Оценочный материал для промежуточной аттестации по дисциплине «Основы информационной безопасности» 1 семестр

Квалификация выпускника	*Бакалавр*
Направление подготовки	Безопасность информационных систем и технологий **09.03.02** *Шифр* **Информационные системы и технологии** *наименование*
Форма обучения*	**очная**
Кафедра-разработчик	Информатики и вычислительной техники *наименование*
Выпускающая кафедра	**Информатики и вычислительной техники** *наименование*

Типовые задания для контрольной работы:

Практическое задание № 1.

Сравнительный анализ энтропийных кодов модели источника сообщения

Цель работы – *смоделировать источник сообщения и провести сравнительный анализ энтропийных кодов для выявления самой эффективной.*

Шаги выполнения:

- Построение модели без памяти для сообщения (возможна программная реализация).
- Разработка энтропийных кодов (Фано и Шенона) по модели.
- Оптимизация кода Шеннона.
- Разработка блочного кода минимальной длины.
- Сравнение эффективности работы энтропийных кодов на основании изученных характеристик (скорости кода, избыточности на символ, степень сжатия и т.д.).
- Анализ результатов; написание отчёта о проделанной работе.

В качестве индивидуального сообщения предлагается перевод на иностранный язык следующих строк: «К счастью или к несчастью, время не ждет. Оно вздыхает с предсказаниями, тихо просыпается и опять уходит». Задания выполняются согласно индивидуальным вариантам (таблица 1).

Таблица 1 – Варианты индивидуальных заданий

Вариант	Язык
1	Грузинский
2	Французский
3	Немецкий
4	Итальянский
5	Испанский
6	Португальский
7	Датский
8	Шведский
9	Норвежский
10	Турецкий
11	Словенский
12	Польский
13	Украинский
14	Эстонский
15	Болгарский

Практическое задание № 2.

Проект по теме «Основы информационной безопасности»

Цель работы – *изучение основ информационной безопасности и анализ существующих подходов и методов решения проблемы защиты информации в современном мире.*

Проект направлен на пробуждение в студентах интереса к самостоятельному погружению в специфику некоторой узкой области сферы информационной безопасности, отвечающей интересам студента.

Шаги выполнения:

- Выбор и согласование с преподавателем темы проектной работы.
- Изучение литературы по выбранной теме.
- Выделение проблематики по выбранной теме в области информационной безопасности.
- Анализ существующих методов и подходов, использующихся в обеспечении информационной безопасности по выбранной теме.
- Выявление тенденций развития технологий по выбранной теме, определение направлений будущих исследований.
- Подготовка отчета по проделанной работе.

Примеры тем проектов:

1. Проблемы информационной безопасности в облачном хранилище
2. Развитие технологий обнаружения вторжений и противодействия им
3. Этические и правовые аспекты использования хакерских технологий. Обзор инцидентов последнего 10-летия
4. Использование искусственного интеллекта в информационной безопасности
5. Анализ рисков информационной безопасности с учетом угроз квантовых вычислений
6. Квантовая криптография: мифы и реальность
7. Применение машинного обучения для улучшения баз вирусных сигнатур
8. Биометрическая аутентификация: особенности внедрения и применения
9. Мультифакторная аутентификация: тренды и сценарии развития
10. Сравнение моделей разграничения доступа: дискреционный, мандатный и ролевой подходы
11. Использование искусственного интеллекта и машинного обучения в защите от DDoS
12. Кейлоггеры: принцип работы, методы обнаружения и защиты
13. Проблемы и методы обнаружения и устранения Trojan horse-вирусов
14. Реализация сетевой безопасности с помощью виртуальных частных сетей (VPN)
15. Анализ сетевых топологий и выбор методов защиты с помощью межсетевых экранов

Типовые вопросы к экзамену:

1. Какие юридические основы определяют информационную безопасность?
2. Какие обязательства по обеспечению информационной безопасности возлагаются на работников организации?
3. Расскажите о правовой ответственности за нарушение требований информационной безопасности.
4. Какие документы должны быть разработаны в организации для обеспечения информационной безопасности?
5. Какие полномочия у специалистов по информационной безопасности в организации?
6. Какие права и обязанности у пользователей информационных ресурсов в организации?
7. Какие разрешительные документы должны быть получены для работы с информацией, составляющей государственную тайну?
8. Что такое персональные данные и как они определяются законодательством РФ?
9. Какие права у субъектов персональных данных и как они могут их осуществить?
10. Какие данные могут считаться конфиденциальными?
11. Какие данные могут считаться общедоступными?
12. Что такое уязвимости информационных систем, и как возникают?
13. Как оценить уровень уязвимостей в информационной системе, и какие методы и инструменты для этого существуют?
14. Как проводить аудит уязвимостей в информационных системах, и какие выводы можно сделать на его основе?
15. Как определить приоритеты при устранении уязвимостей в информационных системах, и какие критерии следует использовать?
16. Каким образом можно обеспечить превентивную защиту от уязвимостей в информационных системах, и какой роли здесь играет образование пользователей?
17. Что такое аутентификация? Каким образом можно использовать мультифакторную аутентификацию для дополнительной защиты информации? Какие виды мультифакторной аутентификации существуют и как они работают?
18. Что такое политика безопасности, и что в нее входит?
19. Каким образом разработать и реализовать политику безопасности в организации?
20. Каким образом можно обеспечить защиту от внутренних угроз в рамках политики безопасности, таких как утечки информации или нарушения правил доступа?
21. Что такое кодирование и как оно помогает обеспечивать безопасность информации?
22. Какие виды кодирования принято выделять? Назовите их назначение
23. Расскажите про различные методы кодирования, такие как поточное и блочное.
24. Расскажите про использование криптографических хеш-функций для кодирования информации.
25. Что такое помехоустойчивое кодирование и как оно используется для обеспечения безопасности данных?
26. Какой принцип лежит в основе кода Хэмминга и в каких случаях он может быть полезным?
27. Какие параметры оценки помехоустойчивых кодов вы знаете? Зачем они нужны, как вычисляются?
28. Расскажите о кодах обнаружения атак. В чем их преимущества и недостатки
29. Что такое криптография? Какие задачи в ней решаются?
30. Что такое криптоанализ? Расскажите про известные вам классы атак
31. Какие методы шифрования вам известны?
32. Что такое конфиденциальность и почему она важна для обеспечения безопасности данных?
33. Какие данные в организации могут считаться конфиденциальными, и как их защищать?
34. Расскажите про основные методы защиты конфиденциальности данных в организации.
35. Расскажите про программы шифрования файлов и основные методы их шифрования.
36. Расскажите про использование ключей. Как можно организовать безопасное хранение и распределение ключей?
37. Что такое целостность и почему она важна для обеспечения безопасности данных?
38. Какие виды угроз существуют в отношении целостности данных?

39. Как защитить целостность данных при использовании облачных технологий и систем хранения информации?
40. Как организовать процесс резервного копирования и восстановления данных для обеспечения целостности информации в организации?
41. Что такое доступность и почему она важна для обеспечения безопасности данных?
42. Какие виды угроз существуют в отношении доступности данных?
43. Расскажите про основные методы защиты доступности данных, используемые в информационной безопасности.
44. Как защитить доступность данных при использовании облачных технологий и систем хранения информации?
45. Что такое системы разграничения прав доступа и как они помогают обеспечивать безопасность данных?
46. Расскажите про процесс аутентификации и авторизации пользователей при работе с информационными системами.
47. Каким образом можно организовать доступ к конфиденциальным данным только для определенных категорий пользователей, например, руководителей или администраторов?
48. Как организовать автоматическое изменение прав доступа в зависимости от изменения должностных обязанностей пользователей?
49. Расскажите про основные виды уязвимостей сетевых технологий и методы их предотвращения.
50. Расскажите про основные методы защиты от сетевых атак, таких как DoS-атаки и перехват трафика.
51. Какие принципы можно использовать для создания защищенных виртуальных частных сетей и туннелирования трафика?
52. Как возможно избежать утечки информации в сетевых технологиях, например, при передаче данных через открытые сети или при использовании общедоступных ресурсов?