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 информации в телекоммуникационных сетях
(наименование учебной дисциплины)

10.05.02 Информационная безопасность телекоммуникационных систем, направленность (профиль) «Управление безопасностью телекоммуникационных систем и сетей»
(код и наименование ОПОП ВО)

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ.

Тема 1. Проблемы информационной безопасности автоматизированных сетей.

1. Что стандартизирует модель ISO/OSI OSI?
2. Каково назначение стека протоколов TCP/IP?
3. В чем состоит проблема безопасности IP – сетей?
4. На каком уровне модели OSI работает коммутатор?
5. К какому уровню модели OSI относится формирование сетевых пакетов установленного вида?

Тема 2. Политика безопасности.

1. В чем сущность политики безопасности?
2. Что включает верхний уровень политики безопасности?
3. Какие компоненты входят в структуру политики безопасности организации?
4. Назовите основные этапы разработки политики безопасности организации.
5. Дайте определение «специализированной политики безопасности»

Тема 3. Технологии аутентификации.

1. Раскройте понятие «аутентификация»
2. Дайте определение «авторизации»
3. Что такое администрирование действий пользователей?
4. Как происходит аутентификация на основе PIN-кода?
5. Назовите функции средств аутентификации.

Тема 4. Технологии межсетевых экранов.

1. Перечислите виды межсетевых экранов.
2. Назовите функции межсетевых экранов.
3. Раскройте принцип трансляции сетевых адресов.
4. Как происходит функционирование пакетного фильтра?
5. Какие существуют проблемы безопасности межсетевых экранов?

Тема 5. Технологии защиты от вирусов.

1. Что представляют собой компьютерные вирусы?
2. Чем отличаются файловые вирусы от загрузочных?
3. Назовите причины опасности макровирусов.
4. Какие можно применять методы защиты от компьютерных вирусов?
5. Назовите способы распространения вредоносных программ?

Тема 6. Технологии анализа защищенности и обнаружения сетевых атак.

1. Что такое сетевая атака?
2. В чем состоит технология анализа защищенности?
3. Функции межсетевых экранов нового поколения (NGFW)?
4. Какие уровни входят в концепцию адаптивного управления безопасностью?
5. Какие есть средства анализа защищенности сетевых протоколов?

Тема 7. Требования к системам защиты информации.

1. Дайте определение системе защиты информации.
2. Перечислите классы защищенности автоматизированных систем.
3. Какие существуют особенности защиты информации при работе с системами управления базами данных?
4. Как обеспечить безопасность информации на рабочем месте пользователя ПК?
5. Назовите основные требования к информационной безопасности.

Тема 8. Аудит безопасности информационных систем.

1. Дайте определение аудита безопасности.
2. Каков порядок проведения аудита безопасности?
3. Какой существует порядок планирования процедуры аудита?
4. Какие есть методы сбора информации для аудита?
5. Дайте характеристику основным подходам к анализу данных аудита.

Тема 9. Разработка и защита Web-сайтов.

1. Дайте понятие web-сайта.
2. Каковы основы языка разметки документов HTML?
3. Из чего состоит HTML документ?
4. Как происходит форматирование текста в HTML документе?
5. Какие есть функции в языке программирования JavaScript?

Критерии оценки:

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

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

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

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ЛАБОРАТОРНЫХ РАБОТ

Лабораторная работа №1 «Разработка обзорного документа по сертифицированным продуктам в заданной области информационной безопасности»

1. Как проводится сертификация средств защиты информации?
2. Что показывают характеристики данного средства защиты?
3. Какой регулятор контролирует данную область информационной безопасности?
4. Какая основная информация содержится в сертификате?
5. Назначение средств защиты информации от несанкционированного доступа?
6. Для чего предназначены средства контроля защищенности?
7. Для чего предназначены средства резервного копирования?

Лабораторная работа №2 «Создание сайтов на языке JavaScript и обеспечение их информационной безопасности»

1. Какой способ компиляции языка JavaScript?
2. Какие утилиты для статического анализа в JavaScript?
3. Какие утилиты для динамического анализа в JavaScript?
4. Как узнать JavaScript-кода web-страницы?
5. Как подключить JavaScript-файл к web-странице?
6. Что означает (values)?
7. Что означает (typeof)?

Лабораторная работа №3 «Разработка и защита Web-приложений с серверными сценариями на языке PHP»

1. Какие типы переменных поддерживает язык PHP??
2. В чем отличие php-страницы от html-страницы?
3. Как передать переменную в php-страницу?
4. Какие параметры существуют у функции date()?
5. Для чего используется функция isset()?
6. Каким образом происходит инициализация массивов в языке PHP?
7. Каким образом в языке PHP происходит обращение к элементам массивов и ассоциативных массивов?

Лабораторная работа №4 «Менеджер паролей: программа Password Commander»

1. Объясните, что такое аккаунт в программе Password Commander?

2. Для какой цели используются группы в программе Password Commander?
3. Какие поля по умолчанию используются в записях?
4. Какие типы паролей можно создавать с помощью генератора паролей?
5. В каком виде хранятся пароли в программе Password Commander по умолчанию?
6. Объясните, что такое пасскарта в программе Password Commander?
7. Приведите примеры программ, предназначенных для хранения паролей?

Лабораторная работа №5 «Фаервол Comodo Firewall»

1. Существуют две политики работы межсетевого экрана: «запрещено все, что явно не разрешено», «разрешено все, что явно не запрещено». Объясните, каковы их плюсы и минусы.
2. Каким образом можно выполнить блокирование порта с определенным номером с помощью фаервола Comodo Firewall?
3. Каким образом можно уменьшить количество информационных сообщений с помощью настроек Comodo Firewall?
4. Возможна ли конфликтная ситуация между Comodo Firewall и другими фаерволами?
5. Каким образом в фаерволе Comodo Firewall можно ограничить доступ программ в сеть Интернет?
6. Дайте определение межсетевого экрана
7. Каким образом можно уменьшить количество информационных сообщений с помощью настроек Comodo Firewall?

Лабораторная работа №6 «Антивирусная программа: Kaspersky Internet Security»

1. Какие настройки есть в окне параметров Kaspersky Internet Security?
2. Перечислите типы уведомлений, в зависимости от степени важности события с точки зрения безопасности компьютера.
3. Как включить защиту для сетевого экрана?
4. Как выключить мониторинг уязвимости?
5. Какие четыре системные задачи с заранее определённым набором проверяемых объектов создает по умолчанию Kaspersky Internet Security?
6. Каково назначение программы Kaspersky Internet Security?
7. Назовите компоненты, задачи и другие составляющие в левой части окна Kaspersky Internet Security.

Критерии оценки:

5 баллов (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные

определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

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

2-1 балла (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

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

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

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

2. На сколько уровней модель OSI разделяет коммуникационные функции:

(1) семь

(2) восемь

(3) пять

3. Какие задачи выполняют уровни OSI в процессе передачи данных по сети:

(1) уровни выполняют одинаковые задачи, постоянно повторяя передающие сигналы по сети

(2) каждый уровень выполняет свою определенную задачу

(3) первых три уровня выполняют одинаковые задачи, последующие выполняют определенные задачи

4. Выбрать правильное расположение уровней модели OSI от 7 до 1:

(1) прикладной, канальный, представления, сеансовый, транспортный, сетевой, физический

(2) представления, прикладной, сеансовый, транспортный, сетевой, канальный, физический

(3) прикладной, представления, сеансовый, транспортный, сетевой, канальный, физический

5. Верно ли утверждение: «Каждый уровень модели выполняет свою функции. Чем выше уровень, тем более сложную задачу он решает»:

(1) верно

(2) не верно

6. На базе протоколов, обеспечивающих механизм взаимодействия программ и процессов на различных машинах, строится:

(1) горизонтальная модель

(2) вертикальная модель

(3) сетевая модель

7. Какой уровень представляет собой набор интерфейсов, позволяющим получить доступ к сетевым службам:

(1) представления

(2) прикладной

(3) сеансовый

8. Какой уровень обеспечивает контроль логической связи и контроль доступа к среде:

(1) представления

(2) прикладной

(3) канальный

9. Какой уровень обеспечивает битовые протоколы передачи информации:

(1) физический

(2) канальный

(3) транспортный

10. Основными элементами модели OSI являются:

(1) уровни, прикладные процессы и физические средства соединения

(2) уровни и прикладные процессы

(3) уровни

11. Единицей информации канального уровня являются:

(1) сообщения

(2) потоки

(3) кадры

12. Согласно этому протоколу передаваемое сообщение разбивается на пакеты на отправляющем сервере и восстанавливается в исходном виде на принимающем сервере:

(1) TCP

(2) IP

(3) WWW

13. Доставку каждого отдельного пакета до места назначения выполняет протокол:

(1) TCP

(2) IP

(3) HTTPS

14. Какие функции выполняет протокол IP

(1) маршрутизация

(2) коррекция ошибок

(3) установка соединения

15. Какой уровень управляет потоками данных, преобразует логические сетевые адреса и имена в соответствующие им физические:

(1) сетевой

(2) представительский

(3) транспортный

16. Подтверждение подлинности взаимодействующих объектов обеспечивает:

(1) аутентификация

(2) конфиденциальность

(3) контроль доступа

17. Защиту от несанкционированного использования ресурсов обеспечивает:

(1) контроль доступа

(2) конфиденциальность

(3) аутентификация

18. Цифровая подпись – это:

(1) способ введения электронной метки для файла данных

(2) сведения о пользователе помещаемые в файл

3) файл, подтверждающий ваши права

(4) идентификатор документа

19. К механизмам безопасности относят:

(1) алгоритмы симметричного шифрования

(2) невозможность отказа от полученного сообщения

(3) целостность сообщения

(4) хэш-функции

20. Совокупность аппаратных, программных и специальных компонент вычислительной системы, реализующих функции защиты и обеспечения безопасности это:

(1) политика безопасности (Security Policy)

(2) ядро безопасности (Trusted Computing Base, TCB)

(3) модель безопасности (Security Model)

(4) идентификация (Identification)

21. Специальный нормативный документ, представляющий собой совокупность задач защиты, функциональных требований, требований адекватности, общих спецификаций средств защиты и их обоснования. В ходе квалификационного анализа служит описанием информационного продукта:

(1) профиль защиты

(2) проект защиты

(3) задачи защиты

(4) круг защиты

22. Потенциальные угрозы, определяющие задачи защиты информации в сетях:

(1) прослушивание каналов

(2) внедрение сетевых вирусов

(3) умышленное уничтожение или искажение информации

(4) выход из строя операционной системы

23. Что представляет собой запись и последующий анализ всего проходящего потока сообщений

(1) прослушивание каналов

(2) контроль доступа

(3) аутентификация

(4) аудит

24. К сервисам безопасности относят:

(1) идентификация/аутентификация

(2) протоколирование/аудит

(3) шифрование

(4) аудит

25. Какое управление доступом, осуществляемое на основании заданного администратором множества разрешенных отношений доступа.

(1) мандатное управление доступом (Mandatory Access Control)

(2) дискреционное управление доступом (Discretionary Access Control)

(3) прямое взаимодействие (Trusted Path)

(4) идентификация (Identification)

26. Что представляет собой управление доступом, основанное на совокупности правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов:

(1) дискреционное управление доступом (Discretionary Access Control)

(2) мандатное управление доступом (Mandatory Access Control)

(3) модель безопасности (Security Model)

(4) идентификация (Identification)

27. Что представляет собой предотвращение пассивных атак для передаваемых или хранимых данных:

(1) конфиденциальность

(2) контроль доступа

(3) аутентификация

28. Активные угрозы становятся видимыми на уровне (модели OSI):

(1) транспортном

(2) физическом

(3) канальном

(4) сетевом

29. Что представляет собой совокупность норм и правил, обеспечивающих эффективную защиту системы обработки информации от заданного множества угроз безопасности:

(1) модель безопасности (Security Model)

(2) ядро безопасности (Trusted Computing Base, TCB)

(3) политика безопасности (Security Policy)

(4) прямое взаимодействие (Trusted Path)

30. Что представляет собой принцип организации информационного взаимодействия, гарантирующий, что передаваемая информация НЕ подвергнется перехвату или искажению:

(1) мандатное управление доступом (Mandatory Access Control)

(2) политика безопасности (Security Policy)

(3) прямое взаимодействие (Trusted Path)

(4) идентификация (Identification)

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

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

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

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

32. Виды информационной безопасности:

(1) персональная, корпоративная, государственная

(2) клиентская, серверная, сетевая

(3) локальная, глобальная, смешанная

33. Цели информационной безопасности – своевременное обнаружение, предупреждение:

(1) несанкционированного доступа, воздействия в сети

(2) инсайдерства в организации

(3) чрезвычайных ситуаций

34. Основные объекты информационной безопасности:

(1) компьютерные сети, базы данных

(2) информационные системы, психологическое состояние пользователей

(3) бизнес-ориентированные, коммерческие системы

35. Основными рисками информационной безопасности являются:

(1) искажение, уменьшение объема, перекодировка информации

(2) техническое вмешательство, выведение из строя оборудования сети

(3) потеря, искажение, утечка информации

36. К основным принципам обеспечения информационной безопасности относится:

(1) экономической эффективности системы безопасности

(2) многоплатформенной реализации системы

(3) усиления защищенности всех звеньев системы

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

(1) установление регламента, аудит системы, выявление рисков

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

(3) внедрение аутентификации, проверки контактных данных пользователей

38. Принципом информационной безопасности является принцип недопущения:

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

(2) рисков безопасности сети, системы

(3) презумпции секретности

39. Принципом политики информационной безопасности является принцип:

(1) невозможности миновать защитные средства сети (системы)

(2) усиления основного звена сети, системы

(3) полного блокирования доступа при риск-ситуациях

40. Принципом политики информационной безопасности является принцип:

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

(2) перехода в безопасное состояние работы сети, системы

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

41. Принципом политики информационной безопасности является принцип:

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

(2) одноуровневой защиты сети, системы

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

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

(1) компьютерный сбой

(2) логические закладки («мины»)

(3) аварийное отключение питания

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

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

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

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

44. Принцип Кирхгофа:

(1) секретность ключа определена секретностью открытого сообщения

(2) секретность информации определена скоростью передачи данных

(3) секретность закрытого сообщения определяется секретностью ключа

45. ЭЦП – это:

(1) электронно-цифровой преобразователь

(2) электронно-цифровая подпись

(3) электронно-цифровой процессор

46. Наиболее распространены угрозы информационной безопасности корпоративной системы:

(1) покупка нелицензионного ПО

(2) ошибки эксплуатации и неумышленного изменения режима работы системы

(3) сознательного внедрения сетевых вирусов

47. Наиболее распространены угрозы информационной безопасности сети:

(1) распределенный доступ клиент, отказ оборудования

(2) моральный износ сети, инсайдерство

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

48. Наиболее распространены средства воздействия на сеть офиса:

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

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

(3) компьютерные сбои, изменение администрирования, топологии

49. Утечкой информации в системе называется ситуация, характеризуемая:

(1) потерей данных в системе

(2) изменением формы информации

(3) изменением содержания информации

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

(1) целостность

(2) доступность

(3) актуальность

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

(1) вероятное событие

(2) детерминированное (всегда определенное) событие

(3) событие, происходящее периодически

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

(1) регламентированной

(2) правовой

(3) защищаемой

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

(1) программные, технические, организационные, технологические

(2) серверные, клиентские, спутниковые, наземные

(3) личные, корпоративные, социальные, национальные

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

(1) владелец сети

(2) администратор сети

(3) пользователь сети

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

(1) руководств, требований обеспечения необходимого уровня безопасности

(2) инструкций, алгоритмов поведения пользователя в сети

(3) нормы информационного права, соблюдаемые в сети

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

(1) аудит, анализ затрат на проведение защитных мер

(2) аудит, анализ безопасности

(3) аудит, анализ уязвимостей, риск-ситуаций

57. Что такое компьютерный вирус?

(1) прикладная программа

(2) системная программа

(3) программа, выполняющая на компьютере несанкционированные действия

(4) база данных.

58. Основные типы компьютерных вирусов:

(1) аппаратные, программные, загрузочные

(2) программные, загрузочные, макровирусы

(3) файловые, программные, макровирусы

59. Этапы действия программного вируса:

(1) размножение, вирусная атака

(2) запись в файл, размножение

(3) запись в файл, размножение, уничтожение программы

60. В чем заключается размножение программного вируса?

(1) программа-вирус один раз копируется в теле другой программы

(2) вирусный код неоднократно копируется в теле другой программы

61. Что называется вирусной атакой?

(1) неоднократное копирование кода вируса в код программы

(2) отключение компьютера в результате попадания вируса

(3) нарушение работы программы, уничтожение данных, форматирование жесткого диска

62. Какие существуют методы реализации антивирусной защиты?

(1) аппаратные и программные

(2) программные и административные

(3) только программные

63. Какие существуют основные средства защиты данных?

(1) резервное копирование наиболее ценных данных

(2) аппаратные средства

(3) программные средства

64. Какие существуют вспомогательные средства защиты?

(1) аппаратные средства

(2) программные средства

(3) административные методы и антивирусные программы

65. На чем основано действие антивирусной программы?

(1) на ожидании начала вирусной атаки

(2) на сравнении программных кодов с известными вирусами

(3) на удалении зараженных файлов

66. Какие программы относятся к антивирусным:

(1) AVP, DrWeb, Norton AntiVirus

(2) MS-DOS, MS Word, AVP

(3) MS Word, MS Excel, Norton Commander

67. Утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами:

(1) руткит

(2) бэкап

(3) камбэк

68. Компьютерные вирусы:

(1) файлы, которые невозможно удалить

(2) программы, способные к саморазмножению (самокопированию)

(3) файлы, имеющие определенное расширение

69. DDos — программы:

(1) реализуют атаку с одного компьютера с ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера

(2) оба варианта верны

(3) реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров

70. Отличительными способностями компьютерного вируса являются:

(1) способность к самостоятельному запуску и многократному копированию кода

(2) значительный объем программного кода

(3) легкость распознавания

71. DoS — программы:

(1) реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров

(2) оба варианта верны

(3) реализуют атаку с одного компьютера с ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера

72. Компьютерные вирусы:

(1) являются следствием ошибок в операционной системе

(2) пишутся людьми специально для нанесения ущерба пользователем ПК

(3) возникают в связи со сбоями в аппаратных средствах компьютера

73. Троянские программы бывают:

(1) сетевые программы

(2) программы передачи данных

(3) программы – шпионы

74. Основная масса угроз информационной безопасности приходится на:

(1) троянские программы

(2) шпионские программы

(3) черви

75. Троянская программа, троянец:

(1) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей

(2) являются вредоносными программами, которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы

(3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам

76. Информационная безопасность зависит от:

(1) компьютеров, поддерживающей инфраструктуры

(2) пользователей

(3) информации

77. Сетевые черви бывают:

(1) Web-черви

(2) черви операционной системы

(3) черви MS Office

78. Таргетированная атака – это:

(1) атака на сетевое оборудование

(2) атака на компьютерную систему крупного предприятия

(3) атака на конкретный компьютер пользователя

79. Сетевые черви бывают:

(1) почтовые черви

(2) черви операционной системы

(3) черви MS Office

80. Stuxnet – это:

(1) троянская программа

(2) макровирус

(3) промышленный вирус

81. По «среде обитания» вирусы можно разделить на:

(1) загрузочные

(2) очень опасные

(3) опасные

82. Какие вирусы активизируются в самом начале работы с операционной системой:

(1) загрузочные вирусы

(2) троянцы

(3) черви

83. По «среде обитания» вирусы можно разделить на:

(1) не опасные

(2) очень опасные

(3) файловые

84. Какие угрозы безопасности данных являются преднамеренными:

(1) ошибки персонала

(2) открытие электронного письма, содержащего вирус

(3) не авторизованный доступ

85. По «среде обитания» вирусы можно разделить на:

(1) опасные

(2) не опасные

(3) макровирусы

86. Под какие системы распространение вирусов происходит наиболее динамично:

(1) Windows

(2) Mac OS

(3) Android

87. Макровирусы:

(1) существуют для интегрированного офисного приложения Microsoft Office

(2) эти вирусы различными способами внедряются в исполнимые файлы и обычно активизируются при их запуске

(3) заражают загрузочный сектор гибкого или жёсткого диска

88. Какой вид идентификации и аутентификации получил наибольшее распространение:

(1) системы PKI

(2) постоянные пароли

(3) одноразовые пароли

89. Файловые вирусы:

(1) заражают загрузочный сектор гибкого или жёсткого диска

(2) существуют для интегрированного офисного приложения Microsoft Office

(3) эти вирусы различными способами внедряются в исполнимые файлы и обычно активизируются при их запуске

90. Для периодической проверки компьютера на наличие вирусов используется:

(1) компиляция

(2) антивирусное сканирование

(3) дефрагментация диска

91. Антивирусный сканер запускается:

(1) автоматически при старте операционной системы и работает в качестве фонового системного процессора, проверяя на вредоносность совершаемые другими программами действия

(2) оба варианта верны

(3) по заранее выбранному расписанию или в произвольный момент пользователем. Производит поиск вредоносных программ в оперативной памяти, а также на жестких и сетевых дисках компьютера

92. Как называется вирус, попадающий на компьютер при работе с электронной почтой:

(1) текстовый

(2) сетевой

(3) файловый

93. Антивирусный монитор запускается:

(1) автоматически при старте операционной системы и работает в качестве фонового системного процессора, проверяя на вредоносность совершаемые другими программами действия. Основная задача состоит в обеспечении максимальной защиты от вредоносных программ при минимальном замедлении работы компьютера

(2) по заранее выбранному расписанию или в произвольный момент пользователем. Производит поиск вредоносных программ в оперативной памяти, а также на жестких и сетевых дисках компьютер

(3) оба варианта верны

94. К категории компьютерных вирусов не относятся:

(1) загрузочные вирусы

(2) файловые вирусы

(3) type-вирусы

95. Выберите тип вредоносных программ:

(1) шпионское, рекламное программное обеспечение

(2) Microsoft Office

(3) операционная система Linux

96. Выберите тип вредоносных программ:

(1) Microsoft Office

(2) вирусы, черви, троянские и хакерские программы

(3) операционная система Windows

97. Как называют схему страницы, на которой представлены элементы, имеющиеся на страницах сайта:

(1) матрица

(2) шаблон

(3) фундамент

98. Чтобы отличать теги от текста, их заключают в:

(1) круглые скобки

(2) угловые скобки

(3) фигурные скобки

99. Проектированием структуры web-сайта занимается:

(1) web-программист

(2) провайдер

(3) web-дизайнер

100. Сайт можно создать, воспользовавшись:

(1) языком программирования Си

(2) языком программирования Паскаль

(3) языком разметки гипертекста HTML

Задания в открытой форме

1) … – концептуальная модель, которая характеризует и стандартизирует коммуникационные функции телекоммуникационной или вычислительной системы без учета ее внутренней структуры и технологии.
2) … – сетевая модель, описывающая процесс передачи цифровых данных.
3) … – массовая рассылка корреспонденции рекламного характера лицам, не выражавшим желания её получить.
4) ... – процедура скрытного перенаправления жертвы на ложный IP-адрес.
5) ... – совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от определенного множества угроз и составляет необходимое условие безопасности системы.
6) … – уровень выносится управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.
7) … – разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников.
8) … – программные средства контроля доступа в систему, используемые для защиты уязвимой информации и программных средств.
9) … – процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно определяющий этого субъекта в информационной системе.

10) … – процедура проверки подлинности, например проверка подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных.
11) … – предоставление определенному лицу или группе лиц прав на выполнение определенных действий.
12) … – всестороннее обследова-ние, позволяющее оценить текущее состояние информационной безопасно-сти организации и спланировать дальнейшие шаги по повышению уровня защищенности.
13) … – основная функция систем межсетевых экранов (или брандмауэров), которая позволяет сетевому администратору распределить пользователям как доступ из внешней сети к службам компьютеров, находя-щимся внутри сети предприятия, или к защищенному сегменту сети, так и доступ пользователей из внутренней сети к соответствующим ресурсам внешней сети.
14) … – программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.
15) … – компьютерный вирус, записывающийся в первый сектор гибкого или жесткого диска и выполняющийся при загрузке компьютера.
16) … – разновидность вредоносной программы, проникающая в компьютер под видом легитимного программного обеспечения, в отличие от вирусов и червей, которые распространяются самопроизвольно.
17) … – вторжение в операционную систему удаленного компьютера.
18) … – степень адекватности реализованных в ней механизмов защиты информации существующим в данной среде функционирования рискам, связанным с осуществлением угроз безопасности информации.
19) … – возможность нарушения таких свойств информации, как конфиденциальность, целостность и доступность.
20) … – стандартизированный язык гипертекстовой разметки документов для просмотра веб-страниц в браузере.
21) … – мультипарадигменный язык программирования. Поддерживает объектно-ориентированный, императивный и функциональный стили.

Задание на установление соответствия

1. Установить соответствие:

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

2. Установить соответствие:

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

3. Установить соответствие нарушителей по уровням знания АСОД:

1) Физический уровень	a) Пересылаются не биты, а целые сообщения (кадры, фреймы).
2) Канальный уровень	b) Обеспечивает ссогласование различий в разных технологиях канального уровня и общая адресация с помощью глобальных адресов, позволяющих однозначно определить компьютер в сети.
3) Сетевой уровень	c) Следит за доставкой пакетов, отправляя и анализируя соответствующие подтверждения, нумеруют пакеты и расставляют их в нужном порядке после получения
4) Транспортный уровень	d) Происходит преобразование битов информации в сигналы, которые затем передаются по среде. Используемый физический протокол зависит от того, каким образом компьютер подключен к сети.

4. Установить соответствие нарушителей по времени действия:

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

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

1) 1 уровень	a) Применяющие пассивные средства (технические средства перехвата без модификации компонентов системы).
2) 2 уровень	b) Применяющие только агентурные методы

	получения сведений
3) 3 уровень	c) Использующие только штатные средства и недостатки системы защиты, их сильные и слабые стороны.
4) 4 уровень	d) Применяющие методы и действия активного воздействия (модификация и подключение дополнительных технических устройств).

6. Установить соответствие:

1) Угроза безопасности	a) Это некая неудачная характеристика системы, которая делает возможным возникновение угрозы.
2) Уязвимость	b) Это угроза раскрытия информации.
3) Атака	c) Это потенциально возможное происшествие, которое может оказать воздействие на информацию в системе.
4) Угроза конфиденциальности	d) Это действие по использованию уязвимости; реализация угрозы.

7. Установить соответствие:

1) Линейная структура процесса вычислений	a) Предполагает, что для получения результата некоторые действия необходимо выполнить несколько раз.
2) Разветвленная структура процесса вычислений	b) Предполагает, что конкретная последовательность операций зависит от значений одной или нескольких переменных.
3) Циклическая структура процесса вычислений	c) Предполагает, что для получения результата необходимо выполнить некоторые операции в определенной последовательности.

8. Установить соответствие:

1) Правильность	a) Возможность проверки получаемых результатов
2) Универсальность	b) Обеспечение полной повторяемости результатов, т. е. обеспечение их правильности при наличии различного рода сбоев
3) Надежность	c) Обеспечение правильной работы при любых допустимых данных и защиты от неправильных данных;
4) Проверяемость	d) Функционирование в соответствии с техническим заданием

9. Установить соответствие:

1) Точность результатов	a) Возможность совместного функционирования с некоторым оборудованием
2) Защищенность	b) Возможность совместного функционирования с другим программным обеспечением
3) Программная совместимость	c) Обеспечение конфиденциальности информации
4) Аппаратная совместимость	d)Обеспечение погрешности результатов не выше заданной;

10. Установить соответствие средства обеспечения информационной безопасности:

1)Организационные	a)Сюда входит весь перечень программного обеспечения, который поможет обеспечить должную информационную безопасность ресурса
2) Программные	b)Сюда входят сами приборы и устройства, которые обеспечивают защиту информации.
3) Аппаратные	c) Сюда входят: обеспечение качественного помещения для размещения серверов, качественное оборудование, продуманная кабельная система, организация правового статуса ресурса или компании и др.

11. Установить соответствие:

1)Угроза целостности	a)Это вероятный ущерб, который зависит от защищенности системы.
2)Угроза доступности	b)Это стоимость потерь, которые понесет компания в случае реализации угрозы конфиденциальности, целостности или доступности по каждому виду ценной информации.
3)Ущерб	c)Это угроза нарушения работоспособности системы при доступе к информации.
4)Риск	d)Это угроза изменения информации.

12. Установить соответствие:

1) Шифр	a) Это любой знак, в том числе буква, цифра или знак препинания.
2) Символ	b) Совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты.

3) Алфавит	c) Конечное множество используемых для кодирования информации символов.

13. Установить соответствие:

1)Ключ	a) Можно использовать для обратимого изменения текста сообщения с целью сделать его непонятным для всех, кроме тех, кому оно предназначено.
2)Шифрсистема	b)Информация, необходимая для шифрования и расшифрования сообщений.
3)Криптостойкость	c) Характеристика шифра, определяющая его защиту к дешифрованию без знания ключа.

14. Установить соответствие:

1) Шифр замены	a) Группа методов шифрования подстановкой, в которых для замены символов исходного текста используется не один, а несколько алфавитов по определенному правилу.
2) Шифр многоалфавитной замены	b)Основан на том, что символы исходного текста, обычно разделенные на блоки и записанные в одном алфавите, заменяются одним или несколькими символами другого алфавита в соответствии с принятым правилом преобразования.
3) Шифр перестановки	c) Основан на том, что входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов.
4) Шифр простой (или одноалфавитной) замены	d)Группа методов шифрования, которые сводятся к созданию по определённому алгоритму таблицы шифрования, в которой для каждой буквы открытого текста существует единственная сопоставленная ей буква шифртекста.

15. Установить соответствие:

1)Аутентификация	a) процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно определяющий этого субъекта в информационной системе
2)Авторизация	b) процедура проверки подлинности, например проверка подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных.

3)Идентификация	c) предоставление определенному лицу или группе лиц прав на выполнение определенных действий.

16. Установить соответствие:

1) Сеансовый уровень	a) Отвечает за преобразование протоколов и кодирование/декодирование данны
2) Уровень представления данных	b) То, с чем взаимодействуют пользователи, своего рода графический интерфейс всей модели OSI, с другими он взаимодействует по минимуму.
3) Прикладной уровень	c) Управляет взаимодействием между приложениями, открывает возможности синхронизации задач, завершения сеанса, обмена информации

18. Установить соответствие:

1) HTML	a) Высокоуровневый язык программирования, который поддерживает императивный, функциональный, событийно-ориентированный и другие подходы.
2) JavaScript	b) Высокоуровневый язык программирования общего назначения с динамической строгой типизацией и автоматическим управлением памятью, ориентированный на повышение производительности разработчика, читаемости кода и его качества, а также на обеспечение переносимости написанных на нём програм
3) Python	c) Стандартизированный язык гипертекстовой разметки документов для просмотра веб-страниц в браузере

19. Установить соответствие:

1)TCP/IP	a) Набор протоколов, который задает стандарты связи между компьютерами и содержит подробные соглашения о маршрутизации и межсетевом взаимодействии.
2)FTP	b) Протокол прикладного уровня для передачи гипертекста
3) HTTP	c) Протокол, относящийся к прикладному уровню и отвечающий за передачу данных между двумя системами.

20. Установить соответствие:

1) Дискреционный принцип контроля доступа	a) Механизм восстановления параметров разграничения доступа при сбоях и отказах оборудования. С этой целью ведется две копии базы данных, в которой хранятся настройки системы защиты. Вторая копия базы данных обновляется каждый раз при завершении работы пользователей. Если при входе в систему первая копия базы данных оказывается разрушенной, то система защиты автоматически использует вторую копию и при этом восстанавливает первую.
2) Мандатный принцип контроля доступа	b) Разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений субъектам на обращение к информации такого уровня конфиденциальности.
3) Очистка памяти	c) Предполагает назначение каждому объекту списка контроля доступа, элементы которого определяют права доступа к объекту конкретных пользователей или групп.

21. Установить соответствие:

1) Уровень системы управления базами данных	a) Отвечает за взаимодействие с пользователем
2) Уровень прикладного программного обеспечения	b) Отвечает за хранение и обработку данных информационной системы.
3) Уровень операционной системы	c) Отвечает за взаимодействие узлов информационной системы
4) Уровень сети	d) Отвечает за обслуживание СУБД и прикладного программного обеспечения.

Задания на установление правильной последовательности

1. Установить в порядке увеличения единицы измерения количества информации:
1. 1 ТБ

2. 30 Гбайт
3. 50 Килобайт
4. 100 Мегабайт

2. Установить в порядке убывания единицы измерения памяти:
1. 2 байта
2. 4 байта
3. 3 бита
4. 1 байт

3. Установить этапы разработки программного обеспечения:
1. Разработка алгоритма
2. Написание программы
3. Постановка задачи
4. Разработка математической модели

4. Установить в порядке возрастания функциональных возможностей:
1. WordPad
2. Блокнот
3. Microsoft Office Word
4. Corel Ventura Publisher

5. Установить этапы разработки модели:
1. Построение модели
2. Объект
3. Корректировка модели
4. Анализ результатов
5. Исследование модели на компьютере

6. 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

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 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

11. 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

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 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

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 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»

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

17. Выберите правильную последовательность этапов построения политики безопасности:
1. Выбор и установка средств защиты;
2. Организация обслуживания по вопросам информационной безопасности;
3. Создание системы периодического контроля информационной безопасности

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

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

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

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

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

Максимальный балл за тестирование представляет собой разность двух чисел: максимального балла по промежуточной аттестации для данной

формы обучения (36) и максимального балла за решение компетентностно-ориентированной задачи (6).

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

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

Соответствие 100-балльной и 5-балльной шкал

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

2.2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

Компетентностно-ориентированная задача № 1

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

Компетентностно-ориентированная задача № 2

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).

Компетентностно-ориентированная задача № 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.

Компетентностно-ориентированная задача № 4

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

Компетентностно-ориентированная задача № 5
Файловый архив емкостью 412 Мб скачивается 20 минут. Соответствует ли действительности заявленная скорость провайдера в 35 Мбит/с.

Компетентностно-ориентированная задача № 6
Пусть исходный алфавит содержит следующие символы: АБВГДЕВЖЗИЙКЛМНОПРСТУФХИЧШЩЬЫЬЭЮЯ.

Зашифруйте с помощью шифра Вижинера и ключа ЯБЛОКО слово ПОДСТАНОВКА.

Компетентностно-ориентированная задача № 7
Решить уравнение $221x \equiv 111 \pmod{360}$

Компетентностно-ориентированная задача № 8
Определите ключи шифра Цезаря, если известны следующая пара открытый текст — шифротекст: ВИНОГРАД — ШЯДЕЩЖЦЪ (исходный алфавит: АБВГДЕЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ)

Компетентностно-ориентированная задача № 9
Пусть хеш-функция y=h(x1x2…xn) определяется как результат выполнения побитовой операции «сумма по модулю 2» для всех байтов сообщения, представленного в двоичном виде Длина хеш-кода равна 8 битам Для каждого из шести сообщений, записанных в левом столбце, найдите соответствующий результат вычисления хеш-функции из правого столбца Все сообщения и значения хеш-функции представлены в шестнадцатеричном формате
а) 34 0A9 0B6
б) 32 7F 0B3
в) 1A 0B4 96
г) 0D2 0C1 0B2
д) 0E4 36 29
е) 21 0AE 54

Компетентностно-ориентированная задача № 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.

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.