Автономная некоммерческая организация
профессионального образования
«Колледж информационных технологий «КАСПИЙ»
367013, г. Махачкала, пр-кт. Гамидова, зд.18м
ОГРН: 1220500003580, ИНН: 0572030404

КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем
квалификация- Техник по защите информации

Махачкала, 2025 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Контрольно-оценочные средства (КОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами. КОС включает контрольные материалы для промежуточной аттестации. освоение содержания профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами. обеспечивает достижение студентами следующих результатов:

- Иметь практический опыт
- умений
- знаний

Формы промежуточной аттестации по профессиональному модулю в ходе освоения ОПОП ППССЗ

Наименование профессионального модуля	**Форма промежуточной аттестации (дифференцированный зачет, экзамен)**
МДК 02.01 Программные и программно-аппаратные средства защиты	Контрольная работа Дифференцированный зачет Экзамен
МДК 02.02 Криптографические средства защиты информации	Контрольная работа Дифференцированный зачет

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ

В результате аттестации по профессиональному модулю осуществляется комплексная проверка компетенций (ОК, ПК).

Результаты обучения компетенции	**Показатели оценки результата**	**Форма контроля и оценивания**
Иметь практический опыт	• установки, настройки программных средств защиты информации в автоматизированной системе; • обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; • тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; • решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; • применения электронной подписи,	1.Контрольные задания для экзамена по междисциплинарному курсу МДК 02.01 Задание № 1. Контрольные задания для дифференцированного зачета по междисциплинарному курсу МДК 02.01 Задание № 2. 2. Контрольные задания для экзамена по междисциплинарному курсу МДК 02.02 Задание № 2. Контрольные задания для дифференцированного зачета по междисциплинарному

	симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных; • учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; • работы с подсистемами регистрации событий; • выявления событий и инцидентов безопасности в автоматизированной системе.	курсу МДК 02.01 Задание № 2.
Знать	• устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; • устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; • диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; • применять программные и программно-аппаратные средства для защиты информации в базах данных; • проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; • применять математический аппарат для выполнения криптографических преобразований; • использовать типовые программные криптографические средства, в том числе электронную подпись; • применять средства гарантированного уничтожения информации; • устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; • осуществлять мониторинг и регистрацию сведений, необходимых	11.Контрольные задания для экзамена по междисциплинарному курсу МДК 02.01 Задание № 1. Контрольные задания для дифференцированного зачета по междисциплинарному курсу МДК 02.01 Задание № 2. 2. Контрольные задания для экзамена по междисциплинарному курсу МДК 02.02 Задание № 2. Контрольные задания для дифференцированного зачета по междисциплинарному курсу МДК 02.01 Задание № 2.

	для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, • предупреждения и ликвидации последствий компьютерных атак	
Уметь	• основные понятия криптографии и типовых криптографических методов и средств защиты информации; • особенности и способы применения программных и программно- аппаратных средств гарантированного уничтожения информации; • типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.	1.Контрольные задания для экзамена по междисциплинарному курсу МДК 02.01 Задание № 1. Контрольные задания для дифференцированного зачета по междисциплинарному курсу МДК 02.01 Задание № 2. 2. Контрольные задания для экзамена по междисциплинарному курсу МДК 02.02 Задание № 2. Контрольные задания для дифференцированного зачета по междисциплинарному курсу МДК 02.01 Задание № 2.

ВОПРОСЫ К ЭКЗАМЕНУ
ПО МДК 02.01 ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ

1. Предмет и задачи программно-аппаратной защиты информации.
2. Основные понятия программно-аппаратной защиты информации.
3. Классификация методов и средств программно-аппаратной защиты информации.
4. Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно- аппаратными средствами.
5. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты).
6. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами
7. Автоматизация процесса обработки информации.
8. Понятие автоматизированной системы.
9. Особенности автоматизированных систем в защищенном исполнении.
10. Основные виды АС в защищенном исполнении.
11. Методы создания безопасных систем.
12. Методология проектирования гарантированно защищенных КС.
13. Дискреционные модели.
14. Мандатные модели.
15. Источники дестабилизирующего воздействия на объекты защиты.
16. Способы воздействия на информацию.
17. Причины и условия дестабилизирующего воздействия на информацию
18. Понятие несанкционированного доступа к информации.
19. Основные подходы к защите информации от НСД.
20. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам.
21. Доступ к данным со стороны процесса.
22. Особенности защиты данных от изменения. Шифрование.
23. Алгоритм загрузки ОС. Штатные средства замыкания среды.
24. Расширение BIOS как средство замыкания программной среды.
25. Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды.
26. Понятие АМДЗ (доверенная загрузка).
27. Способы изучения ПО: статическое и динамическое изучение.
28. Задачи защиты от изучения и способы их решения.
29. Защита от отладки.
30. Защита от дизассемблирования.
31. Защита от трассировки по прерываниям.
32. Классификация вредоносного программного обеспечения.
33. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения.
34. Поиск следов активности вредоносного ПО.
35. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО.
36. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.
37. Ботнеты. Принцип функционирования. Методы обнаружения.
38. Классификация антивирусных средств. Сигнатурный и эвристический анализ.
39. Защита от вирусов в "ручном режиме".

40. Основные концепции построения систем антивирусной защиты на предприятии.

41. Несанкционированное копирование программ как тип НСД.

42. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования.

43. Привязка ПО к аппаратному окружению и носителям.

44. Защитные механизмы в современном программном обеспечении на примере MS Office

45. Проблема защиты отчуждаемых компонентов ПЭВМ.

46. Методы защиты информации на отчуждаемых носителях. Шифрование.

47. Средства восстановления остаточной информации. Создание посекторных образов НЖМД.

48. Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов.

49. Нормативная база, документирование результатов.

50. Безвозвратное удаление данных. Принципы и алгоритмы.

51. СОВ и СОА, отличия в функциях. Основные архитектуры СОВ.

52. Использование сетевых снифферов в качестве СОВ.

53. Аппаратный компонент СОВ.

54. Программный компонент СОВ.

55. Модели системы обнаружения вторжений.

56. Классификация систем обнаружения вторжений.

57. Обнаружение сигнатур.

58. Обнаружение аномалий.

59. Другие методы обнаружения вторжений.

60. Сети, работающие по технологии коммутации пакетов.

61. Стек протоколов TCP/IP. Особенности маршрутизации.

62. Штатные средства защиты информации стека протоколов TCP/IP.

63. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.

64. Виртуальная частная сеть. Функции, назначение, принцип построения.

65. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.

66. Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки.

67. Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки.

68. Методы защиты информации при работе в сетях общего доступа.

69. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности.

70. Основные типы firewall. Симметричные и несимметричные firewall.

71. Уровень 1. Пакетные фильтры.

72. Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне.

73. Уровень 3. Proxy-сервера прикладного уровня.

74. Однохостовые и мультихостовые firewall.

75. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций.

76. Требования по сертификации межсетевых экранов.

77. Средства идентификации и аутентификации. Управление доступом.

78. Средства контроля целостности информации в базах данных.

79. Средства аудита и контроля безопасности. Критерии защищенности баз данных.

80. Применение криптографических средств защиты информации в базах данных.

81. Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации.

82. Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25.

83. Классификация отслеживаемых событий. Особенности построения систем мониторинга.

84. Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования.

85. Классификация сетевых мониторов.

86. Системы управления событиями информационной безопасности (SIEM).

87. Обзор SIEM-систем на мировом и российском рынке

88. Классификация методов и средств программно-аппаратной защиты информации.

89. Источники дестабилизирующего воздействия на объекты защиты.

90. Основные подходы к защите информации от НСД.

91. Работа автономной АС в защищенном режиме.

92. Методы защиты информации на отчуждаемых носителях. Шифрование

93. Основные виды АС в защищенном исполнении.

94. Причины и условия дестабилизирующего воздействия на информацию.

95. Особенности защиты данных от изменения. Шифрование.

96. Вредоносное программное обеспечение как особый вид разрушающих воздействий.

97. Несанкционированное копирование программ как тип НСД.

ПРАКТИЧЕСКИЕ ЗАДАНИЯ

Задание 1. Изучить технологии учета и хранения информации. Описать, как происходит сбор и регистрация данных. Назовите основные требования к сбору данных и к хранимым данным. Перечислите основные средства сбора текстовой, графической, звуковой и видеоинформации. Какие еще средства сбора информации вам известны?

Задание 2. Изучить технологический процесс обработки информации. Перечислить и охарактеризовать технологические процессы процесса обработки информации. В чем заключается различие между централизованным и децентрализованным способами обработки информации? Какие режимы обработки информации вам известны?

Задание 3. Изучить технологии передачи и представления информации. Описать, как происходит передача данных.

Задание 4. Выполнить задания:

•набрать в одном из текстовых редакторов текст из 10 предложений на тему «Моя профессия»;

- вставить в набранный текст рисунок;
- сохранить текст на каких-либо носителях;
- создать свою электронную почту;
- отправить, набранную информацию по электронной почте;
- получить информацию по электронной почте;
- изменить полученный текст, введя диаграмму;
- сохранить текст.

Задание 5. Продумать и создать технологию учета и отработки заявок на выполнение работ по ремонту компьютерной техники в салоне по ремонту компьютерного оборудования «Сервис- ТЕХНО». Результат выполнения задания оформить в виде таблицы.

Задание 6. Используя технологии поиска информации, найдите разницу между терминами “хранение” и “сохранение данных”.

Задание 7. Используя средства Интернета, перечислите устройства защиты технических устройств информатизации от изменения напряжения и тока их электропитания.

Задание 8. Ознакомиться с технологиями создания и управления учетными записями пользователей. Примените к созданной учётной записи настройки, указанные в варианте.

Таблица 1 – Варианты заданий

Вариант / Параметр	1	2	3	4	5	6	7	8	9	10
Максимальный срок действия пароля	30	90	60	30	90	60	30	90	60	30
Минимальная длина пароля	6	7	8	9	10	6	7	8	9	10
Требовать неповторяемости паролей	6	5	4	3	2	6	5	4	3	2
Пароль должен отвечать требованиям сложности	+	-	-	+	-	-	+	-	+	+
Пороговое значение блокировки	3	4	5	6	7	3	4	5	6	7
Блокировка учётной записи на…	10	20	30	45	60	10	20	30	45	60
Сброс счётчика блокировки через…	5	10	15	20	30	10	20	30	45	60
Завершение работы системы	+	+			+		+		+	
Локальный вход в систему	+	+	+	+	+	+	+	+	+	+
Изменение системного времени	+		+		+		+		+	

Задание 9. Создайте новую учетную запись пользователя с помощью командной строки.

Задание 10. Создайте учетные записи для двух разных пользователей. Для одного пользователя проверьте действенность флажка – требования смены пароля пользователя при следующей регистрации в системе, для другого – запрет на изменение пароля пользователем.

Задание 11. Создайте локальную группу. Поместите в локальную группу созданных вами пользователей и административного пользователя. Проделайте это двумя способами: через окно свойств группы и окно свойств пользователя.

Задание 12. Измените параметр «Пароль должен отвечать требованиям сложности» Политики паролей на «Включен» и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль. Этот пароль является результатом выполнения вашего задания.

Задание 13. После успешного выполнения предыдущего задания, измените пароль вашей учетной записи, а в качестве нового пароля укажите прежний пароль. Все сообщения зафиксируйте, проанализируйте и объясните поведение системы безопасности.

Задание 14. Проведите эксперименты с другими параметрами Политики учетных записей.

Задание 15.

1. Создайте папку, в которую поместите текстовый файл и приложение в виде файла с расширением exe, например, одну из стандартных программ Windows, такую как notepad.exe (Блокнот).
2. Установите для этой папки разрешения полного доступа для одного из пользователей группы Администраторы и ограниченные разрешения для пользователя с ограниченной учетной записью.
3. Выполните различные действия с папкой и файлами для обеих учетных записей и установите, как действуют ограничения, связанные с назначением уровня доступа ниже, чем полный доступ.
4. Установите общий доступ к папке и подключитесь к ней через сеть с другого виртуального компьютера.
5. Установите разрешения общего доступа так, чтобы администратор не имел ограничений, а пользователь имел ограниченный уровень доступ

a. Экспериментально убедитесь в выполнении правил объединения разрешений NTFS и разрешений общего доступа.

b. Составьте отчет о проведенных экспериментах.

Задание 16. Разработайте стратегию регулирования безопасности при коллективном доступе к общим папкам для различных групп пользователей.

1. Опишите параметры и значения параметров Политики аудита. Заполнить таблицу.
2. Просмотрите события в журнале событий.
3. Информация о каких событиях сохраняется в системном журнале?
4. Какие данные по каждому событию отображаются в журнале?
5. Включите аудит успеха и отказа всех параметров.
6. Выйдите из системы и предпримите попытку входа в операционную систему с неверным паролем.
7. Откройте журнал событий, найдите соответствующую запись.

a. Удалите раннее созданную учетную запись и зафиксируйте все события системного журнала, связанные с этим действием.

Задание 17. Создать несколько файлов, заполнить их данными. Сделать копии файлов и произвести для некоторых из них «незаметные» для пользователей изменения в файлах. К таким изменениям можно отнести, к примеру:

- изменение кода цвета объектов, в частности текста;
- замена символов на похожие символы с другими кодами символов;

•вставка объектов со 100 %-ной прозрачностью, отсутствующими цветами заливками или совпадающими с цветом фона;

•изменение текста до минимального, установка цвета текста под цвет фона;

•вставка текста с атрибутами «скрытый текст», опция «Шрифт» => «Видоизменение»;

•изменение рисунка (областей с мало отличимой палитрой цветов);

•изменение метаданных файлов (к примеру, вкладка «Подробно» с полями «Авторы»,

• «Организация» и пр.);

•прочее.

Задание 18. Используя программную реализацию механизма хэш-функций, проверить целостность и неизменность файлов. Предоставить снимки экрана, описание действий и результатов. Прокомментировать детально результаты работы: когда совпадают, когда расходятся и почему.

Задание 19. Современная диалектика оформлялась на основе обобщения огромного фактического материала. Причем она обобщает материалы не отдельной области знаний, а совокупность фактов бытия природы и всемирно-исторической практики и опирается на потенциал всего человеческого познания, на данные истории и достижения современного научно- технического прогресса. Согласны ли вы с такой оценкой диалектики? Если да, то покажите это на конкретном материале естественных и гуманитарных наук.

Задание 20. Изучить возможность атаки на хэш-функцию, продемонстрировать пример.

Задание 21. Продемонстрировать возможность тайной передачи данных (картинок, текста) в документах так, чтобы проверка контрольной суммы не обнаружила изменений.

Задание 22. Заданы документы с различным уровнем секретности, заданы пользователи с различным уровнем доступа (список документов и пользователей и их уровни доступа/секретности составить самостоятельно. Не менее 5 пользователей и 5 документов).

1.Для каждого пользователя составить список документов, доступных ему для работы при условии, что пользователь не понижает своего уровня допуска.

2. Для одного из пользователей составить список документов, доступных ему для работы при условии, что пользователь может понизить свой уровень доступа на один уровень.

3.Один из пользователей имеет возможность работать с несколькими документами. На основе этих документов он создает новый документ. Какой гриф секретности нужно присвоить этому документу?

4.Показать на примере одного из пользователей, что мандатная политика безопасности не может быть нарушено программой типа "Троянский конь".

Задание 23. Проверка разрешений NTFS.

1. Зарегистрируйтесь в системе под разными учетными записями и проверьте разрешения

NTFS.

2. Проверьте разрешения доступа к папке Misc для пользователя User81.

3. Проверьте разрешения доступа к папке Misc для пользователя User82.

4. Зарегистрируйтесь в системе как User82 и откройте папку Public\Library\Misc. Попробуйте создать файл в папке Misc. Удалось ли это? Почему?

5. Проверьте разрешения доступа к папке Manuals для пользователя Administrator. Попробуйте создать файл в папке Manuals. Удалось ли это? Почему?

6. Проверьте разрешения доступа к папке Manuals для пользователя User81. Попробуйте создать файл в папке Manuals. Удалось ли это? Почему?

7. Проверьте разрешении доступа к папке Manuals для пользователя User82. Попробуйте создать файл в папке Manuals. Удалось ли это? Почему?

Параметр	Значение
Аудит событий Входа в систему	
Аудит управления Учетными записями	
Аудит доступа к службе каталогов	
Аудит входа в систему	
Аудит доступа к объектам	
Аудит изменения политики	
Аудит использования привилегий	
Аудит отслеживания процессов	
Аудит системных событий	

ДИФФЕРЕНЦИРОВАННЫЙ ЗАЧЕТ

1) Возможность за приемлемое время получить требуемую информационную услугу называется:

1. Конфиденциальность
2. Доступность
3. Целостность
4. Непрерывность

Эталон ответа: b

2) К аспектам информационной безопасности не относится:

1. Доступность
2. Целостность
3. Конфиденциальность
4. Защищенность

Эталон ответа: d

3) По каким критериям нельзя классифицировать угрозы:

1. по расположению источника угроз
2. по аспекту информационной безопасности, против которого угрозы направлены в первую очередь
3. по способу предотвращения
4. по компонентам информационных систем, на которые угрозы нацелены

Эталон ответа: c

4) Главное достоинство парольной аутентификации – …

1. простота

2. надежность
3. секретность
4. запоминаемость

Эталон ответа: a

5) Сколько уровней включает в себя сетевая модель OSI?

1. 5
2. 7
3. 6
4. 8

Эталон ответа: b

6) Межсетевой экран (Брандмауэр, firewall) – это…

1. Комплекс аппаратных средств
2. Комплекс программных средств
3. Комплекс аппаратных или программных средств
4. Комплекс аппаратных и программных средств

Эталон ответа: c

7) На каком уровне сетевой модели OSI не работает межсетевой экран:

1. Физический
2. Сеансовый
3. Сетевой
4. Транспортный

Эталон ответа: a

8) Межсетевого экрана какого класса не существует:

1. экранирующий маршрутизатор
2. экранирующий коммутатор
3. экранирующий транспорт
4. экранирующий шлюз

Эталон ответа: b

9) Что из перечисленного не входит в состав программного комплекса антивирусной защиты:

1. Подсистема сканирования
2. Подсистема управления
3. Подсистема обнаружения вирусной активности
4. Подсистема устранения вирусной активности

Эталон ответа: d

10) На каком этапе заканчивается жизненный цикл автоматизированной системы?

1. Бета-тестирование системы
2. Внедрение финальной версии системы в эксплуатацию
3. Прекращение сопровождения и технической поддержки системы
4. Альфа-тестирование системы

Эталон ответа: c

11) Какие задачи выполняет теория защиты информации:

1. предоставлять полные и адекватные сведения о происхождении, сущности и развитии проблем защиты
2. аккумулировать опыт предшествующего развития исследований, разработок и практического решения задач защиты информации
3. формировать научно обоснованные перспективные направления развития теории и практики защиты информации
4. выполняет все вышеперечисленные

Эталон ответа: d

12) Какой из протоколов не относится к протоколам защищенной передачи данных в сети Интернет:

1. SSL

2. SET
3. HTTP
4. IPSec

Эталон ответа: c

13) Какого метода разграничения доступа не существует:

1. разграничение доступа по спискам
2. разграничение доступа по уровням секретности и категориям
3. локальное разграничение доступа
4. парольное разграничение доступа

Эталон ответа: c

14) К основным функциям подсистемы защиты операционной системы относятся:

1. идентификация, аутентификация, авторизация, управление политикой безопасности и разграничение доступа
2. криптографические функции
3. сетевые функции
4. все вышеперечисленные

Эталон ответа: d

15) Риск – это…

1. вероятностная оценка величины возможного ущерба, который может понести владелец информационного ресурса в результате успешно проведенной атаки
2. фактическая оценка величины ущерба, который понес владелец информационного ресурса в результате успешно проведенной атаки
3. действие, которое направлено на нарушение конфиденциальности, целостности и/или доступности информации, а также на нелегальное использование других ресурсов сети
4. реализованная угроза

Эталон ответа: a

ВОПРОСЫ К ЭКЗАМЕНУ
МДК 02.02 КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

1. Классификация основных методов криптографической защиты.
2. Методы симметричного шифрования.
3. Шифры замены, пропорциональный шифр.
4. Простая замена, многоалфавитная подстановка.
5. Методы перестановки. Табличная перестановка, маршрутная перестановка.
6. Гаммирование. Гаммирование с конечной и бесконечной гаммами.
7. Основные методы криптоанализа.
8. Криптографические атаки.
9. Криптографическая стойкость. Абсолютно стойкие криптосистемы.
10. Принципы Керкхоффса.
11. Перспективные направления криптоанализа, квантовый криптоанализ.
12. Основные принципы поточного шифрования.
13. Применение генераторов ПСЧ в криптографии.
14. Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.
15. Кодирование информации. Символьное кодирование. Смысловое кодирование.
16. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII.
17. Компьютеризация шифрования.
18. Аппаратное и программное шифрование.
19. Стандартизация программно-аппаратных криптографических систем и средств.
20. Современные программные и аппаратные криптографические средства.
21. Структурная схема симметричных криптографических систем.
22. Классификация основных методов криптографической защиты.
23. Методы симметричного шифрования.
24. Шифры замены, пропорциональный шифр.
25. Простая замена, многоалфавитная подстановка. Основные методы криптоанализа.
26. Криптографическая стойкость. Абсолютно стойкие криптосистемы.
27. Принципы Керкхоффса.
28. Перспективные направления криптоанализа, квантовый криптоанализ.
29. Основные принципы поточного шифрования.
30. Применение генераторов ПСЧ в криптографии.
31. Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.
32. Кодирование информации. Символьное кодирование. Смысловое кодирование.
33. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII.
34. Компьютеризация шифрования.
35. Аппаратное и программное шифрование.
36. Стандартизация программно-аппаратных криптографических систем и средств.
37. Современные программные и аппаратные криптографические средства.
38. Структурная схема симметричных криптографических систем.
39. Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р
40. Симметричные алгоритмы DES, AES.
41. Симметричный алгоритм ГОСТ 28147-89.
42. Симметричный алгоритм RC4.

43. Криптосистемы с открытым ключом. Необратимость систем.
44. Структурная схема шифрования с открытым ключом.
45. Элементы теории чисел в криптографии с открытым ключом.
46. Аутентификация данных. Общие понятия.
47. Электронная цифровая подпись. Основные понятия.
48. Алгоритмы цифровой подписи.
49. MAC.
50. Однонаправленные хеш-функции.
51. Алгоритмы распределения ключей с применением симметричных и асимметричных схем.
52. Протоколы аутентификации.
53. Взаимная аутентификация. Односторонняя аутентификация.
54. Абонентское шифрование. Пакетное шифрование.
55. Защита центра генерации ключей
56. Криптомаршрутизатор.
57. Пакетный фильтр.
58. Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протокола WPA.
59. Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протокола WEP.
60. Принципы функционирования электронных платежных систем.
61. Электронные пластиковые карты. Персональный идентификационный номер.
62. Применение криптографических протоколов для обеспечения безопасности электронной коммерции.
63. Скрытая передача информации в компьютерных системах.
64. Проблема аутентификации мультимедийной информации.
65. Защита авторских прав.
66. Методы компьютерной стеганографии.
67. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ.

ПРАКТИЧЕСКИЕ ЗАДАНИЯ

Задание № 1

Назовите основные требования к сбору данных и к хранимым данным. Перечислите основные средства сбора текстовой, графической, звуковой и видеоинформации. Какие еще средства сбора информации вам известны? Предложите технологию учета и отработки заявок на выполнение работ по ремонту компьютерной техники в салоне по ремонту компьютерного оборудовании «Сервис-ТЕХНО».

Задание № 2

Опишите технологический процесс обработки информации. Перечислите и охарактеризуйте технологические процессы процесса обработки информации. Какие режимы обработки информации вам известны? Перечислите устройства защиты технических устройств информатизации от изменения напряжения и тока их электропитания.

Задание № 3

Опишите технологию создания и управления учетными записями пользователей. Создайте учетные записи для двух разных пользователей. Для одного пользователя проверьте действенность флажка – требования смены пароля пользователя при следующей регистрации в системе, для другого – запрет на изменение пароля пользователем. Создайте локальную группу. Поместите в локальную группу созданных вами пользователей и административного пользователя. Проделайте это двумя способами: через окно свойств группы и окно свойств пользователя.

Задание № 4

Опишите параметры локальной политики безопасности операционной системы Windows, параметры и значения параметров Политики учетной записи, параметры и значения параметров Политики паролей. Измените параметр «Пароль должен отвечать требованиям сложности» Политики паролей на «Включен» и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль.

Задание № 5

Создайте папку, в которую поместите текстовый файл и приложение в виде файла с расширением exe. Установите для этой папки разрешения полного доступа для одного из пользователей группы Администраторы и ограниченные разрешения для пользователя с ограниченной учетной записью. Установите общий доступ к папке и подключитесь к ней через сеть с другого виртуального компьютера. Предложите стратегию регулирования безопасности при коллективном доступе к общим папкам для различных групп пользователей.

Задание № 6

Опишите параметры и значения параметров Политики аудита. Просмотрите события в журнале событий. Информация о каких событиях сохраняется в системном журнале? Какие данные по каждому событию отображаются в журнале? Включите аудит успеха и отказа всех параметров.

Задание № 7

Опишите причины возникновения остаточной информации. Приведите примеры устройств уничтожения информации с магнитных носителей. Перечислите основные требования к современным устройствам уничтожения информации с магнитных носителей. Охарактеризуйте программные методы уничтожения информации. Обоснуйте выбор устройства уничтожения информации с магнитных носителей.

Задание № 8

Проведите анализ защищенности заданного объекта защиты информации по следующим разделам: виды возможных угроз, характер происхождения угроз, классы каналов несанкционированного получения информации, источники появления угроз, причины нарушения целостности информации, потенциально возможные злоумышленные действия.

Задание № 9

Опишите разделы реестра Windows. В каких разделах реестра хранится информация о выбранной политике безопасности? Опишите возможности программы REGEDIT.EXE. Проведите исследование реестра Windows для нахождения следов активности вредоносного ПО

Задание т № 10

Создайте новую книгу для проведения простых вычислений суммы, разности, произведения над числами, удовлетворяющими некоторому условию, на основе данных, вводимых пользователем. Задайте проверку выполнения условия (например, только положительные, только отрицательные, только целые из определенного диапазона значений и т.п.) для ячеек, в которые будет осуществляться ввод данных. Установите защиту: ячейки для ввода данных должны быть разблокированы, остальное содержимое листа – защищено от изменений; формулы, по которым производятся вычисления, – скрыты. При установке защиты листа разрешить всем пользователям настраивать ширину столбцов и высоту строк, менять заливку ячеек.

Задание 11.

Описать простейшие стеганографические алгоритмы. Выбрать контейнер и выполнить внедрение в него некоторой информации. От чего зависит криптостойкость стеганографических систем?

Задание 12.

Опишите последовательность действий при использовании алгоритма Диффи-Хеллмана. Для каких целей может применяться алгоритм Диффи-Хеллмана? На чём основывается безопасность обмена ключа по схеме Диффи-Хеллмана?

Задание 13.

Приведите алгоритм реализации цифровой подписи RSA. В чем отличие подписи RSA от алгоритма шифрования RSA? Приведите примеры программно-аппаратных средств, реализующих основные функции электронной цифровой подписи.

Задание 14.

Представьте алгоритм работы российского стандарта шифрования ГОСТ 28147-89. Выполнить ручное шифрование исходного текста с помощью алгоритма ГОСТ 28147-89. Сравните алгоритмы шифрования ГОСТ 28147-89 и DES. Приведите примеры программ симметричного шифрования.

Задание 15. Перечислите классические алгоритмы шифрования, которые описаны и реализованы в программе CrypTool. Зашифруйте и расшифруйте сообщение с помощью одного из имеющегося в программе CrypTool классического шифра замены и шифра перестановки.

Задание 16. Приведите алгоритм шифрования текста методом гаммирования. Зашифруйте и расшифруйте сообщение по представленному алгоритму. Опишите особенности двоичного гаммирования.

Задание 17. Приведите алгоритм шифрования текста методом перестановки. Зашифруйте и расшифруйте сообщение по представленному алгоритму. Приведите примеры классических методов шифрования.

Задание 18. Приведите алгоритм шифрования текста методом замены. Зашифруйте и расшифруйте сообщение по представленному алгоритму. Приведите примеры классических методов шифрования. Опишите сходства и различия шифра Гронсфельда и шифра Цезаря.

Задание 19. Опишите методику криптоанализа, основанную на исследовании частотности закрытого текста. Исследуйте частотность зашифрованного текста. Приведите типовые методы криптоанализа классических алгоритмов.

Задание 20. Составить алгоритм шифрования и расшифрования методом Виженера. Оцените криптостойкость данного метода шифрования.

ДИФФЕРЕНЦИРОВАННЫЙ ЗАЧЕТ

Задание 1. Составить программу шифрования по выбранному методу.

Задание 2. Составить алгоритм программы расшифрования по выбранному методу. Составить программу расшифрования по выбранному методу.

Задание 3. Расшифровать текст,

а) зашифрованный шифром Цезаря со сдвигом на 4 позиции:

Уокдгнбэылмбаноюзыбожмдлокнднебиь

б) зашифрованный шифром Цезаря со сдвигом на 6 позиции:

Иыфщлзвмелнмцйкяиыкъбиьъзвгйякялмъзиьдъвбъжязъ

в) зашифрованный заменой по кодовому слову «пароль»:

випигьпжоймгсзпчгумйрпигяиьлйжбийржгясыипипльбийнсынгнсьзъ

Задание 2. Составить программу шифрования по выбранному методу.

Задание 3. Составить алгоритм программы расшифрования по выбранному методу Составить программу расшифрования по выбранному методу.

Задание 4. Дешифровать сообщения:

а) Бирои имч еыеес витсч арзки танет есарл лпюсп мотоо еипнф кйаои крслт мн;

б) тиооско нцрпоед иявдттж афэелиа ткокнбв еапанъг уитриоб;

в) икинорткелэоидаржделлок.

Задание 5. Составить программу шифрования по выбранному методу.

Задание 6. Составить алгоритм программы расшифрования по выбранному методу. Составить программу расшифрования по выбранному методу.

Задание 7. Получить от преподавателя текстовый файл, содержащий большой художественный текст на русском языке в открытом виде. Написать программу «Частота символов». Исследовать частотность символов открытого теста.

Задание 8. Получить от преподавателя текстовый файл, содержащий большой объем зашифрованного текста на русском языке. Исследовать частотность зашифрованного текста.

Задание 9. Сравнивая реальную частотность символов русского языка, полученную в пункте 1, с частотностями зашифрованного текста, составить таблицу замен алгоритма шифрования и расшифровать зашифрованный текст, реализовав программу дешифровки. Дешифровке подвергните только первые 15–20 символов, наиболее часто встречающиеся в шифротексте.

Задание 10. Выполнить эвристический анализ текста, полученного в результате дешифровки. По смыслу текста выявить те замены, которые оказались неверными, и сформировать верные замены. Доведите результат дешифровки до приемлемого (удобочитаемого) вида.

Задание 11. Расшифровать фразу, зашифрованную столбцовой перестановкой:

a) ОКЕСНВРП_ЫРЕАДЕЫН_В_РСИКО;

b) ДСЛИЕЗТЕА_Ь_ЛЬЮВМИ_ _АОЧХК;

c) НМВИАИ_НЕВЕ_СМСТУОРДИАНКМ;

d) ЕДСЗЬНДЕ_МУБД_УЭ_КРЗЕМНАЫ;

e) СОНРЧОУО_ХДТ_ИЕИ_ВЗКАТРРИ.

Задание 12. Расшифровать фразу, зашифрованную двойной перестановкой (сначала были переставлены столбцы, затем строки):

a) СЯСЕ_ _ЛУНЫИАККННОГЯДУЧАТН;

b) МСЕЫ_ЛЫВЕНТОСАНТУЕИ_РЛПОБ;

c) АМНРИД_УЕБСЫ_ЕЙРСООКОТНВ_;

d) ОПЧУЛС_БООНЕВ_ОЖАЕОНЕЩЕИН;

e) ЕШИАНИРЛПГЕЧАВРВ_СЕЫНА_ЛО.

Задание 13. Расшифровать текст. Каждой букве алфавита соответствует двузначное число:

1) 39 25 20 34 82 63 66 46 35 20 25 82 86 39 51 74 35 51 66 20 44 37 25 27

51 35 44 20 90 37 51 25 25 51 63 91 20 11 37 46 48 25 20 37 61 51 14 82 82 66 82

35 29 82 91 25 51 74 51 24 78 51 24 59 46 86 51 44 74 20 25 37 37, 37 44 82 31 11
37 82 51 46 25 51 34 82 25 37 82 86 37 25 27 51 35 44 20 90 37 51 25 25 48 44
46 82 78 25 51 14 51 18 37 59 44, 51 74 82 35 20 90 37 59 44 66 90 82 25 25 48 44
37 61 10 44 20 18 20 44 37, 86 61 20 25 86 51 39 66 86 51 44 10 66 82 86 46 51
35 10 37 66 51 46 51 39 51 63 66 39 59 91 37. 56 46 51 86 20 66 20 82 46 66
59 24 35 10 18 37 78 51 35 18 20 25 37 91 20 90 37 63, 4651, 66 51 18 14 20 66
25 51 35 82 91 10 14 29 46 20 46 20 44 35 20 91 14 37 56 25 48 78 37 66 66 14 82
24 51 39 20 25 37 63, 35 10 86 51 39 51 24 37 46 82 14 37 44 25 51 18 37 78 37 91
25 37 78 91 25 20 31 46 51 61 51 66 25 51 39 25 48 78 39 37 24 20 78 10 18
35 51 91, 25 51 25 82 10 24 82 14 59 31 46 24 51 14 42 25 51 18 51 39 25 37
44 20 25 37 59 24 20 25 25 48 44 39 51 74 35 51 66 20 44, 66 56 37 46 20 59,
56 46 51 51 61 82 66 74 82 56 82 25 37 82 37 25 27 51 35 44 20 90 37 51 25 25 51 63
61 82 91 51 74 20 66 25 51 66 46 37 25 82 37 44 82 82 46 66 44 48 66 14 20, 82
66 14 37 51 46 66 10 46 66 46 39 10 82 46 39 37 24 37 44 20 59 10 18 35 51 91 20;
2) 74 29 23 27 17 99 71 25 49 32 29 34 27 63 32 25 17 99 60 62 25 34 95 29 53
59 82 27 71 29 77 99 34 27 91 17 99 71 49 99 27 15 60 32 25 50 27 17 62 27 95 27
50 25 91 32 59 77 95 29 50 25 99 59, 25 99 74 29 53 25 59 17 99 25 91 23 49 71 25
17 99 60 49 25 34 32 25 71 95 27 82 27 32 32 25 29 50 17 25 15 77 99 32 59 77
62 95 25 53 95 29 23 32 25 17 99 60 34 15 35 17 27 99 27 71 25 12 25 99 95 29 45
49 74 29. 62 95 27 63 34 27 71 17 27 12 25, 50 27 17 62 27 95 27 50 25 91 32 29
35 95 29 50 25 99 29 17 29 82 49 83 62 25 17 27 50 27 62 95 25 34 59 74 99 25
71 50 27 53 25 62 29 17 32 25 17 99 49 17 71 35 53 29 32 29 17 32 29 15 49 23
49 27 82 32 29 34 27 63 32 25 95 29 50 25 99 29 77 10 27 12 25 25 50 25 95 59 34
25 71 29 32 49 35 49 95 27 53 27 95 71 49 95 25 71 29 32 49 27 82 74 95 49 99 49 23
32 89 83 74 25 99 74 29 53 59 50 15 25 74 25 71 62 49 99 29 32 49 35 49 53
29 62 25 82 49 32 29 77 10 49 83 59 17 99 95 25 91 17 99 71. 34 15 35 62 25 17 15
27 34 32 49 83 25 62 99 49 82 29 15 60 32 25 62 95 49 82 27 32 27 32 49 27 34 49
17 74 25 71 89 83 82 29 17 17 49 71 25 71 12 25 95 35 23 27 91 53 29 82 27 32 89.
74 29 23 27 17 99 71 25 49 32 29 34 27 63 32 25 17 99 60 95 29 50 25 99 89 34
25 17 99 49 12 29 27 99 17 35 25 62 99 49 82 49 53 29 67 49 27 91 62 95 25 12 95 29
82 82 32 25 12 25 25 50 27 17 62 27 23 27 32 49 35.

Задание 14 Составить алгоритм шифрования и расшифрования методом Виженера.

Задание 15. Задан некоторый текст, зашифрованный шифром Виженера, требуется определить ключевое слово и прочитать открытый текст.

Шифрованный текст

Влцдутжбюцхъяррмшбрхцэооэцгбрьцмйфктъъюьмшэсяцпунуящэйтаьэдкцибр
ьцгбрпачкъуцпъбьсэгкцъгуущарцёэвърюуоюэкааэбрняфукабъарпяъафкъиьжяффнйо
яфывбнэнфуюгбрьсшьжэтбэёчюъюръегофкбьчябашвёэуъъюаднчжчужцёэвлрнчулб
юпцуруньъшсэюъзкцхъяррнрювяспэмасчкпэужьжыатуфуярюравртубурьпэщлафоуф
бюацмнубсюкйтаьэдйюнооэгюожбгкбрънцэпотчмёодзцвбцшщвщепчдчдръюьскасэг
ъппэгюкдойрсрэвоопчщшоказръббнэугнялёкьсрбёуыэбдэулбюасшоуэтъшкрсдугэфл

бубуъчнчтртпэгюкиугюэмэгюккъъпэгяапуфуэзьрадзьжчюрмфцхраююанчёчюъыхьъ
цомэфъцпоирькнщпэтэузуябащущбаыэйчдфрпэцъьрьцъцпоилуфэдцойэдятррачкубу
фнйтаьэдкцкрннцюабугюуубурьпйюэъжтгюркующоъуфъэгясуоичщщчдцсфырэдщэ
ъуяфшёчцюйрщвяхвмкршрпгюопэуцчйтаьэдкцибрьцыяжтюрбуэтэбдуящэубъибрюв
ъежагибрбагбрымпуноцшяжцечкфодщоъчжшйуъцхчщвуэбдлдъэгясуахзцэбдэулькнъ
щбжяцэьрёдъьвюврнуяфуоухфекьгцччгэъжтанопчынажпачкъуъмэнкйрэфщэъьбуд
эндадъярьеюэлэтчоубъцэфэвлнёэгфдсэвэёкбсчоукгаутэыпуббцчкпэгючсаъбэнэфърк
ацхёваетуфяепърювържадфёжбьфутощоявьъгупчршуитеачйчирамчюфчоуяюонкяжы
кгсцбрясшчйотъъжрсщчл.

Задание 16. Написать программу, выполняющую задачу исследования ДСЧ для одного из следующих вариантов:

1. Исследовать равномерность датчика (проверить гипотезу о равномерности распределения совокупности ДСЧ).
2. Определить период ДСЧ для различных параметров.
3. Исследовать автокорреляцию совокупности ДСЧ для различных параметров на глубину 100
4. отсчетов.
5. Построить гистограмму частоты появления каждого возможного значения совокупности ДСЧ.

Задание 17. Разработать и отладить ПО для исследования датчика псевдослучайных чисел.

Представить результаты исследования в графическом виде.

Задание 18. Дана кодовая таблица азбуки Морзе

А • —	Л • — • •	Ц — • — •
Б — • • •	М — —	Ч — — — •
В • — —	Н — •	Ш — — — —
Г — — •	О — — —	Щ — — • —
Д — • •	П • — — •	Ъ • — — • — •
Е •	Р • — •	Ы — • — —
Ж • • • —	С • • •	Ь — • • —
З — — • •	Т —	Э • • — • •
И • •	У • • —	Ю • • — —
Й • — — —	Ф • • — •	Я • — • —
К — • —	Х • • • •	

Декодируйте сообщение:

— — — — — • — • • — — — — • • — • — • — • — • — —

Закодируйте с помощью азбуки Морзе слова ПАРОЛЬ, ЭКРАНИРОВАНИЕ, **КОДИРОВАНИЕ.**

Задание 19. Дана таблица ASCII-кодов:

Расшифровать слово при помощи таблицы ASCII кодов: 49 20 6C 6FF 75.

Закодировать при помощи таблицы ASCII кодов слово Windows. Результат представить в шестнадцатеричной системе счисления.

Задание 20. Дана кодировочная таблица (первая цифра кода – номер строки, вторая – номер столбца):

Таблица ASCII-кодов

SP	!	"	#	$	%	&	`	(	)	*	+	,	-	.	/
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
@	A	B	C	D	E	F	G	M	I	J	K	L	M	N	O
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
`	a	в	c	d	e	f	g	h	i	j	k	l	m	n	0
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127

	0	1	2	3	4	5	6	7	8
0	А	Б	В	Г	Д	Е	Ё	Ж	З
1	И	К	Л	М	Н	О	П	Р	С
2	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
3	Ы	Ь	Э	Ю	Я	_	.	,	?
4	:	;	-	!	»				

С помощью этой кодировочной таблицы закодируйте фразу: ЯЗНАЮ МЕТОДЫ ШИФРОВАНИЯ.

Задание 21. Используя таблицу кодирования.

2	О	100
3	И	010
4	Е	011
5	П	1110
6	М	1100
7	ПРОБЕЛ	1101
8	А	0010
9	С	0011
10	Г	00000
11	В	00001
12	К	00010
13	Б	00011
14	З	111100
15	Т	111101
16	Ь	111110
17	Н	111111

Закодируйте слово СИМВОЛ. Рассчитайте полученную степень сжатия. Раскодируйте слово 11101011000000010100101100110000010.

ДИФФЕРЕНЦИРОВАННЫЙ ЗАЧЕТ

Практические вопросы

1.Сколько ключей, дающих различный результат шифрования, возможно при последовательном выполнении двух простых подстановок? Трех?

2. Сколько ключей, дающих различный результат шифрования/расшифрования, возможно для Полибианского квадрата (для фиксированного размера таблицы)?

3. Рассчитайте вероятность того, что в тексте из 100 символов буква «О» появится до 5 раз; в тексте из 1000 символов – до 50.

4. Составьте формулу расчета количества ключей в системе омофонов.

5. Как может быть взломана система Вижинера при шифровании длинного сообщения коротким ключом?

Оцените необходимое количество циклов повторения ключа.

6. В первых версиях машины Enigma одновременно применялись 3 ротора из 5 возможных. Сколько возможно различных разовых ключей?

7. Какое количество вариантов открытых текстов может быть составлено из символов шифротекста, если длина текста – N символов, количество вхождений каждого символа алфавита n1, n2, ..., nm?

8. Поставьте в соответствие таблице перестановок в шифре блочной одинарной перестановки число в диапазоне от 0 до N!. Так, чтобы ключ мог быть выражен одним числом.

9. В каких случаях множественные перестановки влияют на надежность алгоритма? 4. Можно ли менять порядок перестановок? В каких случаях?

10. Почему шифрование одноразовым блокнотом обладает абсолютной криптографической стойкостью? 2. За счет чего происходит синхронизация самосинхронизирующихся шифров?

11. Какие атаки могут быть осуществлены на шифры гаммирования?

12. Почему РСЛОС не могут применяться непосредственно для создания генераторов ПСЧ?

13. Что такое тактирование и прореживание, в чем смысл их применения?

14. В чем, на ваш взгляд, принципиальное отличие шифра RC4 от других приведенных здесь генераторов?

15. В чем состоит неудобство использования алгоритмов, основанных на «нерешаемых» проблемах?

16. Для каких целей используются различные режимы шифрования?

17. Почему шифры, основанные на сетях Фейстеля, оказываются обратимы, независимо от внутренней функции?

18. Оцените количество пар ключей, которые могут быть получены при атаке «встреча посередине» для одного блока, в зависимости от длин ключей и блоков. Все неопределенные распределения считайте равномерными.

19. Чем отличается задача поиска коллизий от задачи поиска вторых прообразов?

20. Как можно рассчитать вероятность совпадений дней рождений в группе из n человек? (выведите формулу).

21. Почему при длине хеш-значения в n бит, задача поиска коллизий требует примерно 2 2 n вычислений? (приведите приближенные расчеты).

22. Оцените время и требования к памяти, для поиска коллизий на 64-битных и 128-битных хеш-функциях.

23. Почему длина сообщения также является параметром при хешировании?

24. К чему приведет выбор составных p и q в RSA?

25. Как должны формироваться ключи, если n раскладывается на 3 множителя? Почему такие схемы не используются?

26. Может ли шифрующая экспонента в системе RSA быть четной?

27. Чем отличается решение задачи RSA от разложения на множители?

28. Какую проблему нужно решить криптоаналитику, для вскрытия схемы El Gamal?

29. Почему для шифрования в схеме EL Gamal каждый раз должно использоваться новое значение k?

30. Сопоставьте схему El Gamal и приведенную схему на эллиптических кривых.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1.Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449548.

2.Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2020. — 240 с. — (Профессиональное образование). — ISBN 978-5-534-10711-1. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456793

3.Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2020. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст: электронный // ЭБС Юрайт [сайт].