доступа, воздействия в сети
   b. инсайдерства в организации
   c. чрезвычайных ситуаций

5. Основные объекты информационной безопасности:
   a. Компьютерные сети, базы данных
   b. Информационные системы, психологическое состояние пользователей
   c. Бизнес-ориентированные, коммерческие системы

6. Основными рисками информационной безопасности являются:
   a. Искажение, уменьшение объема, перекодировка информации

b. Техническое вмешательство, выведение из строя оборудования сети
c. Потеря, искажение, утечка информации

7. К основным принципам обеспечения информационной безопасности относится:
a. Экономической эффективности системы безопасности
b. Многоплатформенной реализации системы
c. Усиления защищенности всех звеньев системы

8. Основными субъектами информационной безопасности являются:
a. руководители, менеджеры, администраторы компаний
b. органы права, государства, бизнеса
c. сетевые базы данных, фаерволлы

9. К основным функциям системы безопасности можно отнести все перечисленное:
a. Установление регламента, аудит системы, выявление рисков
b. Установка новых офисных приложений, смена хостинг-компании
c. Внедрение аутентификации, проверки контактных данных пользователей

10. Принципом информационной безопасности является принцип недопущения:
a. Неоправданных ограничений при работе в сети (системе)
b. Рисков безопасности сети, системы
c. Презумпции секретности

11. Принципом политики информационной безопасности является принцип:
a. Невозможности миновать защитные средства сети (системы)
b. Усиления основного звена сети, системы
c. Полного блокирования доступа при риск-ситуациях

12. Принципом политики информационной безопасности является принцип:
a. Усиления защищенности самого незащищенного звена сети (системы)
b. Перехода в безопасное состояние работы сети, системы
c. Полного доступа пользователей ко всем ресурсам сети, системы

13. Принципом политики информационной безопасности является принцип:
a. Разделения доступа (обязанностей, привилегий) клиентам сети (системы)

b. Одноуровневой защиты сети, системы
c. Совместимых, однотипных программно-технических средств сети, системы

14. К основным типам средств воздействия на компьютерную сеть относится:
a. Компьютерный сбой
b. Логические закладки («мины»)
c. Аварийное отключение питания

15. Когда получен спам по e-mail с приложенным файлом, следует:
a. Прочитать приложение, если оно не содержит ничего ценного – удалить
b. Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
c. Удалить письмо с приложением, не раскрывая (не читая) его

16. Принцип Кирхгофа:
a. Секретность ключа определена секретностью открытого сообщения
b. Секретность информации определена скоростью передачи данных
c. Секретность закрытого сообщения определяется секретностью ключа

17. ЭЦП – это:
a. Электронно-цифровой преобразователь
b. Электронно-цифровая подпись
c. Электронно-цифровой процессор

18. Наиболее распространены угрозы информационной безопасности корпоративной системы:
a. Покупка нелицензионного ПО
b. Ошибки эксплуатации и неумышленного изменения режима работы системы
c. Сознательного внедрения сетевых вирусов

19. Наиболее распространены угрозы информационной безопасности сети:
a. Распределенный доступ клиент, отказ оборудования
b. Моральный износ сети, инсайдерство
c. Сбой (отказ) оборудования, нелегальное копирование данных

20. Наиболее распространены средства воздействия на сеть офиса:
a. Слабый трафик, информационный обман, вирусы в интернет
b. Вирусы в сети, логические мины (закладки), информационный перехват

c. Компьютерные сбои, изменение администрирования, топологии

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

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

23. Угроза информационной системе (компьютерной сети) – это:
   a. Вероятное событие
   b. Детерминированное (всегда определенное) событие
   c. Событие, происходящее периодически

24. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
   a. Регламентированной
   b. Правовой
   c. Защищаемой

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

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

27. Политика безопасности в системе (сети) – это комплекс:
   a. Руководств, требований обеспечения необходимого уровня безопасности
   b. Инструкций, алгоритмов поведения пользователя в сети
   c. Нормы информационного права, соблюдаемые в сети

28. Наиболее важным при реализации защитных мер политики безопасности является:
   a. Аудит, анализ затрат на проведение защитных мер

b. Аудит, анализ безопасности
c. Аудит, анализ уязвимостей, риск-ситуаций

29. Под информационной безопасностью понимается…
a. защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.
b. программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
c. нет правильного ответа

30. Защита информации – это..
a. комплекс мероприятий, направленных на обеспечение информационной безопасности.
b. процесс разработки структуры базы данных в соответствии с требованиями пользователей
c. небольшая программа для выполнения определенной задачи

31. От чего зависит информационная безопасность?
a. от компьютеров
b. от поддерживающей инфраструктуры
c. от информации

32. Основные составляющие информационной безопасности:
a. Целостность
b. Достоверность
c. Конфиденциальность

33. Доступность – это…
a. возможность за приемлемое время получить требуемую информационную услугу.
b. логическая независимость
c. нет правильного ответа

34. Целостность – это..
a. целостность информации
b. непротиворечивость информации
c. защищенность от разрушения
35. Конфиденциальность – это..
a. защита от несанкционированного доступа к информации

b. программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
c. описание процедур

36. Для чего создаются информационные системы?
a. получения определенных информационных услуг
b. обработки информации
c. все ответы правильные

37. Целостность можно подразделить:
a. Статическую
b. Динамичную
c. структурную

38. Где применяются средства контроля динамической целостности?
a. анализе потока финансовых сообщений
b. обработке данных
c. при выявлении кражи, дублирования отдельных сообщений

39. Какие трудности возникают в информационных системах при конфиденциальности?
a. сведения о технических каналах утечки информации являются закрытыми
b. на пути пользовательской криптографии стоят многочисленные технические проблемы
c. все ответы правильные

40. Угроза – это…
a. потенциальная возможность определенным образом нарушить информационную безопасность
b. система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
c. процесс определения отвечает на текущее состояние разработки требованиям данного этапа

41. Атака – это…
a. попытка реализации угрозы
b. потенциальная возможность определенным образом нарушить информационную безопасность
c. программы, предназначенные для поиска необходимых программ.

42. Источник угрозы – это..
a. потенциальный злоумышленник
b. злоумышленник
c. нет правильного ответа

43. Окно опасности – это…
a. промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.

b. комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
c. формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

44. Какие события должны произойти за время существования окна опасности?
a. должно стать известно о средствах использования пробелов в защите.
b. должны быть выпущены соответствующие заплаты.
c. заплаты должны быть установлены в защищаемой И.С.

45. Угрозы можно классифицировать по нескольким критериям:
a. по спектру И.Б.
b. по способу осуществления
c. по компонентам И.С.

46. По каким компонентам классифицируется угрозы доступности:
a. отказ пользователей
b. отказ поддерживающей инфраструктуры
c. ошибка в программе

47. Основными источниками внутренних отказов являются:
a. отступление от установленных правил эксплуатации
b. разрушение данных
c. все ответы правильные

48. Основными источниками внутренних отказов являются:
a. ошибки при конфигурировании системы
b. отказы программного или аппаратного обеспечения
c. выход системы из штатного режима эксплуатации

49. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:
a. невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности
b. обрабатывать большой объем программной информации
c. нет правильного ответа

50. Какие существуют грани вредоносного П.О.?
a. вредоносная функция
b. внешнее представление
c. способ распространения

51. По механизму распространения П.О. различают:
a. Вирусы
b. Черви
c. все ответы правильные

52. Вирус – это…
a. код обладающий способностью к распространению путем внедрения в другие программы

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

53. Черви – это…
a. код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения
b. код обладающий способностью к распространению путем внедрения в другие программы
c. программа действий над объектом или его свойствами

54. Конфиденциальную информацию можно разделить:
a. Предметную
b. Служебную
c. глобальную

55. Природа происхождения угроз:
a. Случайные
b. Преднамеренные
c. природные

56. Предпосылки появления угроз:
a. Объективные
b. Субъективные
c. преднамеренные

57. К какому виду угроз относится присвоение чужого права?
a. нарушение права собственности
b. нарушение содержания
c. внешняя среда

58. Отказ, ошибки, сбой – это:
a. случайные угрозы
b. преднамеренные угрозы
c. природные угрозы

59. Отказ - это…
a. нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
b. некоторая последовательность действий, необходимых для выполнения конкретного задания
c. структура, определяющая последовательность выполнения и взаимосвязи процессов

60. Ошибка – это…
a. неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния
b. нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
c. негативное воздействие на программу

61. Сбой – это…

a. такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
b. неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния
c. объект-метод

62. Побочное влияние – это…
a. негативное воздействие на систему в целом или отдельные элементы
b. нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
c. нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

63. СЗИ (система защиты информации) делится:
a. ресурсы автоматизированных систем
b. организационно-правовое обеспечение
c. человеческий компонент

64. Что относится к человеческому компоненту СЗИ?
a. системные порты
b. администрация
c. программное обеспечение

65. Что относится к ресурсам А.С. СЗИ?
a. лингвистическое обеспечение
b. техническое обеспечение
c. все ответы правильные

66. По уровню обеспеченной защиты все системы делят:
a. сильной защиты
b. особой защиты
c. слабой защиты

67. По активности реагирования СЗИ системы делят:
a. Пассивные
b. Активные
c. полупассивные

68. Правовое обеспечение безопасности информации – это…
a. совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации
b. система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
c. нет правильного ответа

69. Правовое обеспечение безопасности информации делится:
a. международно-правовые нормы
b. национально-правовые нормы

c. все ответы правильные

70. Информацию с ограниченным доступом делят:
   a. государственную тайну
   b. конфиденциальную информацию
   c. достоверную информацию

71. Что относится к государственной тайне?
   a. сведения, защищаемые государством в области военной, экономической … деятельности
   b. документированная информация
   c. нет правильного ответа

72. Вредоносная программа - это…
   a. программа, специально разработанная для нарушения нормального функционирования систем
   b. упорядочение абстракций, расположение их по уровням
   c. процесс разделения элементов абстракции, которые образуют ее структуру и поведение

73. Основополагающие документы для обеспечения безопасности внутри организации:
   a. трудовой договор сотрудников
   b. должностные обязанности руководителей
   c. коллективный договор

74. К организационно - административному обеспечению информации относится:
   a. взаимоотношения исполнителей
   b. подбор персонала
   c. регламентация производственной деятельности

75. Что относится к организационным мероприятиям:
   a. хранение документов
   b. проведение тестирования средств защиты информации
   c. пропускной режим

76. Какие средства используется на инженерных и технических мероприятиях в защите информации:
   a. Аппаратные
   b. Криптографические
   c. физические

77. Программные средства – это…
   a. специальные программы и системы защиты информации в информационных системах различного назначения
   b. структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла
   c. модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

78. Криптографические средства – это…

a. средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования
b. специальные программы и системы защиты информации в информационных системах различного назначения
c. механизм, позволяющий получить новый класс на основе существующего

79. По отношению к защищаемой информации существуют следующие угрозы:
a. несанкционированный доступ
b. утечка
c. сокрытие
d. разглашение

80. Клавиатурные шпионы применяются злоумышленником для ...
a. Отслеживания журнала посещения
b. Определения прав доступа пользователей ОС
c. Перехвата паролей пользователей операционной системы
d. Определения количества пользователей

81. Защита информации - это ...
a. совокупность информационных систем, взаимодействующих между собой, причем одна часть этих систем может иметь интересы, прямо противоположные интересам другой
b. состояние информации, при котором изменять её могут только уполномоченные лица
c. комплекс мероприятий по обеспечению конфиденциальности, целостности, доступности, учета и неотрекаемости информации
d. данные, представленные в виде, пригодном для хранения, обработки и передачи, и представляющие определенную ценность

82. Для любой информационной системы характерны следующие понятия:
a. непредвиденное обстоятельство
b. происшествие
c. злоумышленник
d. уязвимость
e. угроза

83. В зависимости от способов перехвата информации, от физической природы сигналов и среды их распространения технические каналы утечки информации можно разделить на:
a. внешние
b. параметрические
c. электрические
d. дистанционные
e. электромагнитные

84. Что означает слово "конфиденциальный" в переводе с латинского?

a. безопасность
b. доверие
c. хранение
d. защита
e. По источникам появления угрозы подразделяют на:
f. внешние и внутренние
g. естественные и искусственные
h. пользовательские и сетевые

85. Процесс сообщения субъектом своего имени или номера, с целью получения определённых полномочий (прав доступа) на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом:

a. Авторизация
b. Аутентификация
c. Обезличивание
d. Деперсонализация
e. Идентификация

86. Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации:

a. Авторизация
b. Обезличивание
c. Деперсонализация
d. Аутентифика́ция
e. Идентификация

87. Процесс, а также результат процесса проверки некоторых обязательных параметров пользователя и, при успешности, предоставление ему определённых полномочий на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом

a. Авториза́ция
b. Идентификация
c. Аутентификация
d. Обезличивание
e. Деперсонализация

88. Простейшим способом идентификации в компьютерной системе является ввод идентификатора пользователя, который имеет следующее название:

a. Токен
b. Password
c. Пароль
d. Login
e. Смарт-карта

89. Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе – по сети интернет:

a. Идентификация
b. Аутентификация

c. Авторизация
d. Экспертиза
e. Шифрование

90. Для безопасной передачи данных по каналам интернет используется технология:

a. Www
b. Dicom
c. Vpn
d. Ftp
e. Xml

91. Комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами и защищающий компьютерные сети от несанкционированного доступа:

a. Антивирус
b. Замок
c. Брандма́уэр
d. Криптография
e. Экспертная система

92. За правонарушения в сфере информации, информационных технологий и защиты информации данный вид наказания на сегодняшний день не предусмотрен:

a. Дисциплинарные взыскания
b. Административный штраф
c. Уголовная ответственность
d. Лишение свободы
e. Смертная казнь

93. Несанкционированный доступ к информации это:

a. Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально
b. Работа на чужом компьютере без разрешения его владельца
c. Вход на компьютер с использованием данных другого пользователя
d. Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей
e. Доступ к субд под запрещенным именем пользователя

94. «Персональные данные» это:

a. Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу
b. Фамилия, имя, отчество физического лица
c. Год, месяц, дата и место рождения, адрес физического лица
d. Адрес проживания физического лица
e. Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна»

95. В данном случае сотрудник учреждения может быть привлечен к ответственности за нарушения правил информационной безопасности:

a. Выход в интернет без разрешения администратора
b. При установке компьютерных игр
c. В случаях установки нелицензионного по
d. В случае не выхода из информационной системы
e. В любом случае неправомочного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности

96. Может ли сотрудник быть привлечен к уголовной ответственности за нарушения правил информационной безопасности предприятия:

a. Нет, только к административной ответственности
b. Нет, если это государственное предприятие
c. Да
d. Да, но только в случае, если действия сотрудника нанесли непоправимый вред
e. Да, но только в случае осознанных неправомочных действий сотрудника

97. Процедура, проверяющая, имеет ли пользователь с предъявленным идентификатором право на доступ к ресурсу это:

a. Идентификация
b. Аутентификация
c. Стратификация
d. Регистрация
e. Авторизация

98. Наиболее опасным источником угроз информационной безопасности предприятия являются:

a. Другие предприятия (конкуренты)
b. Сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам
c. Рядовые сотрудники предприятия
d. Возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных
e. Хакеры

99. Выберите, можно ли в служебных целях использовать электронный адрес (почтовый ящик), зарегистрированный на общедоступном почтовом сервере, например на mail.ru:

a. Нет, не при каких обстоятельствах
b. Нет, но для отправки срочных и особо важных писем можно

c. Можно, если по нему пользователь будет пересылать информацию, не содержащую сведений конфиденциального характера
d. Можно, если информацию предварительно заархивировать с помощью программы winrar с паролем
e. Можно, если других способов электронной передачи данных на предприятии или у пользователя в настоящий момент нет, а информацию нужно переслать срочно

100. Документированная информация, доступ к которой ограничивает в соответствии с законодательством РФ:

a. Информация составляющая государственную тайну
b. Информация составляющая коммерческую тайну
c. Персональная
d. Конфиденциальная информация
e. Документированная информация

Задания в открытой форме

1. … – это сфера деятельности, связанная с созданием, распространением, преобразованием и потреблением информации. Назовите субъекты информационных отношений.
2. … информации заключается в ее существовании в неискаженном виде, не измененном по отношению к некоторому ее исходному состоянию.
3. ... свойство, характеризующее способность обеспечивать своевременный и беспрепятственный доступ пользователей к интересующим их данным.
4. … свойство, указывающее на необходимость введения ограничений на доступ к ней определенного круга пользователей.
5. Основные 7 принципов обеспечения информационной безопасности: …
6. Защита … – не разовое мероприятие, а непрерывный целенаправленный процесс, предполагаемый принятие соответствующих мер на всех этапах жизненного цикла защиты системы.
7. Важно правильно выбрать тот уровень защиты, при котором затраты, риск взлома и размер возможного ущерба были бы приемлемыми – это принцип …
8. на этапе разработки системы защиты в нее должна закладываться некая избыточность, которая позволила бы увеличить срок ее жизнеспособности – описывается принцип …
9. Определяются законодательными актами страны, которыми регламентируется правила использования, обработки и передачи

информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил. Это … меры защиты информации.

10. Нормы поведения, которые традиционно сложились по мере распространения сетевых и информационных технологий. Это … меры защиты информации.
11. Представляют собой мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры телекоммуникаций для обеспечения защиты информации. Это … меры защиты информации.
12. Реализуются в виде механических, электрических и электронных устройств, предназначенных для препятствования проникновению и доступу потенциального нарушителя к компонентам защиты. Это … меры защиты информации.
13. Представляют из себя программное обеспечение, предназначенное для выполнения функций защиты информации. Это … меры защиты информации.
14. … - это отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации.
15. … - это отношения, возникающие при создании и использовании информационных технологий и средств их обеспечения
16. … - это отношения, возникающие при защите информации и прав субъектов, участвующих в информационных процессах и информатизации
17. … - это отношения, возникающие
18. Документированная информация представляет собой обыкновенные данные, а подход, отождествляющий информацию и данные, носит название «...».
19. К сведениям … следует относить такие сведения, распространение которых может нанести ущерб интересам РФ в одной или нескольких областях деятельности.
20. К … сведениям следует относить такие сведения, распространение которых может нанести ущерб интересам министерства, ведомства или отраслям экономики РФ в одной или нескольких областях деятельности.
21. Понятие … тесно связано с понятием защиты информации и является реализацией системы защиты информации для конкретного объекта или одного из его структурных подразделений или конкретной работы.

Задание на установление правильной последовательности

1. Выберите правильную последовательность этапов по созданию системы защиты персональных данных:
    1. Опытная и промышленная эксплуатация
    2. Проектный этап
    3. Аттестация или декларирование
    4. Предпроектный этап

2. Выберите правильную последовательность этапов в жизненном цикле атаки:
    1. Выбор способа атаки
    2. Закрепление
    3. Эксплуатация
    4. Достижение цели
    5. Исполнение команд
    6. Разведка и сбор данных
    7. Доставка

3. Выберите правильную последовательность этапов разработки профиля защиты.
    1. Анализ среды применения ИТ-продукта с точки зрения
    2. безопасности.
    3. Выбор профиля-прототипа.
    4. Синтез требований.

4. Выберите правильную последовательность этапов защиты информации, информационных технологий и автоматизированных систем от атак:
    1. Анализ рисков для активов организации, включающий в себя выявление ценных активов и оценку возможных последствий реализации атак с использованием скрытых каналов
    2. Реализация защитных мер по противодействию скрытых каналов
    3. Организация контроля за противодействием скрытых каналов.
    4. Выявление скрытых каналов и оценка их опасности для активов организации

5. Выберите правильную последовательность этапов работы по обеспечению режима ИБ:
    1. Выявление максимально полного множества потенциальных угроз, способов и каналов их осуществления;
    2. Определение и выработка политики информационной безопасности;

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

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

6. Установите последовательность этапов работы по обеспечению информационной безопасности:

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

7. Выберите правильную последовательность этапов процесса управления рисками:

1. идентификация активов и ценности ресурсов, нуждающихся в защите;
2. анализ угроз и их последствий, определение слабостей в защите;
3. классификация рисков, выбор методологии оценки рисков и проведение оценки;
4. выбор, реализация и проверка защитных мер;
5. оценка остаточного риска;
6. выбор анализируемых объектов и степени детальности их рассмотрения;

8. Выберите правильную последовательность этапов обеспечения информационной:

1. оценка стоимости;
2. реализация политики;
3. квалифицированная подготовка специалистов;
4. аудит;
5. разработка политики безопасности;

9. Выберите правильную последовательность этапов развития информационной безопасности до первой половину 20-го века:

1. Характеризуется использованием естественно возникавших средств информационных коммуникаций. В этот период основная задача информационной безопасности заключалась в защите сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих для человека лично или сообщества, к которому он принадлежал, жизненное значение.
2. Связан с началом использования искусственно создаваемых технических средств электро- и радиосвязи. Для обеспечения скрытности и

помехозащищенности радиосвязи необходимо было использовать опыт первого периода информационной безопасности на более высоком технологическом уровне, а именно применение помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала).

3. Связан с появлением радиолокационных и гидроакустических средств. Основным способом обеспечения информационной безопасности в этот период было сочетание организационных и технических мер, направленных на повышение защищенности радиолокационных средств от воздействия на их приемные устройства активными маскирующими и пассивными имитирующими радиоэлектронными помехами.

4. Связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров). Задачи информационной безопасности решались, в основном, методами и способами ограничения физического доступа к оборудованию средств добывания, переработки и передачи информации.

10. Выберите правильную последовательность этапов развития информационной безопасности после первой половины 20-го века:

1. Обусловлен созданием и развитием локальных информационно-коммуникационных сетей. Задачи информационной безопасности также решались, в основном, методами и способами физической защиты средств добывания, переработки и передачи информации, объединённых в локальную сеть путём администрирования и управления доступом к сетевым ресурсам.

2. Связан с использованием сверхмобильных коммуникационных устройств с широким спектром задач. Угрозы информационной безопасности стали гораздо серьёзнее. Образовались сообщества людей — хакеров, ставящих своей целью нанесение ущерба информационной безопасности отдельных пользователей, организаций и целых стран. Информационный ресурс стал важнейшим ресурсом государства, а обеспечение его безопасности — важнейшей и обязательной составляющей национальной безопасности. Формируется информационное право — новая отрасль международной правовой системы.

3. Связан с созданием и развитием глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения. Можно предположить что очередной этап развития информационной безопасности, будет связан с широким использованием сверхмобильных коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве и времени, обеспечиваемым космическими информационно-коммуникационными системами. Для решения задач информационной безопасности на этом этапе необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов.

11. Выберите последовательность уровней защищенности персональных данных

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

12. Выберите последовательность уровней безопасности информации:

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

13. Выберите последовательность проведения моделирования угроз:

1. Определение негативных последствий от угроз безопасности информации.
2. Определение объектов воздействия угроз безопасности информации.
3. Оценка возможности реализации угроз и их актуальности.

14. Выберите правильную последовательность этапов оценки угроз безопасности информации:

1. Определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;
2. Инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;
3. Определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;
4. Оценка способов реализации (возникновения) угроз безопасности информации;
5. Оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;
6. Оценка сценариев реализации угроз безопасности информации в системах и сетях.

15. Выберите правильную последовательность этапов построения политики безопасности:

1. Выбор и установка средств защиты;
2. Организация обслуживания по вопросам информационной безопасности;
3. Создание системы периодического контроля информационной безопасности

4. Обследование информационной системы на предмет установления организационной и информационной структуры и угроз безопасности информации;
5. Подготовка персонала работе со средствами защиты;

16. Выберите правильную последовательность этапов жизненного цикла информационного сервиса:
1. Сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию.
2. На данном этапе выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение.
3. На данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно закупка.
4. На данном этапе сервис не только работает и администрируется, но и подвергается модификациям.

17. Установите этапы существования оборудования ИБ:
1. Установка.
2. Эксплуатация.
3. Выведение из эксплуатации.
4. Инициация.
5. Закупка.

18. Выберите правильную последовательность этапов построения системы защиты:
1. Анализ
2. Реализация системы защиты
3. Сопровождение системы защиты.
4. Разработка системы защиты

19. Выберите последовательность приоритетных этапов защиты информации:
1. Защита информации от несанкционированного доступа;
2. Защита информации в системах связи;
3. Защита юридической значимости электронных документов;
4. Защита конфиденциальной информации от утечки по каналам побочных электромагнитных излучений и наводок;
5. Защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ;
6. Защита от несанкционированного копирования и распространения программ и ценной компьютерной информации.

20. Устранение уязвимости состоит из следующих этапов:
1. Инсталляция программного модуля для устранения угрозы информационной безопасности.

2. Разработка «патча» (заплатки), призванного устранить существующий пробел.

3. Появление сигнала от пользователей или от администратора сети о наличии слабого места в информационной системе.

Задание на установление соответствия

1. Установить соответствие

1) Целостность	a) заключается в ее существовании в неискаженном виде, не измененном по отношению к некоторому ее исходному состоянию.
2) Доступность	b) свойство, указывающее на необходимость введения ограничений на доступ к ней определенного круга пользователей.
3) Конфиденциальность	c) свойство, характеризующее способность обеспечивать своевременный и беспрепятственный доступ пользователей к интересующим их данным.

2. Установить соответствие

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

3. Установить соответствие

1) Принцип разумной достаточности	a) защита не должна обеспечиваться только за счет секретности структурной безопасности и алгоритмов функционирования ее подсистемы.

2) Принцип разумной избыточности	b) Должны быть реализованы принципы гибкости управления, обеспечивающие возможность настройки механизмов в процессе функционирования системы.
3) Принцип гибкости управления и применения	c) на этапе разработки системы защиты в нее должна закладываться некий потенциал, который позволил бы увеличить срок ее жизнеспособности.
4) Открытость алгоритмов и механизмов защиты	d) Необходимо правильно выбрать тот уровень защиты, при котором затраты, риск взлома и размер возможного ущерба были бы приемлемыми.

4. Установить соответствие

1) Первый фактор	a) прочность существующего механизма защиты, характеризующаяся степенью сопротивляемости этих механизмов попыткам их обхода или преодоления.
2) Второй фактор	b) величина ущерба, наносимого владельцу АСОД в случае успешного осуществления угроз безопасности
3) Третий фактор	c) каждый путь осуществления угрозы должен быть перекрыт соответствующим механизмом защиты

5. Установить соответствие мер защиты информации:

1) Правовые	a) Реализуются в виде механических, электрических и электронных устройств, предназначенных для препятствования проникновению и доступу потенциального нарушителя к компонентам защиты.
2) Морально-этические	b) Представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры телекоммуникаций для обеспечения защиты информации
3) Административные	c) К ним относятся нормы поведения, которые традиционно сложились по мере распространения сетевых и информационных технологий.
4) Технические	d) Определяются законодательными актами страны, которыми регламентируется правила

	использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

6. Установить соответствие мер защиты информации:

1) К сведениям особой важности следует относить	a) Все иные из числа сведений, составляющих государственную тайну.
2) К совершенно секретным сведениям следует относить	b) Такие сведения, распространение которых может нанести ущерб интересам министерства, ведомства или отраслям экономики РФ в одной или нескольких областях деятельности.
3) К секретным сведениям следует относить	c) Такие сведения, распространение которых может нанести ущерб интересам РФ в одной или нескольких областях деятельности.

7. Установить соответствие

1) Коммерческая тайна	a) Служебные сведения, которые не относятся к государственной тайне, доступ к которым ограничен органами государственной власти и федеральными органами исполнительной власти в соответствии с законодательством.
2) Служебная тайна	b) Режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду
3) Профессиональная тайна	c) Информация, полученная гражданами при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности.

8. Установить соответствие

1) Основные организационные	a) Мероприятия по обеспечению достаточного уровня физической защиты

и организационно-технические мероприятия по созданию и поддержанию функционирования системы защиты включают:	всех компонентов АСОД (противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности средств вычислительной техники, носителей информации и т.п.).
2) Разовые мероприятия включают:	b) Распределение реквизитов разграничения доступа (пароли, ключи шифрования и т.д.).
3) Периодически проводимые мероприятия включают:	c) Общесистемные мероприятия по созданию научно-технических и методологических основ защиты АСОД.
4) Постоянно проводимые мероприятия включают:	d) Общесистемные мероприятия по созданию научно-технических и методологических основ защиты АСОД.

9. Установить соответствие

1) Общедоступные персональные данные	a) Это персональные данные, касающиеся расовой или национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья.
2) Специальные категории персональных данных	b) Это персональные данные, доступ к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.
3) Биометрические персональные данные	c) Это сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность.

10. Установить соответствие

1) Основные организационные и организационно-	a) Мероприятия по непрерывной поддержке функционирования и управления используемыми средствами защиты.

технические мероприятия по созданию и поддержанию функционирования системы защиты включают:	
2) Разовые мероприятия включают:	b) Анализ системных журналов и принятие мер по обнаруженным нарушениям правил работы.
3) Периодически проводимые мероприятия включают:	c) Мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов АСОД.
4) Постоянно проводимые мероприятия включают:	d) Мероприятия, проводимые при осуществлении или возникновении определенных изменений в самой защищаемой АСОД или внешней среде (мероприятия, проводимые по необходимости).

11. Установить соответствие технических каналов утечки информации:

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

12. Установить соответствие технических каналов утечки информации:

1) Прямой акустический (окна, двери, щели, проемы)	a) Электронные устройства перехвата речевой информации с датчиками контактного типа, установленными на инженерно-технических коммуникациях
2) Акусто-вибрационный (через ограждающие кострукции)	b) Специализированные высокочувствительные микрофоны, установленные в воздуховодах или смежных помещениях
3) Акусто-электрический (через соединительные линии ВТСС)	c) Аппаратура высокочастотного облучения, установленная за пределами КЗ
4) Акусто-электромагнитный (параметрический)	d) Аппаратура «высокочастотного навязывания», подключенная к соединительным линиям ВТСС

13. Установить соответствие технических каналов утечки информации:

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

14. Установить соответствие дальности подавления диктофонов:

1) Аналоговые диктофоны	a) 5–6 м.
2) Цифровые диктофоны	b) Не более 1,5 м

3) Аналоговые диктофоны в металлическом корпусе	c) 4–5 м
4) Современные цифровые диктофоны в металлическом корпусе	d) Практически не подавляются

15. Установить соответствие

1) I группа	a) Блокираторы представляют собой генераторы помех с ручным управлением, обеспечивающие подстановку заградительной помехи в диапазоне частот работы базовых станций соответствующего стандарта (т.е. в диапазоне рабочих частот приемников телефонов сотовой связи). Помеха приводит к срыву управления сотовым телефоном базовой станции (потеря сети) и следовательно невозможности установления связи и передачи информации.
2) II группа	b) В своем составе кроме передатчика помех имеют еще специальный приемник, обеспечивающий прием сигналов в диапазонах частот работы передатчиков телефонных аппаратов соответствующего стандарта. Учитывая, что вся система сотовой связи работает в дуплексном режиме, специальный приемник используется как средство автоматического управления передатчиком помех. При обнаружении сигнала в одном из диапазонов частот приемник выдает сигнал управления на включения передатчика заградительных помех соответствующего диапазона частот. При пропадании сигнала приемник выдает сигнал управления на выключение сигнала помех соответствующего диапазона.
3) III группа	c) Так называемые «интеллектуальные блокираторы связи». На примере GSM: приемник блокиратора в течение короткого

	времени (примерно 300 мкс) обнаруживает в КЗ излучение входящего в связь мобильного телефона, вычисляет номер частотного канала и временной слот, выделяемый данному телефону.

16. Установить соответствие:

1) Косвенные каналы	a) связанные с доступом к элементам АСОД, но не требующие изменения компонентов системы.
2) Прямые каналы	b) не связанные с физическим доступом к элементам АСОД.
3) Прямые каналы	c) связанные с доступом к элементам АСОД и изменением структуры компонентов АСОД.

17. Установить соответствие:

1) Нарушитель	a) намеренно идущий на нарушение из корыстных побуждений.
2) Злоумышленник	b) лицо, предпринявшее попытку выполнения запрещенных действий по ошибке, незнанию или осознанно со злым умыслом или без такового, и использующее для этого различные возможности, методы и средства.
3) взломщик	c) Лицо, которое с корыстными целями осуществляет несанкционированный доступ к данным или программам.

18. Установить соответствие нарушителей по уровням знания АСОД:

1) 1 уровень	a) Обладает высоким уровнем знаний и опытом работы с техническими средствами системы и ее обслуживания.
2) 2 уровень	b) Знает функциональные особенности АСОД, основные закономерности формирования в нестандартных массивах данных и потоков запросов к ним. Умеет пользоваться штатными средствами.
3) 3 уровень	4) Знает структуру, функции и механизмы действия средств защиты, их слабые и сильные стороны.

5) 4 уровень	6) Обладает уровнем знаний в области программирования и вычислительных технологий, проектирования и эксплуатации АСОД.

19. Установить соответствие нарушителей по времени действия:

1) 3 уровень	a) В период неактивности компонентов системы (нерабочее время, перерывы, ремонт и т.п.).
2) 2 уровень	b) Во время функционирования АСОД (во время работы компонентов системы).
3) 1 уровень	c) Как в процессе функционирования АСОД, так и в период неактивности системы.

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

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

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

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

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

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

Соответствие 100-балльной и 5-балльной шкал

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

2.2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

1. Зашифровать строку «Стремитесь не к успеху, а к ценностям, которые он дает», используя шифрование с помощью таблицы Виженера
2. Зашифровать строку «Лучшая месть – огромный успех», используя шифр RSA
3. Зашифровать строку «Упади семь раз и восемь раз поднимись.», используя алгоритм шифрования Эль-Гамаля
4. Зашифровать строку «Я не жертва обстоятельств, я - результат моих решений.», используя алгоритм шифрования Деффи-Хеллмана
5. Зашифровать строку «Надо любить жизнь больше, чем смысл жизни», используя шифрование с помощью таблицы Виженера
6. Зашифровать строку «Лучшая месть – огромный успех», используя шифр RSA
7. Зашифровать строку «Если нет ветра, беритесь за вёсла.», используя алгоритм шифрования Эль-Гамаля
8. Зашифровать строку «Я не провалил тест. Я просто нашел сто способов написать его неправильно.», используя алгоритм шифрования Деффи-Хеллмана
9. Включите шифрование твердотельного накопителя используя операционную систему Windows 10
10. Воспользовавшись операционной системой Linux произведите сканирование локальной сети на поиск подозрительных устройств
11. Зашифровать строку «Научитесь говорить “Я не знаю”, и это уже будет прогресс.», используя шифр RSA
12. Зашифровать строку «Жизнь - это то, что с тобой происходит, пока ты строишь планы.», используя шифрование с помощью таблицы Виженера
13. Зашифровать строку «Мы становимся тем, о чем мы думаем.», используя алгоритм шифрования Эль-Гамаля

14. Опишите модель поведения нарушителя для административного корпуса завода ООО «СтройМаш»
15. Зашифровать строку «Стоит только поверить, что вы можете – и вы уже на полпути к цели.», используя шифр RSA
16. Зашифровать строку «Я не провалил тест. Я просто нашел сто способов написать его неправильно.», используя алгоритм шифрования Деффи-Хеллмана
17. Не имея непосредственного доступа к персональному компьютеру, совершите удаленный запуск приложений на нём
18. Зашифровать строку «Неудача – это просто возможность начать снова, но уже более мудро.» используя шифрование с помощью таблицы Виженера
19. Произведите установку антивирусного программного обеспечения на персональный компьютер
20. Зашифровать строку «Ты становишься тем, во что веришь.», используя алгоритм шифрования Деффи-Хеллмана

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.