МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование кафедры полностью)

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

«30» 08 2021 г.

ОЦЕНОЧНЫЕ СРЕДСТВА
для текущего контроля успеваемости
и промежуточной аттестации обучающихся
по дисциплине
Информационная безопасность
(наименование дисциплины)

45.03.03 Фундаментальная и прикладная лингвистика, направленность (профиль) «Теоретическая и прикладная лингвистика»
(код и наименование ОПОП ВО)

Курск – 2021

Задания для проведения текущего контроля успеваемости

Вопросы для устного опроса

Вопросы для устного опроса по теме 1

1. Основные понятия защиты информации и информационной безопасности.
2. Классификация угроз информационной безопасности автоматизированных систем.
3. Непосредственные виды угроз для автоматизированных систем: угроза нарушения конфиденциальности, угроза нарушения целостности информации, угроза нарушения работоспособности. Угроза раскрытия параметров автоматизированной системы.

Вопросы для устного опроса по теме 2

4. Назначение и структура стека протоколов TCP/IP. Характеристика протокола TCP/IP с точки зрения информационной безопасности.
5. Основные цели и характерные особенности сетевых атак. Виды сетевых атак: подслушивание (sniffing), подмена доверенного субъекта (IP – spoofing), посредничество в обмене незашифрованными ключами (Man-in-the-Middle).
6. Основные цели и характерные особенности сетевых атак. Виды сетевых атак: перехват сеанса (Session hijacking), отказ в обслуживании (Denial of Service, DoS), парольная атака полного перебора (brute force attack).
7. Основные цели и характерные особенности сетевых атак. Виды сетевых атак: угадывание ключа, атаки на уровне приложений, сетевая разведка, злоупотребление доверием.
8. Основные характеристики спама и методы борьбы с ним.
9. Виды интернет - мошенничества: фишинг и фарминг и методы борьбы с ними.
10. Угрозы и уязвимости проводных корпоративных сетей.

11. Особенности построения и актуальность защиты беспроводных сетей. Виды сетевых атак: вещание радиомаяка, обнаружение WLAN, подслушивание, ложные точки доступа в сеть.

12. Особенности построения и актуальность защиты беспроводных сетей. Виды сетевых атак: отказ в обслуживании, атаки типа “ человек в середине”, атака подмены ARP-записей, анонимный доступ в Интернет.

13. Способы обеспечения информационной безопасности компьютерных сетей. Фрагментарный и комплексный подходы.

14. Пути решения проблем защиты информации в сети Интернет. Информационная безопасность электронного бизнеса.

Вопросы для устного опроса по теме 3

15. Основные понятия политики безопасности. Верхний, средний и нижний уровни политики безопасности.

16. Структура политики безопасности организации. Базовая и специализированные политики безопасности. Процедуры безопасности.

17. Основные этапы разработки политики безопасности.

Вопросы для устного опроса по теме 4

18. Основные понятия криптологии: криптография, криптоанализ, алфавит, текст, зашифрование, расшифрование, блочное и поточное шифрование, криптографическая система, ключ, симметричные и ассиметричные криптосистемы.

19. Шифр простой замены. Частотный анализ, как основной метод криптоанализа шифра простой замены.

20. Функция хэширования. Электронная цифровая подпись.

21. Требования к криптографическим системам. Виды крипто-атак. Криптостойкость шифра.

22. Алгоритм шифрования RSA.

23. Американский стандарт шифрования AES

24. Обзор программных и программно-аппаратных средств криптографической защиты: пакет PGP, система криптографической защиты

информации “Верба - О”, программный комплекс “Inter –PRO”, программно-аппаратный комплекс “Доверенный удостоверяющий центр”.

Вопросы для устного опроса по теме 5

25. Аутентификация, авторизация и администрирование действий пользователей. Аутентификация на основе паролей.
26. Аутентификация на основе PIN-кода.
27. Строгая аутентификация. Примеры протоколов аутентификации.
28. Биометрическая аутентификация пользователя.
29. Электронные системы идентификации и аутентификации.
30. Комбинированные системы идентификации и аутентификации.

Вопросы для устного опроса по теме 6

31. Основные функции и дополнительные возможности межсетевых экранов. Политика работы МЭ.
32. Особенности функционирования межсетевых экранов на уровнях модели OSI. Варианты исполнения МЭ.
33. Основные схемы подключения межсетевых экранов.

Вопросы для устного опроса по теме 7

34. Понятие компьютерного вируса. Классификация вирусов.
35. Специализированные утилиты для борьбы с вредоносным ПО: антишпионы, антируткиты и антикейлоггеры.
36. Троянские программы. Виды троянских программ.
37. Компьютерные черви. Виды компьютерных червей.
38. Методы борьбы с вирусами: обнаружение, основанное на сигнатурах, обнаружение программ подозрительного поведения, метод “белого списка”.
39. Методы борьбы с вирусами: обнаружение вирусов при помощи эмуляции работы программы, эвристический анализ, метод резидентных мониторов.
40. Антивирусные программы: утилита Dr. Web Curelt, программа Dr. Web., антивирус Avira AntiVir Personal, антивирус Avast! Home Edition.

41. Популярные пакеты антивирусной защиты: пакеты компании ESET(ESET NOD32 Antivirus, ESET NOD32 Smart Security), пакеты “Лаборатории Касперского” (Антивирус Касперского, Kaspersky Internet Security, Kaspersky Mobile Security).

Вопросы для устного опроса по теме 8

42. Показатели защищенности средств вычислительной техники от несанкционированного доступа. Показатели защищенности межсетевых экранов.

43. Классы защищенности автоматизированных систем.

44. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных. Защита конфиденциальной информации в АС и на рабочих местах пользователей ПК.

45. Требования к защите информации в локальных вычислительных сетях и при межсетевом взаимодействии. Требования к защите информации при работе с системами управления базами данных.

46. Требования к защите информации при взаимодействии абонентов с сетями общего пользования.

Вопросы для собеседования по теме 9

47. Информационная безопасность как составная часть национальной безопасности РФ. Структура информационной безопасности РФ.

48. Основы информационного права. Информационные отношения.

49. Информация как объект права собственности. Виды защищаемой информации.

50. Государственная система правового обеспечения информационной безопасности.

51. Понятие “государственной тайны”. Основные принципы отнесения сведений, имеющих конфиденциальный характер к государственной тайне.

52. Содержание основных законов Российской Федерации в области информационной безопасности. Закон «О государственной тайне». Закон «Об

информации, информационных технологиях и о защите информации».

53. Правовые аспекты применения ЭЦП.

54. Правовые основы разработки и использования средств криптографической защиты информации.

55. Законодательство об авторском праве и смежных правах.

56. Законодательство о правовой охране программ для ЭВМ и баз данных.

57. Основы патентного права.

58. Система лицензирования деятельности организаций по оказанию услуг в области информационной безопасности.

59. Система сертификации средств защиты информации.

60. Аттестация объектов обработки конфиденциальной информации.

Критерии оценки:

- 0 баллов выставляется обучающемуся, если студент не может ответить на поставленные вопросы или допустил принципиальные ошибки в выполнении предусмотренных программой знаний;
- 1 балл выставляется обучающемуся, если доля правильных ответов от 50% до 90%;
- 2 балла выставляется обучающемуся, если доля правильных ответов более 90%.

Контрольные вопросы для защиты практических работ

Практическая работа №1. Разработка криптографической программы «Шифр Виженера»

1. Квадрат (таблица) Виженера
2. Алфавитный шифр
3. Количество символов в строке для русского алфавита

Практическая работа №2. Разработка криптографической программы «Алгоритм RSA»

1. Генерация ключей RSA
2. Теорема Эйлера
3. Малая теорема Ферма

Практическая работа №3. Менеджер паролей – программа Password Commander

1. Типы паролей, создаваемые с помощью генератора паролей
2. Пасскарта в программе Password Commander
3. Программы, предназначенные для хранения паролей
4. Аккаунт в программе Password Commander

Практическая работа №4. Настройка межсетевого экрана Comodo Firewall

1. Определение и свойства межсетевого экрана
2. Основные схемы подключения межсетевых экранов
3. Классификация межсетевых экранов
4. Типы межсетевых экрановмодели OSI

Практическая работа №5. Эксплуатация антивирусной программы Kaspersky Internet Security.

1. Классификация компьютерных вирусов
2. Отличие троянской программы от вируса
3. Классификация компьютерных червей
4. Метод обнаружения вирусов, основанного на сигнатурах
5. Метод обнаружения вирусов при помощи “белого списка”

Критерии оценки практических работ №1-2:

- 0 баллов выставляется обучающемуся, если студент не выполнил практическую работу.
- 2 балла выставляется обучающемуся, если студент выполнил практическую работу, доля правильных ответов от 50% до 90%.
- 4 балла выставляется обучающемуся, если студент выполнил практическую работу, доля правильных ответов более 90%.

Критерии оценки практических работ №3-5:

- 0 баллов выставляется обучающемуся, если студент не выполнил практическую работу.
- 3 балла выставляется обучающемуся, если студент выполнил практическую работу, доля правильных ответов от 50% до 90%.
- 6 балла выставляется обучающемуся, если студент выполнил практическую работу, доля правильных ответов более 90%.

Контрольные вопросы для защиты лабораторных работ

Лабораторная работа №1. Анализ и управление информационными рисками в программе “Гриф”

1. Назначение системы Гриф
2. Модуль управления системы Гриф
3. Виды защищённости информации на ресурсе
4. Алгоритм задания контрмер

Лабораторная работа №12 Разработка Web - приложений на языке HTML

1. Структура HTML документа
2. Уровни заголовков в спецификации HTML
3. Разметка абзацев в HTML
4. Вывод текста шрифтом Arial.

Лабораторная работа №3. Разработка и защита Web - приложений с клиентскими сценариями на языке JavaScript

1. Вывести значение всех элементов массива в языке JavaScript
2. Операторы языка JavaScript для реализации механизмов цикла
3. Для какой цели в языке JavaScript используется оператор return
4. Определение функции и ее общий вид в языке JavaScript

Лабораторная работа №4. Разработка и защита Web - приложений с серверными сценариями на языке PHP

1. Отличие php-страницы от html-страницы
2. Типы переменных, поддерживающих язык PHP
3. Параметры функции date()
4. Функция isset()

Критерии оценки:

- 0 баллов выставляется обучающемуся, если студент не выполнил лабораторную работу.

- 2 балла выставляется обучающемуся, если студент выполнил лабораторную работу, доля правильных ответов от 50% до 90%.
- 4 балла выставляется обучающемуся, если студент выполнил лабораторную работу, доля правильных ответов более 90%.

Типовые задания для проведения промежуточной аттестации обучающихся

Задания в закрытой форме

Задание №1

Какая угроза информационной безопасности является пассивной?

1. Копирование секретных данных.
2. Внедрение вредоносного программного обеспечения.
3. Кража носителей информации.
4. Удаление файла.

Задание №2

Угрозы нарушения целостности информации приводят к следующему результату:

1. Изменение, искажение или уничтожение информации.
2. Информация становится известной лицам, которые не должны иметь к ней доступ.
3. Снижается работоспособность автоматизированной системы, либо блокируется доступ к ее ресурсам.
4. Злоумышленнику становятся известны параметры автоматизированной системы.

Задание №3

К какому уровню доступа к информации в автоматизированной системе относится перехват данных, передаваемых по каналам связи?

1. Уровень средств взаимодействия с носителем.
2. Уровень носителей информации.
3. Уровень представления информации.
4. Уровень содержания информации.

Задание №4

Какая сетевая атака связана с превышением допустимых пределов функционирования сети?

1. Отказ в обслуживании (DoS –атака).
2. Подслушивание (Sniffing).
3. Атака Man in – the – Middle (человек в середине).
4. Угадывание ключа.

Задание №5

Какая сетевая атака является характерной именно для беспроводных сетей?

1. Вещание радиомаяка.
2. Подслушивание (Sniffing).
3. Атака Man in – the – Middle (человек в середине).
4. Отказ в обслуживании (DoS –атака).

Задание №6

Основной защитой от фишинга являются:

1. Фильтры.
2. Антивирусные программы.
3. Криптографические системы.
4. Системы видеонаблюдения.

Задание №7

Под политикой безопасности организации понимают:

1. Совокупность документированных управленческих решений, направленных на защиту информации.
2. Совокупность юридических законов в области защиты информации.
3. Процедура безопасности.
4. Руководство по архитектуре безопасности.

Задание №8

Политика удаленного доступа – это:

1. Специализированная политика безопасности.
2. Базовая политика безопасности.

3. Процедура безопасности.
4. Руководство по архитектуре безопасности.

Задание №9

Политики безопасности разделяют на уровни:

1. Верхний, средний и нижний.
2. Верхний и нижний.
3. Обобщенный и детальный.
4. Нет разделения на уровни.

Задание №10

Какая криптосистема шифрования является ассиметричной?

1. Алгоритм шифрования RSA.
2. Шифр Виженера.
3. Американский стандарт шифрования AES.
4. Стандарт шифрования ГОСТ 28147-89.

Задание №11

При шифровании методом Виженера слова «Банк» получилось зашифрованное сообщение «ВГТЛ». Какой был использован ключ?

1. 1-3-5
2. 2-6
3. 6-1-4
4. 8-5-2-3

Задание №12

Для проверки электронной цифровой подписи необходимо знать:

1. Открытый ключ отправителя.
2. Секретный ключ отправителя.
3. Два ключа отправителя: секретный и открытый.
4. Не требуется знания никаких ключей.

Задание №13

Под аутентификацией понимают:

1. Процедуру проверки подлинности заявленного пользователя, процесса, устройства.
2. Процедуру распознавания пользователя по его идентификатору.
3. Процедуру предоставления субъекту определенных полномочий и ресурсов в сети.
4. Регистрацию действий пользователя в сети.

Задание №14

Вероятность угадывания PIN –кода из 4 десятичных цифр за 3 попытки равна:

1. 0,0003.
2. 0,003
3. 0,00003.
4. 0,0004.

Задание №15

Различают следующие виды систем идентификации и аутентификации:

1. Электронные, биометрические и комбинированные.
2. Электронные и биометрические.
3. Электронные, биометрические и механические.
4. Электронные, биометрические и криптографические.

Задание №16

Какую функцию не может выполнять межсетевой экран?

1. Лечение файлов, зараженных вирусами.
2. Фильтрация трафика.
3. Трансляция сетевых адресов.
4. Регистрация событий.

Задание №17

Какой межсетевой экран обеспечивает наиболее высокий уровень безопасности?

1. Комплексный межсетевой экран.
2. Экранирующий маршрутизатор.
3. Шлюз сеансового уровня.
4. Прикладной шлюз.

Задание №18

Различают следующие варианты исполнения межсетевых экранов:

1. Программный и программно-аппаратный.
2. Программный и аппаратный.
3. Аппаратный и программно – аппаратный.
4. Существуют только программные межсетевые экраны.

Задание №19

Какая вредоносная программа не размножается, но способна удаленно управлять компьютером и воровать пароли?

1. Троянская программа.
2. Червь.
3. Файловый вирус.
4. Макровирус.

Задание №20

Какая антивирусная программа не конфликтует с другими антивирусами, но не имеет функции автоматического обновления антивирусной базы?

1. Dr. Web Curelt.
2. Kaspersky Internet Security.
3. Eset NOD 32 Antivirus.
4. Avira AntiVir Personal.

Задание №21

Какой метод выявления вируса позволяет обнаруживать только известные вирусы?

1. Обнаружение, основанное на сигнатурах.
2. Обнаружение программ подозрительного поведения.
3. Обнаружение вирусов при помощи эмуляции работы программы.
4. Эвристический анализ.

Задание №22

Сколько существует классов защищенности средств вычислительной техники от несанкционированного доступа?

1. 7.
2. 5.
3. 9.
4. 6.

Задание №23

Какой класс защищенности автоматизированных систем предъявляет наиболее высокие требования к информационной безопасности?

1. 1А
2. 1Г
3. 3Б
4. 3А

Задание №24

Вторая группа классов защищенности автоматизированных систем включает автоматизированные системы:

1. В которых работают несколько пользователей и все они имеют одинаковые права доступа к информации.
2. В которых работают несколько пользователей, и они имеют различные права доступа к информации.

3. В которых работает только один пользователь.

4. В которых работает один пользователь или несколько пользователей, имеющих одинаковые права доступа к информации.

Задание №25

В каком законе определены принципы и порядок засекречивания информации?

1. Закон “О государственной тайне”.

2. Закон “О безопасности”.

3. Закон “Об информации, информационных технологиях и о защите информации”.

4. Закон “Об авторском праве и смежных правах”.

Задание №26

Какой вид деятельности предприятий подлежит лицензированию ФСБ?

1. Эксплуатация негосударственными предприятиями шифровальных средств, предназначенных для криптографической защиты информации, не содержащих сведений, составляющих государственную тайну.

2. Сертификация, сертификационные испытания защищенных технических средств обработки информации (ТСОИ).

3. Аттестование систем информатизации, систем связи и передачи данных, технических средств приема, систем передачи и обработки информации, подлежащей защите.

4. Проведение специальных исследований на побочные электромагнитные излучения и наводки (ПЭМИН) ТСОИ.

Задание №27

Является объектом авторского права, но не признается патентоспособным изобретением:

1. База данных.

2. Устройство.

3. Способ.

4. Вещество.

Задание №28

Основная масса угроз приходится на:

1. Шпионские программы.
2. Троянские программы.
3. Черви.

Задание №29

Какой вид идентификации и аутентификации является наиболее распространённым:

1. Одноразовые пароли.
2. Постоянные пароли.
3. системыPKI.

Задание №30

Под какие системы вирусы распространяются наиболее динамично:

1. Windows.
2. Mac OS.
3. Android.
4. Linux.

Задание №31

Заключительный этап построения системы защиты:

1. Планирование.
2. Сопровождение.
3. Анализ уязвимых мест.
4. Отчётность.

Задание №32

Какие угрозы безопасности информации являются преднамеренными:

1. Открытие электронного письма, содержащего вирус.

2. Ошибка персонала.

3. Не авторизированный доступ.

4. Открытие сайта.

Задания в открытой форме

1. Персональные данные – это

2. Доступностью информации называется

3. К объектам информационной безопасности на предприятии относятся

4. Целостностью информации называется

5. Конфиденциальностью информации называется

6. К коммерческой тайне относится информация

7. Информационной безопасностью предприятия является

8. В состав системы защиты информации входят обеспечивающие подсистемы

9. Под угрозой безопасности информации понимается

10. Причинами информационных угроз являются

11. Основные компьютерные вирусы

12. К основным законам информационной безопасности РФ относятся законы

13. Основными принципами политики безопасности являются

14. Политика безопасности верхнего уровня включает

15. Удаленный доступ к сервису организован

16. Политика управления паролями включает

17. Системный подход к защите информации базируется на принципах

18. Для ИБ используются программные средства

19. Метод принуждения от метода побуждения отличается

20. Криптография занимается

21. Электронная подпись используется для

22. В состав организационно-технических мер входит

23. Межсетевые экраны применяют для

24. Технические средства противодействия классифицируются

25. В состав службы безопасности входят подразделения

26. К мерам по защите информации в интернете относятся

27. Межсетевые экраны-брандмауэры используются для

28. Для защиты электронной почты используется

29. Для защиты от вирусов можно использовать

30. К антивирусным программам относятся

31. Основные источники проникновения вирусов

32. В корпоративной сети необходимо защищать

33. Основные этапы построения системы защиты

34. План защиты включает

35. Ответственным за определение уровня классификации информации является

36. Ответственность за гарантии того, что данные классифицированы и защищены несёт

37. Политики безопасности – это

38. Естественные угрозы безопасности информации вызваны

39. Искусственные угрозы безопасности информации вызваны

40. К посторонним лицам - нарушителям информационной безопасности относятся

41. К основным непреднамеренным искусственным угрозам автоматизированным систем обработки информации относятся

42. К внутренним нарушителям информационной безопасности относится

Задания на установление соответствия

1. Установить соответствие названиям функций

1	Mozilla	А	Стандартная программа Windows
2	Winrar	Б	База данных
3	Блокнот	В	Программа-архиватор
4	Картотека учащихся	Г	Программа-браузер

2. Установить соответствие топологии сети её характеристике

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

3. Установить соответствие между компьютерными изобретениями и именами учёных

1	Всемирная паутина	А	Нейман
2	Компьютерная мышь	Б	Касперский
3	Первая ЭВМ	В	Тим Бернерс-Ли
4	Антивирус	Г	Дуглас Энгельбарт

4. Установить соответствие названиям устройств ПК назначение

1	Модем	А	Устройство для вывода текстов на экран
2	Клавиатура	Б	Устройство для хранения файлов
3	Монитор	В	Устройство для обмена информацией между ПК и провайдером через сеть
4	Жесткий диск	Г	Устройство для ввода символов

5. Установить соответствие названия ОС её назначению

1	NetWare	А	Серверная операционная система для поддержки виртуальных машин, включая виртуальные машины на Linux.
2	LANtastic	Б	Серверная операционная система с объектно-ориентированный

			интерфейсом OS/2 для создания мощного набора графических средств администратора.
3	Windows Server 2019	В	Сетевая операционная система и набор сетевых протоколов для взаимодействия с компьютерами-клиентами, подключёнными к сети
4	LAN server	Г	Сетевая операционная система для DOS, Windows,OS/2 с поддержкой технологии Ethernet, ARCNET и Token Ring

6. Установить соответствие типа файлов именам

1	…….doc	А	Файл запуска программы
2	…….exe	Б	Текстовый файл
3	…….bmp	В	Каталог
4	Сотрудники	Г	Графический файл

7. Установить соответствие имени рабочей области таблицы

1	Строки	А	Специальные символы
2	Столбцы	Б	Сочетание буквы и цифры
3	Ячейки	В	Английские буквы
4	Цифры	Г	Русские буквы

8. Установить соответствие расширения файла типу хранимой информации

1	…….jpg	А	Документ MS Word
2	…….txt	Б	Электронная таблица
3	…….doc	В	Текстовый документ
4	…….xls	Г	Фотография

9. Установить соответствие между способами и видами информации

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

10. Установить соответствие названия протокола его назначению

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

11. Установить соответствие оборудования его назначению

1	Репитер	А	Устройство для объединения ПК в сетях Ethernet
2	Концентратор	Б	Устройство для высокоскоростной коммутации пакетов между портами
3	Коммутатор	В	Устройство для подключения и соединения нескольких локальных сетей
4	Маршрутизатор	Г	Повторитель, усилитель сигналов

12. Установить соответствие между элементами ПК и функциями элементов

1	Процессор	А	Хранение информации
2	Оперативная память	Б	Обработка информации
3	Жесткий диск	В	Отображение информации
4	Монитор	Г	Ввод информации

Задания на установление правильной последовательности

1. Установить этапы разработки программного обеспечения:

1. Разработка алгоритма
2. Написание программы
3. Постановка задачи
4. Разработка математической модели

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 в порядке убывания единицы измерения памяти:

1. 2 байта

2. 4 байта

3. 3 бита

4. 1 байт

7. 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

8. 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

9. 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

10. Установить в порядке увеличения единицы измерения количества информации:

1. 1 ТБ

2. 30 Гбайт

3. 50 Килобайт

4. 100 Мегабайт

11. Установить в порядке возрастания функциональных возможностей:

1. WordPad

2. Блокнот

3. Microsoft Office Word

4. Corel Ventura Publisher

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

1. Дата, время

2. Протокол

3. Порт получателя

4. Номер агента

5. IP-адрес атакующего

6. Тип атаки

13. 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»

14. 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

15. 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

Компетентностно-ориентированные задачи

1. Рассчитать коэффицент Танимото и коэффицент корреляции и определить эффективность поиска страниц, связанных с разработками и публикациями в ФРГ в 2019 г. материалов по антивирусным программам в информационно-поисковых системах Yahoo! и Яндекс.

2. Файловый архив емкостью 412 Мб скачивается 20 минут. Соответствует ли действительности заявленная скорость провайдера в 35 Мбит/с.

3. Определите информационный объём сообщения в байтах, если в греческом алфавите 24 буквы и сообщение на греческом языке, содержащее 150 символов, было записано в коде Unicode.

4. Сколько времени будет скачиваться архив емкостью 500 Мб при скорости 50 Мбит/с.

5. Для кодирования последовательности, состоящей из букв А, Б, В, Г и Д, используется неравномерный двоичный код.

Для букв А, Б, В и Г использованы кодовые слова:

А-111

Б-110

В-101

Г-100

Определите, каким кодовым словом может быть закодирована буква Д.

(Код должен удовлетворять свойству однозначного декодирования. Если можно использовать более одного кодового слова, указать кратчайшее).

6. Определить минимальную длину кодового слова с возможностью исправления 3-х кратных ошибок при кодировании информации длиной 8 бит.

7. Рассчитать коэффициент Танимото и коэффициент корреляции и

определить эффективность поиска страниц, связанных с разработками и публикациями в России в 2019 г. материалов по антивирусным программам в информационно-поисковых системах Google и Яндекс.

8. Рассчитать коэффициент Танимото и коэффициент корреляции и определить эффективность поиска страниц, связанных с разработками и публикациями в США в 2019 г. материалов по антивирусным программам в информационно-поисковых системах Rambler и Google.

9. Рассчитать коэффициент Танимото и коэффициент корреляции и определить эффективность поиска страниц, связанных с разработками и публикациями в ФРГ в 2019 г. материалов по документальным БД в Internet в информационно-поисковых системах Яндекс и Google.

10. Рассчитать коэффициент Танимото и коэффициент корреляции и определить эффективность поиска страниц, связанных с разработками и публикациями в России в 2019 г. материалов по документальным БД в Internet в информационно-поисковых системах Яндекс и Rambler.

Критерии оценки:

- задание в закрытой форме –2балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла.
- решение компетентностно-ориентированной задачи – 6 баллов.