МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование ф-та полностью)
М.О. Таныгин
(подпись, инициалы, фамилия)
« *29* » *августа* 2022 г.

ОЦЕНОЧНЫЕ СРЕДСТВА
для текущего контроля успеваемости
и промежуточной аттестации обучающихся
по дисциплине
Защита информационных процессов в компьютерных системах
(наименование дисциплины)

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

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

Тема 1. Проблемы информационной безопасности сетей.

1. Классификация угроз информационной безопасности автоматизированных систем.
2. Назначение и структура стека протоколов TCP/IP. Характеристика протокола TCP/IP с точки зрения информационной безопасности.
2. 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).
4. 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).
5. Основные цели и характерные особенности сетевых атак. Виды сетевых атак: угадывание ключа, атаки на уровне приложений, сетевая разведка, злоупотребление доверием.
6. Основные характеристики спама и методы борьбы с ним.
7. Виды интернет- мошенничества: фишинг и фарминг и методы борьбы с ними.
8. Угрозы и уязвимости проводных корпоративных сетей.
9. Особенности построения и актуальность защиты беспроводных сетей. Виды сетевых атак: вещание радиомаяка, обнаружение WLAN, подслушивание, ложные точки доступа в сеть.
10. 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.

Тема 2. Политика безопасности.

11. Основные понятия политики безопасности.
12. Верхний, средний и нижний уровни политики безопасности.
13. Структура политики безопасности организации.
14. Базовая и специализированные политики безопасности.
15. Процедуры безопасности.
16. Основные этапы разработки политики безопасности.
17. Способы обеспечения информационной безопасности компьютерных сетей.
18. Фрагментарный и комплексный подходы.
19. Пути решения проблем защиты информации в сети Интернет.

20. Информационная безопасность электронного бизнеса.

Тема 3. Технологии аутентификации.

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

Тема 4. Технологии межсетевых экранов.

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.
34. Пограничные маршрутизаторы;
35. Операционные системы;
36. Персональные межсетевые экраны
37. IP-адреса источника и получателя;
38. Тип транспортного протокола;
39. Поля служебных заголовков протоколов сетевого и транспортного уровней;
40. Порт источника и получателя

Тема 5. Технологии защиты от вирусов.

41. Понятие компьютерного вируса.
42. Классификация вирусов.
43. Специализированные утилиты для борьбы с вредоносным ПО: антишпионы, антируткиты и антикейлоггеры.
44. Троянские программы. Виды троянских программ.
45. Компьютерные черви. Виды компьютерных червей.
46. Методы борьбы с вирусами: обнаружение, основанное на сигнатурах, обнаружение программ подозрительного поведения, метод “белого списка”
47. Методы борьбы с вирусами: обнаружение вирусов при помощи эмуляции работы программы, эвристический анализ, метод резидентных мониторов.

48. Антивирусные программы: утилита Dr. Web Curelt, программа Dr. Web., антивирус Avira AntiVir Personal, антивирус Avast! Home Edition.

49. Популярные пакеты антивирусной защиты: пакеты компании ESET(ESET NOD32 Antivirus, ESET NOD32 Smart Security).

50. Пакеты “Лаборатории Касперского” (Антивирус Касперского, Kaspersky Internet Security, Kaspersky Mobile Security).

Тема 6. Технологии анализа защищенности и обнаружения сетевых атак.

51. Что такое сетевая атака?
52. Назовите виды сетевых атак.
53. Перечислите способы обнаружения сетевых атак.
54. Концепция адаптивного управления безопасностью.
55. Средства анализа защищенности и общие требования к ним.
56. Классификация систем обнаружения атак.
57. Компоненты и архитектура системы обнаружения атак.
58. Обзор современных средств обнаружения атак.
59. Продукты компании Internet Security Systems.
60. Продукты компании Cisco Systems.

Тема 7. Требования к системам защиты информации.

61. Показатели защищенности средств вычислительной техники от несанкционированного доступа.

62. Показатели защищенности межсетевых экранов.

63. Классы защищенности автоматизированных систем.

64.Основные требования и рекомендации по защите информации, составляющей служебную тайну.

65. Защита конфиденциальной информации в АС и на рабочих местах пользователей ПК.

66.Требования к защите информации в локальных вычислительных сетях и при межсетевом взаимодействии.

67. Требования к защите информации при работе с системами управления базами данных.

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

69. Основные требования и рекомендации по защите информации, составляющей коммерческую тайну.

70. Основные требования и рекомендации по персональных данных.

Тема 8. Аудит безопасности информационных систем.

71. Понятие аудита безопасности информационных систем

72. Цели аудита безопасности информационных систем.

73. Стандарты, используемые при проведении аудита.

74. Основные этапы проведения аудита безопасности информационных систем .

75. Анализ рисков и управление рисками.

76. Методы оценки рисков и уровня защиты информационных систем.

77. Обзор программных продуктов для анализа и управления рисками: GRAMM, RiskWath,

78. Обзор программных продуктов для анализа и управления рисками - COBRA

79. Обзор программных продуктов для анализа и управления рисками - ПО компании MethodWare

80. Обзор программных продуктов для анализа и управления рисками - ПО “Аван Гард”.

Тема 9. Разработка и защита Web – сайтов.

81. Защита информации сайта от несанкционированного доступа с помощью аутентификации.

82. Защита контента сайта от несанкционированного копирования.

83. Методы защиты сайта от DDos – атак.

84. Что такое безопасность сайта?

85. Угрозы безопасности сайта.

86. Что такое межсайтовый скриптинг?

87. Уязвимости SQL-инъекций

88. Что такое подделка межсайтовых запросов?

89. Перечислите основные виды атак на веб-сайты?

90. Перечислите основные способы противодействия атакам на веб-сайты?

Критерии оценки:

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

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

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

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

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ЛАБОРАТОРНЫХ РАБОТ

Лабораторная работа № 1 «Создание сайтов на языке JavaScript и обеспечение их информационной безопасности»

1. Является ли HTML языком программирования?
2. Можно ли на HTML разрабатывать динамические сайты?
3. Какова структура HTML документа?
4. Какой тег в заголовочной части документа HTML является обязательным ?
5. Каким образом в документе HTML поисковым машинам предоставляется информация о тематике документа?
6. Каким образом можно оформить стиль документа HTML ?
7. Как определить стиль при котором все заголовки, ограниченные тегом будут выделены синим цветом?
8. Какова цель веб-безопасности?
9. Способы обеспечения безопасности сайта при его разработке?
10. Способы защиты информации от копирования?

Лабораторнаяработа № 2 «Разработка и защита Web - приложений с серверными сценариями на языке PHP.»

1. В чем отличие php-страницы от html-страницы?
2. Какие типы переменных поддерживает язык PHP?
3. Как передать переменную в php-страницу?
4. Какие параметры существуют у функции date()?
5. Что такое межсайтовый скриптинг?
6. Уязвимости SQL-инъекций
7. Что такое подделка межсайтовых запросов?
8. Перечислите основные виды атак на веб-сайты?
9. Перечислите основные способы противодействия атакам на веб-сайты?
10. Что такое безопасность сайта?

Лабораторная работа № 3 «Менеджер паролей: программа Password Commander.»

1) Что такое менеджер паролей и каковы его функции?
2) Приведите примеры программ, предназначенных для хранения паролей? Какие из них имеют русский интерфейс?

3) Обзор популярных менеджеров паролей: KeePass, Dashlane

4) Обзор популярных менеджеров паролей: 1Password, PasswordCommander

5) Обзор популярных менеджеров паролей: LastPass, Padloc

6) Обзор популярных менеджеров паролей: RememBear, Firefox Lockwise

7) Объясните, что такое аккаунт в программе PasswordCommander?

8) Для какой цели используются группы в программе PasswordCommander?

9) Какие поля по умолчанию используются в записях?

10) Можно ли добавить дополнительные поля в записях?

Лабораторная работа №4 «Фаервол Comodo Firewall.»

1) Дайте определение межсетевого экрана.

2) Перечислите основные функции межсетевых экранов.

3) Перечислите основные схемы подключения межсетевых экранов.

4) Перечислите типы межсетевых экранов, функционирующих на отдельных уровнях модели OSI.

5) Основные функции и дополнительные возможности межсетевых экранов. Политика работы МЭ.

6) Особенности функционирования межсетевых экранов на уровнях модели OSI. Варианты исполнения МЭ.

7) Основные схемы подключения межсетевых экранов.

8) Пограничные маршрутизаторы;

9) Операционные системы;

10) Персональные межсетевые экраны

Лабораторная работа №5«Антивирусная программа: Kaspersky Internet Security.»

1) Дайте классификацию компьютерных вирусов.

2) В чем основное отличие вирусов-сценариев от файловых вирусов?

3) Существование каких вирусов зависит от конкретной программы?

4) В чем основное отличие троянской программы от вируса. Приведите пример троянской программы.

5) Методы борьбы с вирусами: обнаружение, основанное на сигнатурах

6) Методы борьбы с вирусами: обнаружение программ подозрительного поведения, метод “белого списка”

7) Методы борьбы с вирусами: обнаружение вирусов при помощи эмуляции работы программы, эвристический анализ, метод резидентных мониторов.

8) Антивирусные программы: утилита Dr. Web Curelt, программа Dr. Web., антивирус Avira AntiVir Personal, антивирус Avast! Home Edition.

9) Популярные пакеты антивирусной защиты: пакеты компании ESET(ESET NOD32 Antivirus, ESET NOD32 Smart Security).

10) Пакеты “Лаборатории Касперского” (Антивирус Касперского, Kaspersky Internet Security, Kaspersky Mobile Security).

Критерии оценки:

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

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

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

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

1.3 СИТУАЦИОННЫЕ ЗАДАЧИ

1. Компания X разрабатывает приложение для хранения и обработки конфиденциальных данных своих клиентов. Какие меры безопасности должны быть предприняты для защиты этих данных? Какие риски могут возникнуть при неправильной реализации мер безопасности?
2. Компания Y использует облачное хранилище для хранения своих данных. Какие меры безопасности должны быть предприняты для защиты данных в облаке? Какие риски могут возникнуть при неправильной реализации мер безопасности?
3. Компания Z использует открытый Wi-Fi для своих сотрудников во время командировок. Какие меры безопасности должны быть предприняты для защиты конфиденциальной информации компании? Какие риски могут возникнуть при неправильной реализации мер безопасности?
4. Компания A рассматривает возможность использования биометрической аутентификации для входа в свою систему. Какие риски могут возникнуть при использовании такого метода аутентификации? Какие меры безопасности должны быть предприняты для защиты данных при использовании биометрической аутентификации?
5. Компания B использует систему виртуальных машин для своих сотрудников. Какие меры безопасности должны быть предприняты для защиты данных в виртуальных машинах? Какие риски могут возникнуть при неправильной реализации мер безопасности?
6. Вы работаете в крупной компании, которая использует распределенную систему для хранения и обработки данных. Один из ваших коллег сообщил вам о том, что он получил письмо от неизвестного отправителя, в котором говорится о возможной утечке конфиденциальной информации из вашей компании. Что вы сделаете в первую очередь, чтобы убедиться в безопасности системы?
7. Ваша компания использует распределенную систему для хранения и обработки данных клиентов. Однако, вы заметили, что произошла утечка некоторой конфиденциальной информации. В результате, несколько клиентов потеряли доверие к вашей компании. Какие меры вы предпримете, чтобы восстановить доверие клиентов и защитить данные в будущем?
8. Вы работаете в команде, которая отвечает за безопасность распределенной системы вашей компании. Один из ваших коллег предложил изменить пароли для всех пользователей системы раз в месяц. Однако, другой коллега считает, что это неэффективно и может негативно повлиять на производительность. Как вы решите эту ситуацию и какие меры безопасности вы предложите вместо изменения паролей?

9. Ваша компания решила использовать облачные технологии для хранения и обработки данных. Какие меры безопасности вы предложите для защиты данных и обеспечения безопасности в облаке?
10. Ваша компания использует распределенную систему для обработки крупных объемов данных. Какие меры безопасности вы предложите для защиты от DDoS-атак и других угроз, связанных с доступом к системе?
11. Задача на анализ рисков: Вам поручено провести анализ рисков для распределенной системы, состоящей из нескольких серверов, на которых хранится конфиденциальная информация. Какие шаги вы будете предпринимать для выполнения этого задания?
12. Задача на выбор метода шифрования: Вы разрабатываете распределенную систему, которая будет использоваться для передачи конфиденциальной информации. Какой метод шифрования вы выберете и почему?
13. Задача на оценку угроз: Ваша компания использует распределенную систему для хранения и обработки конфиденциальной информации. Какие угрозы могут возникнуть для безопасности этой системы и как можно защититься от них?
14. Задача на выбор аутентификационного метода: Вы разрабатываете распределенную систему, которая будет использоваться несколькими пользователями. Какой метод аутентификации вы выберете и почему?
15. Задача на планирование реагирования на инциденты: Ваша компания использует распределенную систему, которая хранит и обрабатывает конфиденциальную информацию. Как вы спланируете реагирование на возможные инциденты, такие как взлом системы или утечка данных? Какие шаги вы предпримете, чтобы свести к минимуму потенциальный ущерб?

Критерии оценки:

9-16 баллов (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

6-8 баллов (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.

1-5 баллов (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

Задание №1

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 №2

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 №3

Основной защитой от фишинга являются:

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

Задание №4

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 №5

Политика удаленного доступа – это:

1. Специализированная политика безопасности.
2. Базовая политика безопасности.
3. Процедура безопасности.
4. Руководство по архитектуре безопасности.

Задание №6

Политики безопасности разделяют на уровни:

1. Верхний, средний и нижний.
2. Верхний и нижний.
3. Обобщенный и детальный.

Нет разделения на уровни.

Задание №7

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 №8

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 №9

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 №10

Какую функцию не может выполнять межсетевой экран?

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

Задание №11

Какой межсетевой экран обеспечивает наиболее высокий уровень безопасности ?

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

Задание №12

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 №13

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

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

Задание №14

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 №15

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 №16

В чем основное отличие системы анализа защищенности от системы обнаружения атак ?

1. Системы анализа защищенности исследуют сеть и ищут уязвимости в ней, системы обнаружения атак предназначены для противодействия сетевым атакам в реальном масштабе времени.
2. Системы анализа защищенности предназначены для противодействия сетевым атакам в реальном масштабе времени, системы обнаружения атак только моделируют сетевые атаки в целях поиска уязвимостей в защите сети.
3. Системы анализа защищенности и системы обнаружения атак – это одно и то же.
4. В отличии от систем обнаружения атак системы анализа защищенности только выдают предупреждения об обнаруженных атаках, но не противодействуют им в автоматическом режиме.

Задание №17

Какой метод анализа сетевой информации не требует знаний о возможных атаках и используемых ими уязвимостях?

1. Статистический метод.
2. Экспертные системы.
3. Нейронные сети.
4. Такого метода не существует.

Задание №18

Какие системы обнаружения атак (IDS) позволяют обнаруживать новые, ранее неизвестные виды сетевых атак?

1. IDS, которые для выявления атаки используют способ - обнаружение аномального поведения.
2. Пассивные IDS.
3. Активные IDS.
4. IDS, которые для выявления атаки используют способ - обнаружение злоупотреблений.

Задание №19

Сколько существует классов защищенности средств вычислительной техники от несанкционированного доступа ?

1. 7.

2. 5.
3. 9.
4. 6.

Задание №20

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

1. 1А
2. 1Г
3. 3Б
4. 3А

Задание №21

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 №22

Какой стандарт, используемый при проведении аудита, состоит из двух частей: “Практические рекомендации” и “Спецификации системы” ?

1. Стандарт BS7799
2. Стандарт ISO17799
3. Стандарт ISO/IEC15408
4. Стандарт SysTrust

Задание №23

Какой этап проведения аудита является первым ?

1. Инициирование и планирование процедуры аудита.
2. Сбор информации аудита.
3. Анализ данных аудита.
4. Оценка соответствия требованиям стандарта.

Задание №24

В каком методе анализа рисков рассчитываются минимальный и максимальный ущерб?

1. Оценка по верхним и нижним значениям.
2. Оценка рисков на этапе рассмотрения этапов вторжения.
3. Логарифмическая шкала.
4. Оценка на основе выявления слабого звена.

Задание №25

Какая программа предназначена для шифрования HTML – кода?

1. WebCrypt.
2. TrueCrypt.
3. PGP.
4. КРИПТОН Подпись.

Задание №26

Даны два Java – скрипта.

Первый Java – скрипт имеет вид:

```
<script language="JavaScript">

document.onselectstart=function(){return false}

document.onmousedown=function(){return false}

</script>
```

Второй Java – скрипт имеет вид:

```
<script language="JavaScript">
document.onselectstart=function(){return false}
document.oncontextmenu=function(){return false}
document.onmousedown=function(){return false}
</script>
```

Какой из рассмотренных Java – скриптов в целях защиты информации блокирует использование правой кнопку мыши ?

1. Второй
2. Первый
3. Первый и второй.
4. Ни один из рассмотренных Java – скриптов не блокирует правую кнопку мыши.

Задание №27

Какую из двух программ (Easy Watermark или Photoshop) можно использовать для защиты фотографии водяным знаком?

1. Можно использовать обе программы: Easy Watermark или Photoshop.
2. Только Easy Watermark.
3. Только Photoshop.
4. Ни одна из данных программ не позволяет установить на фотографию водяной знак.

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.

33. Выберите соответствие названий типов сетей устройств из приведен- ного перечня в зависимости от их масштаба:

а) муниципальная вычислительная сеть (Munitipal Area Network MAN);

б) территориальная вычислительная сеть (Wide Area Network WAN);

в) локальная вычислительная сеть ЛВС (Local Area Network LAN);

г) кампусная вычислительная сеть (Campus Area Network CAN); д)персональная вычислительная сеть (Personal Area Network PAN).

34. Укажите название утилиты, пересылающей набор тестовых пакетов на удаленный компьютер и получающей от него в случае его нормальной работы ответные пакеты

а) gong;

б) ping;

в) ring;

г) gang.

35. Выберите компоненты, входящие в состав сетевого адаптера: а) постоянное запоминающее устройство с BIOS;

б) разъем для подключения кабеля;

в) контроллер аппаратных прерываний IRQ; г) кварцевый элемент тактового генератора; д) СБИС контроллера сетевого адаптера;

е) панелька для BootROM;

ж) южный мост (Input-Output Controller Hub).

36. Выберите минимальное количество настроек, необходимых для организации работы компьютера настройки в сети с сетевым протоколом TCP/IP:

а) установить IP-адрес компьютера;

б) установить основной шлюз подсети данного компьютера; в)установить маску подсети, в которую входит компьютер;

г) установить IP-адрес DNS-сервера локальной сети компьютера; д) установить IP-адрес почтового сервера домена;

е) установить IP-адрес прокси-сервера.

37. Выберите вариант, в котором правильно расположены в порядке возрастания значений полосы пропускания следующие среды передачи данных коаксиальный медный кабель, кабель на основе медной ви- той пары, оптоволоконный кабель:

а) коаксиальный медный кабель, кабель на основе медной "витой пары", оптоволоконный кабель;

б) оптоволоконный кабель, коаксиальный медный кабель, кабель на основе медной "витой пары";

в) кабель на основе медной "витой пары", коаксиальный медный кабель, оптоволоконный кабель.

38. Выберите ресурсы, выделяемые операционной системой сетевому адаптеру:

а) MAC-адрес адаптера;

б) порт ввода-вывода (I/O port); в) полоса пропускания канала; г) запрос прерывания IRQ;

д) диапазон адресов памяти адаптера.

Укажите вводимую в окне командной строки команду, отображаю- щую IP-адрес компьютера, работающего под операционной системой Windows:

а) cmd;

б) net;

в) ipconfig; г) netstat.

39. Укажите преимущества использования компьютерных сетей:

а) возможность оперативной коммуникации между участниками се- ти и оперативного доступа к информации;

б) возможность совместного использования аппаратных ресурсов; в) возможность практически безграничного увеличения вычисли-

тельной производительности систем;

г) возможность организации совместной работы путем разделения прикладных программ и файлов;

д) упрощение конфигурирования и пользования операционными си- стемами и пользовательскими программами;

е) возможность централизованного управления данными и про- граммами.

40. Выберите соответствие названий и определений сетевых компонентов Windows, приведенных в списке:

а) клиент;

б) протокол;

в) служба;

г) адаптер.

41. Драйвер сетевой платы, непосредственно взаимодействующий с сетевой платой, установленной в компьютере это…,

а) Компонент, регламентирующий правила разбиения потока информации на пакеты и правила адресации компьютеров-участников сети,

б) Компонент, позволяющий подключаться к серверам сети,

в) Компонент, позволяющий выделять сетевые ресурсы на компьютере,на котором он установлен,

42. Выберите типы доступа для сетевых дисков и папок, определяемых в операционной системе Windows:

а) чтение;

б) чтение и выполнение;

в) изменение;

г) запись;

д) полный доступ;

е) просмотр;

ж) список содержимого папки.

43. Какой из сетевых компонентов Windows обеспечивает возможность предоставления ним сетевых ресурсов?

а) адаптер;
б) сетевой протокол;
в) клиент;
г) служба.

44. Какой из сетевых компонентов Windows отвечает за адресацию узлов сети на сетевом уровне?

а) адаптер;
б) сетевой протокол; в) клиент;
г) служба.

45. Выберите правильную команду выделения на Вашем компьютере папки C:\Data в общее пользование по сети с сетевым именем AllData: а) net share AllData =c:\data;

б) net share c:\data AllData; в) net use AllData = c:\data; г) net use c:\data AllData;
д) net view AllData =c:\data;
е) net view c:\data AllData.

46. Выберите команду подключения сетевого ресурса \\FS_stud\user и отображения его как сетевого диска Z:

а) net share Z: \\Fs_stud\user; б) net share \\Fs_stud\user Z: ; в) net use Z: \\Fs_stud\user;
г) net use \\Fs_stud\user Z: д) net view Z: \\Fs_stud\user е) net view \\Fs_stud\user Z:

47. Выберите команду, позволяющую вывести список сетевых имен работающих в данный момент компьютеров Вашей сети:

а) net computer
б) net view в) net config г) net name д) net group

48. Укажите, кто входит в группу пользователей Все в операционной системе Windows:

а) все пользователи локальной сети; б) все пользователи сети предприятия;
в) все зарегистрированные в операционной системе пользователи.

49. Выберите права, которые отличают разрешение Изменение от разреше- ния Полный доступ:

а) добавлять файлы и подпапки;
б) изменять владельца сетевого ресурса; в) изменять данные в файлах;
г) изменять разрешения безопасности; д) удалять подпапки и файлы.

50. Выберите название протокола прикладного уровня, позволяющего одновременно организовывать сетевой доступ к файловым ресурсам и принтерам в Windows и Linux:

а) HTTP б) FTP
в) CIFS/SMB.

51. Укажите номера битов MAC-адреса (нумерация начинается с нуля) для каждого из его полей:

а) Поле U/L - уникальный в глобальном/локальном масштабе;
б) Поле I/G - индивидуальный/групповой;
в) Поле OUA - организационно-уникального идентификатора порядкового номера сетевого контроллера, выпускаемого организацией;
г) Поле OUI - организационно-уникального идентификатора кода организации, выпускающей сетевое оборудование.

52. Выберите максимальную на сегодняшний день стандартизованную скорость передачи данных по технологии Ethernet:

а) 10 Мбит/с;
б) 100 Мбит/с;
в) 1 Гбит/с;
г) 10 Гбит/с;

д) 40 Гбит/с;
е) 100 Гбит/с;
ж) 1 Тбит/с.

53. Укажите уровни модели взаимодействия открытых систем, на которых работает технология Ethernet:

а) сетевой;
б) канальный; в) прикладной;
г) транспортный;
д) представления данных; е) физический;
ж) сеансовый.

54. Укажите размеры максимального кадров Ethernet (не учитывая опциональную возможность передачи гигантских кадров (Jambo Frame)):

а) 32 байта;
б) 64 байта;
в) 128 байт;
г) 256 байт;
д) 512 байт;
е) 1024 байта;
ж) 1518 байт;
з) 2000 байт.

55. Укажите размеры минимальных кадров Ethernet (не учитывая опциональную возможность увеличения минимального размера кадра до 512 байт в полудуплексном режиме работы технологии Gigabit Ethernet):

а) 32 байта;
б) 64 байта;
в) 128 байт;
г) 256 байт;
д) 512 байт;
е) 1024 байта;
ж) 1518 байт;
з) 2000 байт.

Укажите размер MAC-адреса:

а) 2 байта;
б) 3 байта;
в) 4 байта;
г) 6 байт;
д) 8 байт.

56. Наиболее распространены угрозы информационной безопасности сети:

а) Распределенный доступ клиент, отказ оборудования
б) Моральный износ сети, инсайдерство
в) Сбой (отказ) оборудования, нелегальное копирование данных

57. Определите тип кадра Ethernet (DIX, Novell 802.3, 802.3/LLC, SNAP) по байтам заголовка канального уровня:

а) 00:4F:49:02:D8:6A:00:A0:C9:83:16:16:08:00;
б) 00:A0:C9:85:17:B2:00:4F:4E:00:E5:8F:00:54:E0:E0:03;
в) 00:4F:4E:00:CD:4A:00:60:8C:41:DF:C7:00:96:AA:AA:03:00:00
:00:08:00;
г) 00:00:F8:45:13:AC:00:00:C0:02:56:AB:00:78:FF:FF.

58. Выберите неизвестную в общем случае адресную информацию при отправке пакета утилиты ping по IP-адресу назначения:

а) MAC-адрес отправителя;

б) MAC-адрес получателя;
в) IP-адрес отправителя;
г) IP-адрес получателя.

59. Укажите, откуда коммутатор Ethernet узнаѐт MAC-адреса подключѐнных к нему компьютеров, необходимые для заполнения его таблицы MAC-адресов:

а) выполняет последовательный опрос подключѐнных компьютеров;
б) "подсматривает" адрес отправителя во входящих в него пакетах;
в) опрашивает все компьютеры в широковещательном режиме.

60. Укажите, какие пакеты будет захватывать Wireshark при введѐнной команде фильтра ether proto 0x0806

а) только кадры Ethernet с любыми пакетами внутри;
б) только кадры Ethernet с IP пакетами внутри;
в) только кадры Ethernet с ARP-пакетами внутри.

Укажите команды (enable, config t, interface имя_интерфейса), позволяющие осуществлять вход в различные режимы работы Cisco IOS:

а) войти в режим глобального конфигурирования можно коман- дой…;
б) войти в привилегированный режим можно командой…;
в) войти в режим конфигурирования интерфейса можно командой….

61. Хост имеет IP-адрес 192.168.1.47 и маску подсети 255.255.255.224. Укажите адрес подсети и широковещательный адрес подсети, в которую входит данный хост.

Укажите класс (A, B или C) следующих IP-адресов:

а) 172.16.2.2;
б) 10.15.234.28;
в) 192.168.5.137.

62. В Вашей сети находится 31 компьютер. Укажите маску подсети, обеспечивающую выделение этих компьютеров в подсеть с минимально возможным числом IP-адресов

а) 255.255.255.248;
б) 255.255.255.240;
в) 255.255.255.224;
г) 255.255.255.192;
д) 255.255.255.128.

63. Выберите условие, при выполнении которого хост/маршрутизатор пересылает IP-дейтаграмму шлюзу:

а) IP-адрес отправителя и IP-адрес получателя принадлежат разным сетям/подсетям;
б) IP-адрес отправителя и IP-адрес получателя принадлежат одной и той же сети/подсети;
в) IP-адрес получателя и IP-адрес получателя принадлежат одной и той же сети/подсети;

64. Выберите правильное определение для максимальной единицы передачи (Maximum Transfer Unit, MTU):

а) MTU – это максимально допустимый размер заголовка IP-пакета;
б) MTU – это максимально допустимый размер IP-пакета;
в) MTU – это максимально допустимое значение длины поля данных кадров канального уровня.

Выберите адрес, по которому не будут передаваться IP-дейтаграммы в Интернете:

а) 141.25.13.48;
б) 172.31.204.1;
в) 191.15.26.147.

65. Выберите логическую операцию, которая используется для определения адреса сети/подсети из IP-адреса получателя дейтаграммы:

а) IP-адрес получателя XOR маска сети/подсети;
б) IP-адрес получателя OR маска сети/подсети;
в) IP-адрес получателя AND маска сети/подсети.

Укажите маску суперсети с 2000 хостами, если адрес такой сети 212.14.17.0:

а) 255.255.255.0;
б) 255.255.254.0;
в) 255.255.252.0;
г) 255.255.248.0.

66. Выберите правильное утверждение об изменениях MAC- и IP-адресов в пересылаемых в составной сети сетевых пакетах при следовании их по маршруту:

а) MAC-адрес отправителя на каждом шаге изменяется, MAC-адрес получателя остаѐтся неизменным, IP-адреса остаются неизменными;

б) MAC-адрес отправителя и MAC-адрес получателя остаются неизменными на каждом шаге, IP-адреса также остаются неизменными;

в) MAC-адрес отправителя и MAC-адрес получателя изменяются на каждом шаге изменяется, IP-адреса остаются неизменными;

г) MAC-адрес отправителя и MAC-адрес получателя остаются неизменными на каждом шаге, IP-адреса изменяются;

66. Укажите, какя информация служит указателем на первый фрагмент дейтаграммы:

а) нулевое значение флага MF More Fragments;
б) нулевое значение поля Смещение фрагмента;
в) нулевое значение поля Идентификатор пакета.

68. В пакете, пересылаемом в локальной сети порт отправителя = 80, порт получателя = 24561. Выберите из списка тип протокола и привязку портов к клиенту и серверу:

а) протокол UDP, отправитель - сервер, получатель - клиент;
б) протокол UDP, отправитель - клиент, получатель - сервер;
в) протокол TCP, отправитель - сервер, получатель - клиент;
г) протокол TCP, отправитель - клиент, получатель - сервер.

69. Выберите, что характеризует порт транспортного уровня:

а) порт сетевого адаптера, через который хост работает с сетью;
б) область памяти, связанную с сетевым приложением;
в) порт ввода-вывода, закреплѐнный за сетевым адаптером.

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

а) Вероятное событие
б) Детерминированное (всегда определенное) событие
в) Событие, происходящее периодически

71. Команда netstat -an вывела на экран следующие строки. Укажите, какие из них описывают сокеты установленного соединения:

а) TCP 0.0.0.0:135 0.0.0.0:0 LISTENING;
б) TCP 109.201.253.151:3603 74.125.39.104:80 ESTABLISHED;
в) TCP 109.201.253.151:54035 62.165.4.118:33016 TIME_WAIT;
г) TCP 109.201.253.151:54035 90.176.90.125:11740 SYN_RECEIVED.

72. Укажите десятичное значение, идентифицирующее UDP в поле Протокол IP-заголовка:

а) 01;
б) 06;
в) 17.

73. Укажите поля, которые входят в псевдозаголовок, используемый при расчѐте контрольной суммы UDP или TCP:

а) MAC-адрес отправителя; б) MAC-адрес получателя;
в) IP-адрес отправителя; г) IP-адрес получателя; д) порт отправителя;
е) порт получателя;
ж) идентификатор протокола; з) длина пакета с заголовком.

74. Выберите, чему равняется максимальный размер сегмента для заголовка Ipv4 без опций и заголовка TCP длиной 28 байт:

а) 1452 байта;
б) 1460 байт;
в) 1472 байта;
г) 1500 байт.

75. TCP-пакет с полем данных 500 байт имеет десятичное значение SEQ#=15246, а десятичное значение ACK#=32412. Выберите, какими будут десятичные значения этих полей в ответе на данный пакет, если в нѐм пересылается 300 байт данных:

а) SEQ#=15746, ACK#=32712; б) SEQ#=32712, ACK#=15746; в) SEQ#=15747, ACK#=32713; г) SEQ#=15745, ACK#=32711

76. Из захваченных пакетов сеанса TCP извлечены три пакета с флагами: а) PSH, ACK;
б) SYN;
в) FYN, ACK;
г) SYN, ACK.

77. Укажите, какие из них относятся к:
пакетам, устанавливающим соединение, …;
пакетам, передающим данные в сеансе, …;
пакетам, завершающим соединение, ….

78. Выберите название поля заголовка TCP, позволяющего регулировать поток данных с противоположной стороны соединения:

а) Длина заголовка;
б) Окно;
в) Контрольная сумма;
г) Указатель срочности.

79. На каком типе щифрования основан протокола IPSec
а) симметричном
б) асиметричном
в) комбинированном
г) В нём не используется шифрование

80. Почему хэш вставляется в конце передаваемого по сети кадра

а) потому что он формируется аппаратно во время последовательной передачи и завершает кадр
б) потому что это позволяет минимизировать потери информации при случайных искажениях
в) это упрощает разбор кадра при получении

81. Основные угрозы доступности информации:
-хакерская атака
-разрушение или повреждение помещений
-отказ программного и аппаратно обеспечения
-перехват данных
-непреднамеренные ошибки пользователей
-злонамеренное изменение данных

82. Суть компрометации информации
-внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации

-несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений

-внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений

83. Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, …

-способна противостоять только внешним информационным угрозам

-способна противостоять только информационным угрозам, как внешним так и внутренним

-с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации

-с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой — ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды

84. Методы повышения достоверности входных данных

-Отказ от использования данных

-Проведение комплекса регламентных работ

-Многократный ввод данных и сличение введенных значений

-Введение избыточности в документ первоисточник

-Использование вместо ввода значения его считывание с машиночитаемого носителя

-Замена процесса ввода значения процессом выбора значения из предлагаемого множества

85. Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ)

-МЭ работают только на сетевом уровне, а СОВ – еще и на физическом

-МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты

-МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения

86. Сервисы безопасности:

-контроль целостности

-кэширование записей

-регулирование конфликтов

-экранирование

-идентификация и аутентификация

-инверсия паролей

-обеспечение безопасного восстановления

-шифрование

87. Под угрозой удаленного администрирования в компьютерной сети понимается угроза …

-несанкционированного управления удаленным компьютером

-поставки неприемлемого содержания

-перехвата или подмены данных на путях транспортировки

-вмешательства в личную жизнь

-внедрения агрессивного программного кода в рамках активных объектов Web-страниц

88. Причины возникновения ошибки в данных

-Использование недопустимых методов анализа данных

-Преднамеренное искажение данных

-Ошибка при записи результатов измерений в промежуточный документ
-Неверная интерпретация данных
-Ошибки при переносе данных с промежуточного документа в компьютер
-Погрешность измерений
-Неустранимые причины природного характера
-Ошибки при идентификации объекта или субъекта хозяйственной деятельности

89. Наиболее эффективное средство для защиты от сетевых атак -
использование только сертифицированных программ-браузеров при доступе к сети Интернет
-использование сетевых экранов или «firewall»
-посещение только «надёжных» Интернет-узлов
-использование антивирусных программ

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

91. Разделы современной криптографии:
-Управление передачей данных
-Управление паролями
-Криптосистемы с открытым ключом
-Криптосистемы с дублированием защиты
-Системы электронной подписи
-Симметричные криптосистемы
-Управление ключами

92. Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности
-рекомендации X.800
-Оранжевая книга
-Закону «Об информации, информационных технологиях и о защите информации»

93. Утечка информации – это …
-процесс раскрытия секретной информации
-несанкционированный процесс переноса информации от источника к злоумышленнику
-процесс уничтожения информации
-непреднамеренная утрата носителя информации

94. Основные угрозы конфиденциальности информации:
-маскарад
-злоупотребления полномочиями
-блокирование
-перехват данных
-карнавал
-переадресовка

95. Элементы знака охраны авторского права:
-наименования (имен правообладателя
-буквы Р в окружности или круглых скобках
-наименование охраняемого объекта
-года первого выпуска программы
-буквы С в окружности или круглых скобках

96. Защита информации обеспечивается применением антивирусных средств
-не всегда

-нет

-да

97. Преднамеренная угроза безопасности информации

-ошибка разработчика

-повреждение кабеля, по которому идет передача, в связи с погодными условиями

-кража

-наводнение

98. Концепция системы защиты от информационного оружия не должна включать…

-средства нанесения контратаки с помощью информационного оружия

-процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей

-механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры

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

-Программные, технические, организационные, технологические

-Серверные, клиентские, спутниковые, наземные

-Личные, корпоративные, социальные, национальные

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

-Владелец сети

-Администратор сети

-Пользователь сети

Задания в открытой форме

1. Основные угрозы безопасности при работе с распределенными системами включают атаки на …
2. SSL/TLS - это протоколы шифрования, используемые для …
3. Атаки на отказ в обслуживании (DDoS) - это атаки, которые заключаются в …
4. Управление доступом - это процесс определения, кто имеет право на …
5. Блокчейн - это технология, которая позволяет создавать …
6. Распределенная система - это сеть компьютеров, которые работают…
7. Типы угроз, которые могут возникнуть при работе с распределенными системами, включают в себя…
8. Основные принципы криптографии включают в себя…
9. Методы аутентификации пользователей, которые могут быть использованы для защиты распределенных систем от несанкционированного доступа, включают в себя…
10. Атаки на отказ в обслуживании (DDoS) могут привести…
11. Технология блокчейн используется для обеспечения…
12. Использование виртуализации может увеличить уязвимости распределенных систем, но можно принять меры, такие как…

13. Система обнаружения вторжений (IDS) используется для защиты распределенных систем, путем…

14. Для защиты от атак на отказ в обслуживании (DDoS) используются различные инструменты и технологии, включая:…

15. Для защиты распределенных систем от несанкционированного доступа используются различные методы аутентификации пользователей, такие как…

16. Целостность данных играет важную роль в…

17. Использование виртуализации может повысить уязвимость распределенных систем, поскольку виртуальные среды…

18. Система баз данных-это…

19. Для защиты ИС от фишинга можно использовать различные методы, включая обучение сотрудников компании основам безопасности информации, использование…

20. Для защиты ИС от сетевых атак можно применять различные меры, включая использование механизмов защиты периметра, таких как …

Задания на установление соответствия

1.Установите соответствие между названием системных вызовов и их описанием

1	Create	А	Системный вызов позволяет системе прочитать в оперативную память атрибуты файла и список дисковых адресов для быстрого доступа к содержимому файла при последующих вызовах.
2	Read	Б	Когда все операции с файлом закончены, файл следует закрыть, чтобы освободить пространство во внутренней таблице системы.
3	Open	В	Этот системный вызов объ- являет о появлении нового файла и позволяет установить некоторые его атрибуты.
		Г	Чтение данных из файла.

2.Установите соответствие между названием объекта операционной системы и его назначением

1	Write	А	Операция устанавливает указатель текущей позиции на определенное место файла. Последующие данные будут считаны из этой позиции и записаны в нее.
2	Append	Б	Запись данных в файл, также в текущую позицию в файле.

			Если текущая позиция находится в конце файла, размер файла автоматически увеличивается.
3	Seek	В	Некоторые атрибуты файла могут устанавливаться пользователем после создания файла. Этот системный вызов предоставляет такую возможность.
		Г	Этот системный вызов представляет собой усеченную форму вызова write. Он может только добавлять данные к концу файла. Данный вызов в операционных системах может отсутствовать

3.Установите соответствие с названием разделяемой памятью системных вызовов и их описанием

1	shmget	А	Служит для управления разнообразными параметрами, связанными с существующим сегментом
2	shmat	Б	Создает новый сегмент разделяемой памяти или находит существующий сегмент с тем же ключом
3	shmdt	В	Отключает от виртуальной памяти ранее подключенный к ней сегмент с указанным виртуальным адресом начала
		Г	Подключает сегмент с указанным дескриптором к виртуальной памяти обращающегося процесса

4.Установите соответствие между названием видов памяти и его описанием

1	Оперативная память	А	Это промежуточное запоминающее устройство, используемое для ускорения обмена между процессором и RAM. В современных процессорах используется несколько уровней кэш-памяти.
2	Регистры	Б	Это электронная память предназначена для длительного сохранения программы и данных. Используется оно для чтения данных. Как правило, эта информация записывается при изготовлении компьютера и служит для начальной загрузки оперативной системы, проверки работоспособности компьютера.
3	Кэш-память	В	Это устройства, где размещены данные, который процессор обрабатывает в определенный промежуток времени.

		Г	Это сверхскоростная память процессора. Они сохраняют адрес команды, саму команду, данные для её выполнения и результат.

5.Установите соответствие между названием объекта операционной системы и его назначением

1	UFS	А	Это абстрактный уровень поверх более конкретной файловой системы
2	VFS	Б	Описание способов взаимодействия одной компьютерной программы с другими
3	API	В	Название файловой системы, использовавшейся в SCO Unix, System V и некоторых других ранних вариантах Unix.
		Г	Сетевая файловая система, которая позволяет удаленным пользователям обращаться к файлам и директориям на другом компьютере в сети, как если бы они находились на локальном компьютере.

6.Установите соответствие между названием задач алгоритма планирования и его описание

1	Равноправие	А	Минимизация времени, затрачиваемого на ожидание обслуживания и обработку задачи
2	Использование процессора	Б	Поддержка постоянной занятости процессора
3	Время отклика	В	Предоставление каждому процессу справедливой доли процессорного времени
		Г	Быстрая реакция на запросы

7. Установите соответствие между названием условий и его описание

1	Условие взаимного исключения	А	можно исключить, позволяя ОС отнимать у процесса ресурсы
2	Условие ожидания	Б	можно подавить путем разрешения неограниченного разделения ресурсов
3	Условие отсутствия перераспределения	В	можно исключить, предотвращая образование цепи запросов
		Г	можно подавить, предварительно выделяя ресурсы

8. Установите соответствие между названием фреймов и их описанием

1	page frame	А	Диспетчер виртуальной памяти может быстро и относительно легко удовлетворить программные прерывания
2	page fault	Б	Виртуальная страница памяти, отображаемая на физическую страницу
3	Pagefile	В	Содержит объекты, которые могут быть при необходимости выгружены на диск
		Г	Это файл подкачки операционной системы Windows. При нехватке оперативной памяти Windows резервирует определенное место на жестком диске и использует его для увеличения своих возможностей.

9. Установите соответствие между названием реализаций файлов и их описанием

1	Неразрывные файлы	А	Метод отслеживания принадлежности блоков диска файлам заключался в связывании с каждым файлом структуры данных
2	Списки	Б	Простейшей схемой выделения файлам определенных блоков на диске является система, в которой файлы представляют собой наборы последовательных соседних блоков диска
3	Список с индексацией	В	Метод размещения файлов состоит в представлении каждого файла в виде однонаправленного списка блоков диска
		Г	Оба недостатка предыдущей схемы организации файлов в виде списков могут быть устранены, если указатели на следующие блоки хранить не прямо в блоках, а в отдельной таблице, загружаемой в память, элементы которой хранят ссылку на физический блок диска и на элемент таблицы, соответствующий очередному блоку файла

10.Установите соответствие между названием регистров и их описанием

1	Регистр данных	А	Использовался для указания номера цилиндра, с которого необходимо выполнить предкомпенсацию
2	Регистр ошибок	Б	Содержит количество секторов для операции записи или считывания
3	Регистр предкомпенсации	В	Используется при выполнении операций чтения или записи сектора в программном режиме ввода/вывода
		Г	Определяет состояние НЖМД после выполнения операции

11.Установите соответствие между названием методов скрытия дефектов и их описанием

1	Метод резервного сектора	А	При этом методе дорожка содержащая дефект считается нерабочей и "не замечается" контроллером диска
2	Метод резервной дорожки	Б	Суть метода заключается в том, что на каждой дорожке накопителя размещается дополнительный, недоступный в обычном режиме работы, сектор и при обнаружении дефекта в каком-либо рабочем секторе дорожки, вместо него включается резервный
3	Метод пропуска дефектной дорожки	В	Такой метод позволяет исключить всю дорожку при обнаружении на ней дефектов
		Г	Этот метод применим только к накопителям, использующих режим трансляции физических параметров в логические

12.Установите соответствие между названием системных вызовов и их описанием

1	semget	А	для манипулирования значениями семафоров
2	semop	Б	для выполнения разнообразных управляющих операций над набором семафоров
3	semctl	В	для создания и получения доступа к набору семафоров
		Г	запуск новой программы в текущем процессе

13.Установить соответствие технических каналов утечки информации:

1.Прямой акустический (окна, двери, щели, проемы)	. 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
	d. Прослушивание разговоров, ведущихся в помещении без применения технических средств посторонними лицами

Установить соответствие дальности подавления диктофонов:

1.Аналоговые диктофоны	. 5–6 м.
2.Цифровые диктофоны	b. Не более 1,5 м
3.Аналоговые диктофоны в металлическом корпусе	c. 4–5 м
	d. Практически не подавляются

15. Установить соответствие

1.I группа	. 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.
	d. Это специальные устройства, которые обеспечивают бесперебойную передачу данных и сигналов в многопользовательской среде, путем автоматического переключения на наиболее подходящую частоту приема и передачи

16. Установить соответствие:

1.Косвенные каналы	. 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.Полудуплексный канал	c. связанные с доступом к элементам АСОД и изменением структуры компонентов АСОД.
	d. позволяет передавать данные в обоих направлениях, но только в одном направлении за раз.

17. Установить соответствие:

1.Нарушитель	. 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.
	d. Специалист, который занимается поиском и устранением уязвимостей в информационных системах, сетях и приложениях с разрешения их владельцев.

18. Установить соответствие нарушителей по уровням знания АСОД:

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

19.Установить соответствие нарушителей по времени действия:

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

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

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

21. Выберите соответствия для названий стандартных служб и закреплѐн- ных за ними номеров портов:

1.FTP	а)80
2.HTTP	б)21
3.DNS	в)67
4.DHCP	г)53
	д)25

Задания на установление правильной последовательности

1. Установите правильную последовательность этапов оценки рисков в распределенных системах:
a) Идентификация активов и уязвимостей;
b) Оценка уровня угрозы;
c) Оценка вероятности наступления угрозы;
d) Оценка возможных последствий угрозы;
e) Оценка уровня риска;
f) Разработка и реализация мер по управлению рисками.

2. Установите правильную последовательность этапов реализации контроля доступа в распределенных системах:
a) Идентификация пользователей и ресурсов;
b) Аутентификация пользователей и авторизация доступа к ресурсам;
c) Установка прав доступа;
d) Мониторинг доступа;
e) Аудит доступа.

3. Установите правильную последовательность этапов реализации защиты информации в распределенных системах:
a) Оценка уровня угрозы и риска;
b) Разработка и реализация мер по управлению рисками;
c) Использование шифрования данных;
d) Установка мер защиты на уровне операционной системы;
e) Установка мер защиты на уровне приложений.

4. Установите правильную последовательность этапов процесса резервного копирования данных в распределенных системах:
a) Определение частоты создания резервных копий;
b) Определение места хранения резервных копий;
c) Выбор метода резервного копирования;
d) Создание резервных копий;
e) Проверка целостности и доступности резервных копий.

5. Установите правильную последовательность этапов реализации мер по обеспечению физической безопасности в распределенных системах:
a) Идентификация критических зон;
b) Установка систем видеонаблюдения и контроля доступа;
c) Установка физических барьеров;
d) Определение места расположения серверных комнат;
e) Определение места расположения резервных источников питания.

6.Установите правильную последовательность шагов для установки и настройки брандмауэра на сервере, чтобы обеспечить безопасность распределенной системы:
a) Скачать и установить необходимое ПО
b) Настроить правила брандмауэра
c) Запустить брандмауэр и добавить его в автозапуск
d) Протестировать брандмауэр, используя уязвимости, известные для вашей системы
e) Создать резервную копию настроек брандмауэра

7. Установите правильную последовательность действий для защиты распределенной системы от атак, использующих уязвимости веб-приложений:

a) Сканирование веб-приложений на уязвимости
b) Исправление найденных уязвимостей
c) Определение правильных настроек фаервола для предотвращения атак
d) Установка системы обнаружения вторжений
e) Регулярное обновление программного обеспечения системы

8. Установите правильную последовательность действий для обеспечения безопасности данных, передаваемых между узлами распределенной системы:

a) Выбор протокола безопасности передачи данных

b) Установка и настройка сертификатов безопасности
c) Защита паролей и логинов
d) Реализация защиты от атак межсетевого экрана
e) Настройка шифрования данных

9. Установите правильную последовательность действий для защиты распределенной системы от атак на уровне приложений:
a) Сканирование приложений на уязвимости
b) Установка системы обнаружения вторжений
c) Исправление найденных уязвимостей
d) Проверка наличия несанкционированных сценариев веб-приложений
e) Регулярное обновление программного обеспечения системы

10. Установите правильную последовательность действий для обеспечения безопасности распределенной системы при использовании облачных сервисов:
a) Определение рисков использования облачных сервисов
b) Выбор надежного облачного провайдера
c) Настройка управления доступом к данным
d) Настройка механизма резервного копирования
e) Регулярный мониторинг безопасности системы

11. Расставьте действия по установлению безопасной связи между клиентом и сервером:
a) Клиент посылает запрос на подключение к серверу
b) Сервер отправляет клиенту сертификат безопасности
c) Клиент проверяет подлинность сертификата
d) Клиент и сервер обмениваются сеансовым ключом
e) Клиент и сервер начинают обмен данными с использованием сеансового ключа

12. Расставьте действия по обеспечению безопасности данных в распределенной системе:
a) Зашифровать передаваемые данные
b) Аутентифицировать пользователей
c) Ограничить доступ к ресурсам системы на основе ролей и прав
d) Установить межсетевые экраны для блокировки нежелательного трафика
e) Установить обновления безопасности для программного обеспечения системы

13. Расставьте действия по противодействию атаке DDoS на распределенную систему:
a) Определить источник атаки и заблокировать его IP-адрес
b) Установить межсетевые экраны для блокировки входящего трафика

c) Использовать средства для фильтрации трафика и отбраковки подозрительных пакетов

d) Использовать технологии балансировки нагрузки для равномерного распределения трафика по серверам

e) Повысить пропускную способность сети, чтобы выдержать большой объем трафика

14. Установите правильную последовательность действий для обеспечения безопасности в процессе аутентификации пользователей в распределенной системе:

a. Пользователь вводит логин и пароль

b) Система проверяет правильность логина и пароля

c) Система выдает токен для доступа к ресурсам

d) Пользователь получает доступ к ресурсам с помощью токена

15. Установите правильную последовательность действий для защиты данных в распределенной системе:

a) Данные шифруются с помощью алгоритма шифрования

b) Зашифрованные данные передаются по сети

c) Получатель расшифровывает данные с помощью ключа

d) Данные сохраняются в зашифрованном виде на диске

16. Установите правильную последовательность действий для предотвращения атак на распределенную систему:

a) Идентифицирование потенциальных уязвимостей в системе

b) Разработка плана мер по устранению уязвимостей

c) Реализация мер безопасности в системе

d) Мониторинг и обновление мер безопасности в системе

17. Установите правильную последовательность действий для обеспечения физической безопасности распределенной системы:

a) Ограничение доступа к серверной комнате

b) Установка системы видеонаблюдения и контроля доступа

c) Резервное копирование данных

d) Регулярная проверка оборудования и устройств на наличие уязвимостей

18. Установите правильную последовательность действий для обеспечения защиты от внешних атак на распределенную систему:

a. Установка брандмауэра для контроля входящего и исходящего трафика

c. Установка программного обеспечения для обнаружения вредоносных программ

d. Установка системы обнаружения вторжений

e. Регулярное обновление программного обеспечения и операционной системы.

19. Установите последовательность действий для обеспечения безопасности данных в распределенной системе:

a) Разработка политики безопасности
b) Разработка механизмов шифрования данных
c) Установка мер безопасности на всех уровнях системы
d) Создание резервных копий данных
e) Оценка эффективности мер безопасности
f) Регулярное обновление и патчинг системы
g) Обучение пользователей правилам безопасности

20. Установите правильную последовательность действий для мониторинга безопасности в распределенной системе:

a) Разработка политики мониторинга безопасности
b) Установка мониторинговых инструментов на всех уровнях системы
c) Определение критических ресурсов для мониторинга
d) Определение пороговых значений для оповещений о нарушениях безопасности
e) Регулярный анализ и интерпретация данных мониторинга
f) Принятие мер по предотвращению нарушений безопасности

21. Укажите правильную последовательность для столбцов таблицы маршрутизации:

а) IP-адрес следующего по маршруту маршрутизатора;
б) метрика маршрута;
в) адрес сети/подсети/хоста назначения;
г) IP-адрес исходящего порта текущего маршрутизатора;
д) маска подсети назначения.

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. Компания X разрабатывает приложение для хранения и обработки конфиденциальных данных своих клиентов. Какие меры безопасности должны быть предприняты для защиты этих данных? Какие риски могут возникнуть при неправильной реализации мер безопасности?
2. Компания Y использует облачное хранилище для хранения своих данных. Какие меры безопасности должны быть предприняты для защиты данных в облаке? Какие риски могут возникнуть при неправильной реализации мер безопасности?
3. Компания Z использует открытый Wi-Fi для своих сотрудников во время командировок. Какие меры безопасности должны быть предприняты для защиты конфиденциальной информации компании? Какие риски могут возникнуть при неправильной реализации мер безопасности?
4. Компания A рассматривает возможность использования биометрической аутентификации для входа в свою систему. Какие риски могут возникнуть при использовании такого метода аутентификации? Какие меры безопасности должны быть предприняты для защиты данных при использовании биометрической аутентификации?
5. Компания B использует систему виртуальных машин для своих сотрудников. Какие меры безопасности должны быть предприняты для защиты данных в виртуальных машинах? Какие риски могут возникнуть при неправильной реализации мер безопасности?
6. Вы работаете в крупной компании, которая использует распределенную систему для хранения и обработки данных. Один из ваших коллег сообщил вам о том, что он получил письмо от неизвестного отправителя, в котором говорится о возможной утечке конфиденциальной информации из вашей компании. Что вы сделаете в первую очередь, чтобы убедиться в безопасности системы?
7. Ваша компания использует распределенную систему для хранения и обработки данных клиентов. Однако, вы заметили, что произошла утечка некоторой конфиденциальной информации. В результате, несколько клиентов потеряли доверие к вашей компании. Какие меры

вы предпримете, чтобы восстановить доверие клиентов и защитить данные в будущем?

8. Вы работаете в команде, которая отвечает за безопасность распределенной системы вашей компании. Один из ваших коллег предложил изменить пароли для всех пользователей системы раз в месяц. Однако, другой коллега считает, что это неэффективно и может негативно повлиять на производительность. Как вы решите эту ситуацию и какие меры безопасности вы предложите вместо изменения паролей?
9. Ваша компания решила использовать облачные технологии для хранения и обработки данных. Какие меры безопасности вы предложите для защиты данных и обеспечения безопасности в облаке?
10. Ваша компания использует распределенную систему для обработки крупных объемов данных. Какие меры безопасности вы предложите для защиты от DDoS-атак и других угроз, связанных с доступом к системе?
11. Задача на анализ рисков: Вам поручено провести анализ рисков для распределенной системы, состоящей из нескольких серверов, на которых хранится конфиденциальная информация. Какие шаги вы будете предпринимать для выполнения этого задания?
12. Задача на выбор метода шифрования: Вы разрабатываете распределенную систему, которая будет использоваться для передачи конфиденциальной информации. Какой метод шифрования вы выберете и почему?
13. Задача на оценку угроз: Ваша компания использует распределенную систему для хранения и обработки конфиденциальной информации. Какие угрозы могут возникнуть для безопасности этой системы и как можно защититься от них?
14. Задача на выбор аутентификационного метода: Вы разрабатываете распределенную систему, которая будет использоваться несколькими пользователями. Какой метод аутентификации вы выберете и почему?
15. Задача на планирование реагирования на инциденты: Ваша компания использует распределенную систему, которая хранит и обрабатывает конфиденциальную информацию. Как вы спланируете реагирование на возможные инциденты, такие как взлом системы или утечка данных? Какие шаги вы предпримете, чтобы свести к минимуму потенциальный ущерб?
16. Компания X использует распределенную систему для обработки своих данных. Однако, некоторые сотрудники компании заметили, что их персональные данные также обрабатываются в этой системе. Какие меры безопасности необходимо принять для защиты персональных данных при использовании распределенных систем?
17. Компания Y использует распределенную систему для обработки своих финансовых данных. Однако, некоторые сотрудники компании украли логин и пароль от учетной записи администратора, имеющей доступ к

этой системе. Какие меры безопасности необходимо принять для предотвращения таких инцидентов?

18. Компания Z использует распределенную систему для хранения и обработки своих клиентских данных. Однако, система была атакована злоумышленниками, которые украли большое количество этих данных. Какие меры безопасности необходимо принять, чтобы избежать подобных инцидентов в будущем?
19. Компания A использует распределенную систему для обработки своих данных. Однако, некоторые сотрудники компании заметили, что их персональные данные также обрабатываются в этой системе. Какие законодательные нормы необходимо учитывать при обработке персональных данных в распределенных системах?
20. Компания B использует распределенную систему для хранения и обработки своих финансовых данных. Однако, некоторые сотрудники компании заметили, что данные на серверах, находящихся в другой стране, не зашифрованы. Какие меры безопасности необходимо принять для защиты данных при использовании распределенных систем в других странах?
21. Компания решила перевести свою ИТ-инфраструктуру в облако. Какие меры безопасности необходимо принять для защиты данных компании?
22. Разработчик написал код для распределенной системы, однако забыл установить защиту от DDoS-атак. Что следует сделать, чтобы избежать таких атак?
23. Компания хочет сократить расходы на безопасность распределенной системы. Какие меры безопасности можно опустить, чтобы сэкономить деньги, и какие меры необходимо сохранить в любом случае?
24. В компании имеется несколько серверов, расположенных в разных странах. Какие меры безопасности необходимо принять, чтобы защитить данные, хранящиеся на этих серверах?
25. Разработчик написал код для распределенной системы, однако забыл установить защиту от внедрения вредоносного кода. Что следует сделать, чтобы избежать такой угрозы?
26. Компания хочет использовать блокчейн-технологии для хранения данных. Какие меры безопасности необходимо принять, чтобы защитить данные, хранящиеся на блокчейн-платформе?
27. Разработчик написал код для распределенной системы, однако забыл установить защиту от SQL-инъекций. Что следует сделать, чтобы избежать такой угрозы?
28. Компания использует открытый исходный код для своей распределенной системы. Какие меры безопасности необходимо принять, чтобы защитить систему от уязвимостей в коде с открытым исходным кодом?
29. Разработчик написал код для распределенной системы, однако забыл установить защиту от фишинг-атак. Что следует сделать, чтобы избежать такой угрозы?

30. Компания хочет использовать мультифакторную аутентификацию для своей распределенной системы. Какие меры безопасности необходимо принять, чтобы защитить данные, используемые для мультифакторной аутентификации?

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.