

УТВЕРЖДАЮ

Заместитель

И.И.И.

«*И.И.*»

И.И.И.

Заместитель директора по УР

Н.И. Никифорова

2022 г.

Б1.В.07 Основы информационной безопасности
(код и наименование дисциплины (модуля))

09.03.02 «Информационные системы и технологии»
(код и наименование направления подготовки/специальности)

Системы информационной безопасности
(наименование профиля/специализации)

бакалавр
квалификация

форма обучения очно
(очная, очно-заочная, заочная)

Нижнекамск 2022

Составитель ФОС:

Ст. преподаватель

(должность)


(подпись)

Захарова И.Н.

(Ф.И.О)

ФОС рассмотрен и одобрен на заседании кафедры ИСТ,
протокол от 20.04.2022 г. № 8

Зав. кафедрой


(подпись)

О.В. Матухина

(Ф.И.О.)

Эксперт:

Руководитель ООП

Ф.И.О., должность, организация, подпись



Л.Р. Вотякова

Перечень компетенций и индикаторов достижения компетенций с указанием этапов формирования в процессе освоения дисциплины

Компетенция:

ПК – 2 Способен обеспечить информационную безопасность на уровне баз данных

ПК – 2.1 Знает угрозы безопасности баз данных, способы предотвращения

ПК – 2.2 Умеет выявлять угрозы безопасности на уровне баз данных

ПК – 2.3 Владеет навыками применения способов предотвращения угроз безопасности на уровне баз данных

Индекс Компетенции	Этапы формирования компетенции (указать все темы из РПД)				Наименование оценочного средства
	Лекции	Практические Занятия, лабора- торный практи- кум	Лабораторные занятия	Курсовой проект (работа)	
ПК-2.1	Тема 1--8	Не предусмотрены	Лаб.зан. 1-9	Не предусмотрены	Экзамен, реферат
ПК-2.2	-	Не предусмотрены	Лаб.зан. 1-9	Не предусмотрены	Экзамен, реферат
ПК-2.3	-	Не предусмотрены	Лаб.зан. 1-9	Не предусмотрены	Экзамен, реферат

Перечень оценочных средств по дисциплине (модулю)

При оценке результатов деятельности обучающихся в рамках дисциплины Б1.В.07 Основы информационной безопасности используется рейтинговая система. Рейтинговая оценка формируется на основании текущего и промежуточного контроля. Максимальное и минимальное количество баллов по различным видам учебной работы описано в «Положении о балльно-рейтинговой системе оценки знаний студентов и обеспечения качества учебного процесса» ФГБОУ ВО «КНИТУ».

При изучении дисциплины предусматривается экзамен, реферат, выполнение двух расчётно-графических работ. За эти контрольные точки студент может получить минимальное и максимальное количество баллов (см. таблицу).

За экзамен студент может получить минимум 24 балла и максимум – 40 баллов.

Оценочные средства	Кол-во	Min, баллов	Max, баллов
Реферат	1	8	10
Экзамен	1	24	40
Итого:		60	100

Шкала оценивания

Цифровое выражение	Выражение в баллах:	Словесное выражение	Критерии оценки индикаторов достижения при форме контроля:
			экзамен
5	87 - 100	Отлично (зачтено)	Оценка «отлично» выставляется студенту, если теоретическое содержание курса освоено полностью, без пробелов; исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует в ответе дополнительный материал все предусмотренные программой задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному; анализирует полученные результаты; проявляет самостоятельность при выполнении заданий
4	74 - 86	Хорошо (зачтено)	Оценка «хорошо» выставляется студенту, если теоретическое содержание курса освоено полностью, необходимые практические компетенции в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
3	60 - 73	Удовлетворительно (зачтено)	Оценка «удовлетворительно» выставляется студенту, если теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, большинство предусмотренных программой заданий выполнено, но в них имеются ошибки, при ответе на поставленный вопрос студент допускает неточности, недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении программного материала.

2	Ниже 60	Неудовлетворительно (не зачтено)	Оценка «неудовлетворительно» выставляется студенту, если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, необходимые практические компетенции не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, качество их выполнения оценено числом баллов, близким к минимальному
---	---------	-------------------------------------	---

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»

Факультет Информационные технологии

Кафедра Информационных систем и технологий

Направление подготовки: 09.03.02 «Информационные системы и технологии»

Профиль: Системы информационной безопасности

Темы рефератов

Раздел 2. Модели политик безопасности

Варианты тем:

1. Модель Кларка Вилсона
2. Модель «Китайская стена»
3. Модель Белла и Ла Падуллы
4. Модель Гогена-Мезигера
5. Сазерлендская модель
6. Дискреционная (матричная) модель
7. Модель Take-Grant
8. Модель типизированной матрицы доступа (Модель Харрисона-Руззо-Ульмана)
9. Модель Диона
10. Модель Биба
11. Ролевая политика

Критерии оценки реферата:

Структура реферата:

- 1) титульный лист;
- 2) план работы с указанием страниц каждого вопроса, подвопроса (пункта);
- 3) введение;
- 4) текстовое изложение материала, разбитое на вопросы и подвопросы (пункты, подпункты) с необходимыми ссылками на источники, использованные автором;

- 5) заключение;
- 6) список использованной литературы;
- 7) приложения, которые состоят из таблиц, диаграмм, графиков, рисунков, схем (необязательная часть реферата).

Приложения располагаются последовательно, согласно заголовкам, отражающим их содержание.

Реферат оценивается научным руководителем исходя из установленных кафедрой показателей и критериев оценки реферата.

Критерии и показатели, используемые при оценивании учебного реферата

Критерии	Показатели
1. Новизна реферированного текста Макс. - 3 балла	<ul style="list-style-type: none"> - актуальность проблемы и темы; - новизна и самостоятельность в постановке проблемы, в формулировании нового аспекта выбранной для анализа проблемы; - наличие авторской позиции, самостоятельность суждений.
2. Степень раскрытия сущности проблемы Макс. - 2 балла	<ul style="list-style-type: none"> - соответствие плана теме реферата; - соответствие содержания теме и плану реферата; - полнота и глубина раскрытия основных понятий проблемы; - обоснованность способов и методов работы с материалом; - умение работать с литературой, систематизировать и структурировать материал; - умение обобщать, сопоставлять различные точки зрения по рассматриваемому вопросу, аргументировать основные положения и выводы.
3. Обоснованность выбора источников Макс. - 2 балла	<ul style="list-style-type: none"> - круг, полнота использования литературных источников по проблеме; - привлечение новейших работ по проблеме (журнальные публикации, материалы сборников научных трудов и т.д.).
4. Соблюдение требований к оформлению Макс. - 1 балла	<ul style="list-style-type: none"> - правильное оформление ссылок на используемую литературу; - грамотность и культура изложения; - владение терминологией и понятийным аппаратом проблемы; - соблюдение требований к объему реферата;

	- культура оформления: выделение абзацев.
5. Грамотность Макс. - 1 балла	<ul style="list-style-type: none"> - отсутствие орфографических и синтаксических ошибок, стилистических погрешностей; - отсутствие опечаток, сокращений слов, кроме общепринятых; - литературный стиль.
6. Проверка на антиплагиат Макс.1 баллов	<ul style="list-style-type: none"> - проверка реферата в система антиплагиат. - должно быть не менее 70% оригинальности текста

Примерные вопросы теста

по дисциплине Б1.В.07 Основы информационной безопасности

Понятие национальной безопасности Российской Федерации.

2. Национальные интересы РФ и стратегические национальные приоритеты.

3. Роль информационной безопасности в обеспечении национальной безопасности государства.

4. Основные составляющие национальных интересов Российской Федерации в информационной сфере.

5. Понятие информационной безопасности Российской Федерации.

6. Интересы личности общества и государства в информационной сфере.

7. Виды угроз информационной безопасности Российской Федерации.

8. Внешние и внутренние источники угроз информационной безопасности Российской Федерации.

9. Методы обеспечения информационной безопасности Российской Федерации

10. Источники понятий в области информационной безопасности.

11. Основные понятия информационной безопасности.

12. Общеметодологические принципы теории информационной безопасности.

13. Понятие и сущность защищаемой информации.

14. Права и обязанности обладателя информации.

15. Виды защищаемой информации.

16. Перечень сведений конфиденциального характера.

17. Понятие интеллектуальной собственности и особенности ее защиты.

18. Понятие угрозы информационной безопасности.

19. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов.

20. Классификация и виды угроз информационной безопасности.

21. Внутренние и внешние источники угроз информационной безопасности.

22. Угрозы утечки информации и угрозы несанкционированного доступа.

23. Основные элементы канала реализации угрозы безопасности информации.

24. Субъекты и цели информационного противоборства.

25. Составные части и методы информационного противоборства.

26. Информационное оружие, его классификация и возможности.

27. Методы нарушения конфиденциальности, целостности и доступности информации.

28. Информационное противоборство как способ воздействия на информационные системы.

29. Информационная безопасность критически важных объектов.

30. Обеспечение безопасности объектов информационной сферы государства в информационном противоборстве.

31. Компьютерная система как объект информационной безопасности.

32. Основные способы защиты информации.

33. Понятие и классификация средств защиты информации.
34. Характеристика средств защиты информации.
35. Уровни информационной безопасности и их характеристика.
36. Сервисы безопасности программно-технического уровня.
46. Назначение формальных моделей безопасности. Политика безопасности.
47. Дискреционная модель безопасности. Модель Харрисона-Руззо-Ульмана.
48. Мандатная модель безопасности. Модель Белла-ЛаПадулы.
49. Формальные модели целостности.
50. Понятие ролевого управления доступом.

Вариант №1

Задание #1

Вопрос:

Какие из следующих алгоритмов являются симметричными

Выберите несколько из 6 вариантов ответа:

- 1) DES
- 2) Эль-Гамаль
- 3) RSA
- 4) AES
- 5) DSA
- 6) Гост 28147-89

Задание #2

Вопрос:

Шифр DES - это ...

Выберите один из 5 вариантов ответа:

- 1) система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки
- 2) система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители
- 3) блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны
- 4) шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами
- 5) симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит.

Задание #3

Вопрос:

Целостность информации - это...

Выберите один из 4 вариантов ответа:

- 1) ее свойство быть неизменной в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий
- 2) ее свойство быть известной только допущенным и прошедшим проверку субъектам системы.

3) ее свойство быть доступной для авторизованных законных субъектов системы, готовность служб к обслуживанию запросов

4) некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы

Задание #4

Вопрос:

Что может быть использовано в качестве идентификатора?

Выберите несколько из 5 вариантов ответа:

- 1) бесконтактные радиочастотные карты
- 2) пластиковые карты
- 3) имя пользователя
- 4) секретный код
- 5)

Задание #5

Вопрос:

Процесс присвоения пользователю некоторого уникального *идентификатора*, который он должен предъявить системе защиты информации при осуществлении доступа к объекту называют ...

Запишите ответ:

Задание #6

Вопрос:

Что включают в себя организационно-административные меры защиты?

Выберите несколько из 6 вариантов ответа:

- 1) разработку правил обработки информации в АСОИ
- 2) совокупность действий при проектировании и оборудовании вычислительных центров и других объектов АСОИ
- 3) резервирование ресурсов и компонентов АСОИ
- 4) совокупность действий при подборе и подготовке персонала
- 5) организацию скрытого контроля за работой пользователей и персонала АСОИ
- 6) идентификацию и аутентификацию субъектов АСОИ

Задание #7

Вопрос:

Укажите преимущества формальных моделей

Выберите несколько из 4 вариантов ответа:

- 1) математическая строгость
- 2) возможность формального доказательства
- 3) большая абстрактность
- 4) формируют требования к поведению подсистемы безопасности на общем уровне без указания особенностей их реализации

Задание #8

Вопрос:

Какая схема лежит в основе алгоритмов шифрования DES и ГОСТ 28147-89?

Выберите один из 5 вариантов ответа:

- 1) Цезаря
- 2) Кантора
- 3) Фейстеля
- 4) Вижинера
- 5) Эль-гамала

Задание #9

Вопрос:

Стандарт шифрования данных ГОСТ - это ...

Выберите один из 4 вариантов ответа:

- 1) 64 битовый блочный алгоритм с 256 битовым ключом
- 2) 64-битовый блочный алгоритм с 56 битовым ключом
- 3) блок данных представляется в виде двухмерного байтового массива размером 4X4, 4X6 или 4X8
- 4) 64-битовый блочный алгоритм с 48 битовым ключом

Задание #10

Вопрос:

Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста - это метод ...

Выберите один из 5 вариантов ответа:

- 1) гаммирования
- 2) подстановки
- 3) кодирования
- 4) перестановки
- 5) аналитических преобразований

Задание #11

Вопрос:

Что включают в себя программно-аппаратные меры защиты?

Выберите несколько из 6 вариантов ответа:

- 1) разработку правил обработки информации в АСОИ
- 2) распределение реквизитов разграничения доступа (паролей, полномочий и т.п.)
- 3) обеспечение конфиденциальности данных
- 4) контроль целостности данных
- 5) аудит событий, происходящих в АСОИ
- 6) идентификацию и аутентификацию субъектов АСОИ

Задание #12

Вопрос:

К основным преднамеренным искусственным угрозам АСОИ относится:

Выберите несколько из 5 вариантов ответа:

- 1) пересылка данных по ошибочному адресу абонента
- 2) физическое разрушение системы путем взрыва, поджога и т.п.
- 3) неправомерное отключение оборудования или изменение режимов работы устройств и программ
- 4) игнорирование организационных ограничений (установленных правил) при работе в системе

5) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

Задание #13

Вопрос:

При шифрование методом гаммирования ...

Выберите один из 5 вариантов ответа:

- 1) символы шифруемого текста заменяются символами того же или другого алфавита в соответствие с заранее обусловленной схемой замены
- 2) символы шифруемого текста заменяются символами того же или другого алфавита в соответствие с заранее обусловленной схемой замены
- 3) наложение на открытые данные по определенному закону псевдослучайной последовательности, вырабатываемых по определенному алгоритму
- 4) символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов
- 5) замена слов и предложений исходной информации шифрованными

Задание #14

Вопрос:

Укажите основные принципы обеспечения информационной безопасности в АСОИ

Выберите несколько из 6 вариантов ответа:

- 1) Системность
- 2) Комплексность
- 3) Закрытость алгоритмов и механизмов защиты
- 4) Гибкость управления и применения
- 5) Непрерывности защиты
- 6)

Задание #15

Вопрос:

В состав формальных моделей входят следующие модели:

Выберите несколько из 4 вариантов ответа:

- 1) модель избирательного разграничения доступа
- 2) мандатные модели
- 3) модель Кларка-Вилсона
- 4) модель Кларка-Вилсона

Задание #16

Вопрос:

При шифрования методом перестановки ...

Выберите один из 5 вариантов ответа:

- 1) символы шифруемого текста заменяются символами того же или другого алфавита в соответствие с заранее обусловленной схемой замены
- 2) символы открытого текста переставляются по определенному правилу в пределах некоторого блока этого текста
- 3) шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор
- 4) символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов
- 5) замена слов и предложений исходной информации шифрованными

Задание #17

Вопрос:

Конфиденциальность информации - это...

Выберите один из 4 вариантов ответа:

- 1) ее свойство быть неизменной в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий
- 2) ее свойство быть известной только допущенным и прошедшим проверку субъектам системы.
- 3) ее свойство быть доступной для авторизованных законных субъектов системы, готовность служб к обслуживанию запросов
- 4) некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы

Задание #18

Вопрос:

К основным непреднамеренным искусственным угрозам АСОИ относится

Выберите несколько из 5 вариантов ответа:

- 1) физическое разрушение системы путем взрыва, поджога и т.п
- 2) пересылка данных по неправильному адресу
- 3) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех
- 4) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств
- 5) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы

Задание #19

Вопрос:

В чем суть шифрования методом подстановки?

Выберите один из 5 вариантов ответа:

- 1) 2) символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности
- 3) шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор
- 4) символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов
- 5) замена слов и предложений исходной информации шифрованными

Задание #20

Вопрос:

Что понимают под преднамеренными угрозами?

Выберите один из 4 вариантов ответа:

- 1) перехват, ознакомление и разглашение секретной информации
- 2) изменение или искажение, приводящее к нарушению ее качества или полному уничтожению
- 3) создание таких ситуаций, когда определенные преднамеренные действия либо снижают работоспособность АСОИ, либо блокируют доступ к некоторым ее ресурсам
- 4) целенаправленные действия нарушителя

Вариант №2

Задание #1

Вопрос:

Асимметричный алгоритм шифрования - это ...

Выберите один из 4 вариантов ответа:

- 1) Метод защиты информации, где для шифрования и дешифрования информации используются различные ключи, причем ключи генерирует отправитель сообщения
- 2) Метод защиты информации, где для шифрования и дешифрования информации используются больше трех ключей
- 3) Метод защиты информации, где для шифрования и дешифрования информации используют астрономические методы
- 4) Метод защиты информации, где для шифрования и дешифрования информации используются различные ключи, причем ключи генерирует получатель сообщения

Задание #2

Вопрос:

Что включают в себя организационно-административные меры защиты?

Выберите несколько из 6 вариантов ответа:

- 1) разработку правил обработки информации в АСОИ
- 2) совокупность действий при проектировании и оборудовании вычислительных центров и других объектов АСОИ
- 3) резервирование ресурсов и компонентов АСОИ
- 4) совокупность действий при подборе и подготовке персонала
- 5) организацию скрытого контроля за работой пользователей и персонала АСОИ
- 6) идентификацию и аутентификацию субъектов АСОИ

Задание #3

Вопрос:

Какой ключ доступен всем для проверки ЭЦП?

Выберите один из 4 вариантов ответа:

- 1) закрытый
- 2) открытый
- 3) внутренний
- 4) приватный

Задание #4

Вопрос:

Сопоставьте основные каналы утечки информации с их значениями

Укажите соответствие для всех 4 вариантов ответа:

- 1) возможность анализа злоумышленником звуковых волн, распространяющихся в воздухе, возникающих при разговоре в закрытом помещении
- 2) электромагнитное поле, связанное с протеканием электрического тока в аппаратных компонентах АСОИ

3) Связан с возможностью локального или удаленного доступа злоумышленника к элементам АСОИ, к носителям информации, к программному обеспечению, к линиям связи

4) Связан с возможностью визуального наблюдения злоумышленником за работой устройств отображения информации в АСОИ без проникновения в помещения, используя скрытые системы видеонаблюдения

- ___ Электромагнитный канал
- ___ Виброакустический канал
- ___ Визуальный канал
- ___ Информационный канал

Задание #5

Вопрос:

В чем суть шифрования методом подстановки?

Выберите один из 5 вариантов ответа:

1) символы шифруемого текста заменяются символами того же или другого алфавита в соответствие с заранее обусловленной схемой замены

2) символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности

3) шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор

4) символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов

5) замена слов и предложений исходной информации шифрованными

Задание #6

Вопрос:

Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности - это метод ...

Выберите один из 5 вариантов ответа:

1) гаммирования

2) подстановки

3) кодирования

4) перестановки

5) аналитических преобразований

Задание #7

Вопрос:

К моделям доступа, базирующим на ролях относят

Выберите один из 5 вариантов ответа:

1) Модель безопасности Харрисона-Руззо-Ульмана

2) Политика безопасности Белла-ЛаПадулы

3) Модель Биба

4) Модель Кларка-Вилсона

5) Правильного ответа нет

Задание #8

Вопрос:

Основными типами угроз безопасности парольных систем являются следующие

Выберите несколько из 5 вариантов ответа:

- 1) Перебор паролей
- 2) Подсмотр пароля
- 3) Перехват вводимого пароля
- 4) Установление максимального срока действия пароля
- 5) Проверка и отбраковка пароля по словарю

Задание #9

Вопрос:

Что может быть использовано в качестве идентификатора?

Выберите несколько из 5 вариантов ответа:

- 1) бесконтактные радиочастотные карты
- 2) пластиковые карты
- 3) имя пользователя
- 4) секретный код
- 5) пин-код

Задание #10

Вопрос:

Конфиденциальность информации - это...

Выберите один из 4 вариантов ответа:

- 1) ее свойство быть неизменной в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий
- 2) ее свойство быть известной только допущенным и прошедшим проверку субъектам системы.
- 3) ее свойство быть доступной для авторизованных законных субъектов системы, готовность служб к обслуживанию запросов
- 4) некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы

Задание #11

Вопрос:

Что понимают под преднамеренными угрозами?

Выберите один из 4 вариантов ответа:

- 1) перехват, ознакомление и разглашение секретной информации
- 2) изменение или искажение, приводящее к нарушению ее качества или полному уничтожению
- 3) создание таких ситуаций, когда определенные преднамеренные действия либо снижают работоспособность АСОИ, либо блокируют доступ к некоторым ее ресурсам
- 4) целенаправленные действия нарушителя

Задание #12

Вопрос:

Стандарт шифрования данных ГОСТ - это ...

Выберите один из 4 вариантов ответа:

- 1) 64 битовый блочный алгоритм с 256 битовым ключом
- 2) 64-битовый блочный алгоритм с 56 битовым ключом

3) блок данных представляется в виде двухмерного байтового массива размером 4X4, 4X6 или 4X8

4) 64-битовый блочный алгоритм с 48 битовым ключом

Задание #13

Вопрос:

К основным преднамеренным искусственным угрозам АСОИ относится:

Выберите несколько из 5 вариантов ответа:

- 1) пересылка данных по ошибочному адресу абонента
- 2) физическое разрушение системы путем взрыва, поджога и т.п.
- 3) неправомерное отключение оборудования или изменение режимов работы устройств и программ
- 4) игнорирование организационных ограничений (установленных правил) при работе в системе
- 5) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

Задание #14

Вопрос:

Какая длина ключа в ГОСТ 28147-89? (ответ в битах)

Запишите число:

Задание #15

Вопрос:

Какая схема лежит в основе алгоритмов шифрования DES и ГОСТ 28147-89?

Выберите один из 5 вариантов ответа:

- 1) Цезаря
- 2) Кантора
- 3) Фейстеля
- 4) Вижинера
- 5) Эль-гамала

Задание #16

Вопрос:

Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста - это метод ...

Выберите один из 5 вариантов ответа:

- 1) гаммирования
- 2) подстановки
- 3) кодирования
- 4) перестановки
- 5) аналитических преобразований

Задание #17

Вопрос:

В состав формальных моделей входят следующие модели:

Выберите несколько из 4 вариантов ответа:

- 1) модель избирательного разграничения доступа
- 2) мандатные модели
- 3) модель Кларка-Вилсона
- 4) модель Биба

Задание #18

Вопрос:

Целостность информации - это...

Выберите один из 4 вариантов ответа:

- 1) ее свойство быть неизменной в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий
- 2) ее свойство быть известной только допущенным и прошедшим проверку субъектам системы.
- 3) ее свойство быть доступной для авторизованных законных субъектов системы, готовность служб к обслуживанию запросов
- 4) некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы

Задание #19

Вопрос:

Доступность информации - это...

Выберите один из 4 вариантов ответа:

- 1) ее свойство быть неизменной в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий
- 2) ее свойство быть известной только допущенным и прошедшим проверку субъектам системы.
- 3) ее свойство быть известной только допущенным и прошедшим проверку субъектам системы.
- 4) некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы

Задание #20

Вопрос:

К основным непреднамеренным искусственным угрозам АСОИ относится

Выберите несколько из 5 вариантов ответа:

- 1) физическое разрушение системы путем взрыва, поджога и т.п
- 2) пересылка данных по неправильному адресу
- 3) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех
- 4) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств
- 5) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы