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

Теоретические основы компьютерной безопасности
(наименование учебной дисциплины)

10.04.01 Информационная безопасность (профиль) «Защищенные информационные системы»
(код и наименование ОПОП ВО)

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

Тема 1. Основные аспекты построения системы информационной безопасности.

1. Основные объекты информационной безопасности
2. Что является основными рисками информационной безопасности
3. Что относят к основным принципам обеспечения информационной безопасности
4. Что является принципом политики информационной безопасности

Тема 2. Угрозы информационной безопасности, оценка риска их возникновения.

1. Что относят к правовым методам обеспечения информационной безопасности
2. Перечислите виды информационной безопасности
3. Цели информационной безопасности
4. Что является угрозой информационной системы

Тема 3. Персональные данные, защита авторских прав.

1. В каком нормативном правовом акте закреплены все виды конфиденциальной информации?
2. Что такое персональные данные в соответствии с ФЗ-152?
3. Какую информацию запрещено относить к конфиденциальной в соответствии с законом РФ?
4. Раскройте понятие "конфиденциальный документ"
5. Перечислите 4 вида тайн относящихся к персональным данным. В случае если Вам известно больше видов тайн относящихся к ПД их следует перечислить.

Тема 4. Выявление контрафактной продукции.

1. Какие преимущества и недостатки объективных и эвристических методов экспертизы?
2. Что понимается под сенсорным анализом и сенсорной чувствительностью?
3. Что такое порог чувствительности, распознавания?
4. Причины фальсификации продовольственных товаров в современных условиях

5. . Место и роль идентификации при оценке степени соответствия товара

Тема 5. Криптографические методы защиты.

1. Что такое шифрование?
2. Что такое кодирование?
3. Для восстановления защитного текста требуется
4. Сколько лет назад появилось шифрование?
5. Первое известное применение шифра

Тема 6. Методы выбора системы защиты информации.

1. Какую длину имеет IP-адрес
2. Какую длину блока использует алгоритм DES
3. Какую длину ключа использует алгоритм DES
4. Для чего используется алгоритм Диффи-Хеллмана

Критерии оценки:

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

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

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

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

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа № 1 «Анализ защищенности вычислительной системы»

1. Назовите основной элемент информационной безопасности сетевой инфраструктуры
2. Какое программное средство было разработано ООО "Позитив Технолождис"
3. Какие программные средства используются для анализа защищенности операционных систем Microsoft
4. Назовите основные составляющие программного комплекса Magnum v. 1.0.4
5. Какие механизмы защиты аккумулируются в операционных системах компьютеров

Практическая работа № 2 «Шифры полиалфавитной замены»

1. Как называется шифр, в котором каждый символ открытого текста заменяется некоторым, фиксированным при данном ключе, символом другого алфавита?
2. Каким образом в пропорциональных или монофонических шифрах уравнивается частота появления зашифрованных знаков?
3. В чем основной смысл всех методов многоалфавитной подстановки?
4. Как называется способ шифрования, в котором шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите?

Практическая работа № 3 «Потоковые шифры. Скремблирование бинарного потока данных»

1. Что такое криптостойкость?
2. Что такое скремблирование?
3. Требования, предъявляемые к современным криптографическим системам защиты информации
4. Суть метода перестановки

Практическая работа № 4 «Ассиметричные клиптоалгоритмы. Метод RSA»

1. На чем основана безопасность систем RSA?
2. Кроме алгоритма RSA часто используемыми алгоритмами асимметричного шифрования являются
3. Сколько ключей используется в криптографических преобразованиях

4. Преимуществами асимметричных криптографических алгоритмов являются
5. Для максимальной безопасности в алгоритме RSA выбираются

Практическая работа № 5 «Обработка на базе клеточных автоматов»

1. Что называется систематизацией информации
2. Где указывается информация о местоположении курсора
3. В состав персонального компьютера входит?
4. Процесс изучения строения и свойств оригинала с помощью модели называется

Практическая работа № 6 «Интеграция механизмов защиты в программное обеспечение»

1. На что приходиться основная масса угроз информационной безопасности
2. Какой вид идентификации и аутентификации получил наибольшее распространение
3. Заключительным этапом построения системы защиты является
4. Какие угрозы безопасности информации являются преднамеренными

Критерии оценки:

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

2-3 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.

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

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

и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1. Что называется систематизацией информации:
   а) обработка документа с целью получения новых данных
   б) разделение информации по определенному признаку
   в) кодирование данных
2. Выберите изменение формы представления информации:
   а) собака — dog
   б) домашний питомец — попугай
   в) собака — домашний питомец
3. Связанная с получением нового содержания, новой информации обработка:
   а) запись воспоминаний
   б) набор текста в текстовом редакторе и форматирование
   в) решение математической или логической задачи
4. Необходимо преобразовать текстовую информацию в математическую запись и найти ответ на вопрос задачи:
   «У одного мужика 23 овцы, а у другого на 7 больше. Сколько у них овец вместе? »
   а) 23 + (23 + 7) = 53
   б) 23 — (23 + 7) = 53
   в) 23 + (23 — 7) = 53
5. «Символ — … — строка — фрагмент текста», что в этом ряду пропущено:
   а) абзац
   б) слово
   в) предложение
6. Необходимо указать основную позицию пальцев на клавиатуре:
   а) ФЫВА — ОЛДЖ
   б) ОЛДЖ — ФЫВА
   в) АБВГ — ДЕЁЖ
7. Где указывается информация о местоположении курсора:
   а) в окне текстового редактора
   б) в строке состояния текстового редактора
   в) на панели задач

8. Сергей набирал на компьютере текст. Вдруг все буквы, вводимые им, стали прописными, что случилось:
   а) случайно нажал клавишу Caps Lock
   б) случайно нажал клавишу Num Lock
   в) сломался компьютер
9. Выберите предложение, где все пробелы стоят правильно:
   а) «Пора, что железо:куй, поколе кипит!»
   б) «Пора, что железо : куй , поколе кипит!»
   в) «Пора, что железо: куй, поколе кипит!»
10. Нина набирает очень длинное предложение, курсор «подошёл» к концу строки, а ей ещё нужно написать пару слов. Что она должна сделать, чтобы продолжить ввод предложения на следующей строке:
   а) перевести курсор в начало следующей строки с помощью мыши
   б) продолжать набор текста, не обращая внимания на конец строки, на новую строку курсор перейдёт автоматически
   в) перевести курсор в начало следующей строки
11. Если курсор находится внутри абзаца, что произойдет если нажать клавишу Enter:
   а) абзац разобьётся на два отдельных абзаца
   б) курсор переместится в конец текущей строки
   в) курсор останется на прежнем месте
12. Что представляет из себя редактирование текста:
   а) процесс передачи текстовой информации по компьютерной сети
   б) процесс внесения изменений в имеющийся текст
   в) процедуру считывания с внешнего запоминающего устройства ранее созданного текста
13. Положение курсора в слове с ошибкой отмечено чёрточкой: МО|АНИТОР. Какую клавишу нужно нажать, для исправления ошибки:
   а) Backspace
   б) Delete и Backspace
   в) Delete
14. Положение курсора в слове с ошибкой отмечено чёрточкой: ДИАГРАММ|МА. Какую клавишу нужно нажать, для исправления ошибки:
   а) Delete или Backspace
   б) только Delete
   в) только Backspace
15. Для чего служит клавиша Insert при работе с текстом:
   а) удаления символа слева от курсора
   б) переключения раскладки клавиатуры русская/латинская
   в) переключения режима вставка/замена
16. Что нужно нажать, чтобы переместить курсор в начало текста:
   а) Caps Lock

б) Ctrl + Home
в) Esc

17. Что называется фрагментом текста:
а) предложение
б) абзац
в) непрерывная часть текста
18. Что в первую очередь предусматривает копирование текстового фрагмента в текстовом редакторе:
а) выделение копируемого фрагмента
б) открытие нового текстового окна
в) выбор соответствующего пункта меню
19. Сколько раз фрагмент можно вставить в текст, если он был помещён в буфер обмена:
а) это зависит от количества строк в данном фрагменте
б) один
в) столько раз, сколько требуется
20. Что называется буфером обмена:
а) раздел жёсткого магнитного диска
б) раздел оперативной памяти
в) часть устройства ввода
21. Буфер обмена предназначается для:
а) временного хранения копий фрагментов или удалённых фрагментов
б) передачи текста на печать
в) исправления ошибок при вводе команд
22. «Далеко за отмелью, в ельнике, раздалась птичья трель.» Сколько слов будет найдено в процессе автоматического поиска в этом предложении, если в качестве образца задать слово «ель»:
а) 2
б) 3
в) 1
23. Что необходимо указать для того, чтобы считать текстовый файл с диска:
а) имя файла
б) размеры файла
в) дату создания файла
24. В каком — то текстовом процессоре можно использовать только один шрифт и два варианта начертания — полужирное начертание и курсив. Сколько различных начертаний символов можно получить:
а) 3
б) 2
в) 4
25. Необходимо выбрать лишнее:
а) вставка
б) выравнивание

в) изменение цвета
г) изменение начертания

26. Если считать, что символ кодируется одним байтом, определите, чему равен информационный объём представленного высказывания: «Тысячи путей ведут к заблуждению, к истине — только один.»
а) 280 битов
б) 456 битов
в) 518 битов

27. Как называется этап подготовки текстового документа, на котором он заносится во внешнюю память:
а) форматированием
б) вводом
в) сохранением

28. В виде чего хранится на внешнем запоминающем устройстве текст, который был набран в текстовом редакторе:
а) файла
б) папки
в) каталога

29. В состав персонального компьютера входит?
А) Сканер, принтер, монитор
Б) Видеокарта, системная шина, устройство бесперебойного питания
В) Монитор, системный блок, клавиатура, мышь
Г) Винчестер, мышь, монитор, клавиатура

30. Все файлы компьютера записываются на?
А) Винчестер
Б) Модулятор
В) Флоппи-диск
Г) Генератор

31. Как включить на клавиатуре все заглавные буквы?
А) Alt + Ctrl
Б) Caps Lock
В) Shift + Ctrl
Г) Shift + Ctrl + Alt

32. Как называется основное окно Windows, которое появляется на экране после полной загрузки операционной среды?
А) Окно загрузки
Б) Стол с ярлыками
В) Рабочий стол
Г) Изображение монитора

33. Какую последовательность действий надо выполнить для запуска калькулятора в Windows?

А) Стандартные → Калькулятор
Б) Пуск → Программы → Стандартные → Калькулятор
В) Пуск → Стандартные → Калькулятор
Г) Пуск → Калькулятор

34. Как называется программа файловый менеджер, входящая в состав операционной среды Windows?
А) Проводник
Б) Сопровождающий
В) Менеджер файлов
Г) Windows commander

35. Для создания новой папки в программе Windows commander надо нажать на клавиатуре кнопку?
А) F5
Б) F6
В) F7
Г) F8

36. Для удаления файла в программе Windows commander следует нажать на клавиатуре кнопку?
А) F5
Б) F6
В) F7
Г) F8

37. Для запуска любой программы надо на рабочем столе Windows нажать на?
А) Ссылку на программу
Б) Ярлык программы
В) Кнопку запуска программы
Г) Рабочий стол

38.Для того, чтобы найти файл в компьютере надо нажать?
А) Пуск → Найти → Файлы и папки
Б) Пуск → Файлы и папки
В) Найти → Файл
Г) Пуск → Файл → Найти

39.Для настройки параметров работы мыши надо нажать?
А) Настройка → панель управления → мышь
Б) Пуск → панель управления → мышь
В) Пуск → настройка → мышь
Г) Пуск → настройка → панель управления → мышь

40.Как установить время, через которое будет появляться заставка на рабочем столе Windows?
А) Свойства: экран → Заставка → Интервал
Б) Заставка → Период времени
В) Свойства: экран → Заставка → Время
Г) Свойства: Интервал

41.Какие функции выполняет пункт Документы Главного меню Windows?
А) Пункт Документы Главного меню выводит список открытых в данный момент документов и позволяет переключаться между ними
Б) Пункт Документы Главного меню отображает список документов, с которыми работали последние 15 дней. Щелчок по названию или значку документа запускает приложение, с помощью которого он был создан и открывает документ
В) Пункт Документы Главного меню отображает список всех созданных документов и позволяет открыть любой из них
Г) Пункт Документы Главного меню выводит список последних открывавшихся документов. Щелчок по названию или значку документа запускает приложение, с помощью которого он был создан и открывает документ

42. С какой целью производится выделение объектов?
А) С целью группировки и создания тематической группы
Б) С целью последующего изменения их внешнего вида (изменения размера, вида значка и др.
В) С целью их сортировки
Г) С тем, чтобы произвести с ними какие-либо действия (открыть, скопировать, переместить и др.)

43. Как вызвать на экран контекстное меню?
А) Щелкнуть левой кнопкой мыши на объекте и в открывшемся списке выбрать команду "Контекстное меню"
Б) Открыть команду меню "СЕРВИС" и в ней выбрать команду "Контекстное меню"
В) Щелкнуть на объекте правой кнопкой мыши
Г) Дважды щелкнуть левой кнопкой мыши на объекте

44. В какой программе можно создать текстовый документ (отчет по научной работе)?
А) Windows Word
Б) Microsoft Word
В) Microsoft Excel
Г) Microsoft Power Point

45.Сколько документов можно одновременно открыть в редакторе Word?
А) Только один
Б) Не более трех
В) Сколько необходимо
Г) Зависит от задач пользователя и ресурсов компьютера

46. Открыть или создать новый документ в редакторе Microsoft Word можно используя панель?
А) Стандартная
Б) Форматирование
В) Структура
Г) Элементы управления

47. Для включения или выключения панелей инструментов в Microsoft Word следует нажать?
А) Вид → панели инструментов
Б) Сервис → настройка → панели инструментов
В) Щелкнув правой копкой мыши по любой из панелей
Г) Подходят все пункты а, б и в

48. Как создать новый документ "Стандартный отчет" из шаблонов Microsoft Word?
А) Файл → создать → общие шаблоны → отчеты → стандартный отчет
Б) Общие шаблоны → отчеты → стандартный отчет
В) Файл → отчеты → стандартный отчет
Г) Файл → создать → стандартный отчет

49. Для настройки параметров страницы Word надо нажать последовательность?
А) Файл → параметры страницы
Б) Файл → свойства → параметры страницы
В) Параметры страницы → свойства
Г) Правка → параметры страницы

50. Какие вирусы активизируются в самом начале работы с операционной системой:
а) загрузочные вирусы
б) троянцы
в) черви

51. Stuxnet — это:
а) троянская программа

б) макровирус
в) промышленный вирус

52. Таргетированная атака — это:
а) атака на сетевое оборудование
б) атака на компьютерную систему крупного предприятия
в) атака на конкретный компьютер пользователя

53. Под информационной безопасностью понимается:
а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре
б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
в) нет верного ответа

54. Защита информации:
а) небольшая программа для выполнения определенной задачи
б) комплекс мероприятий, направленных на обеспечение информационной безопасности
в) процесс разработки структуры базы данных в соответствии с требованиями пользователей

55. Информационная безопасность зависит от:
а) компьютеров, поддерживающей инфраструктуры
б) пользователей
в) информации

56. Конфиденциальностью называется:
а) защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
б) описание процедур
в) защита от несанкционированного доступа к информации

57. Для чего создаются информационные системы:
а) получения определенных информационных услуг
б) обработки информации
в) оба варианта верны

58. Кто является основным ответственным за определение уровня классификации информации:

а) руководитель среднего звена
б) владелец
в) высшее руководство

59. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:
а) хакеры
б) контрагенты
в) сотрудники

60. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству:
а) снизить уровень классификации этой информации
б) улучшить контроль за безопасностью этой информации
в) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

61. Что самое главное должно продумать руководство при классификации данных:
а) управление доступом, которое должно защищать данные
б) оценить уровень риска и отменить контрмеры
в) необходимый уровень доступности, целостности и конфиденциальности

62. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены:
а) владельцы данных
б) руководство
в) администраторы

Задания в открытой форме

1. К правовым методам относят…
2. Назовите виды информационной безопасности….
3. Назовите цели информационной безопасности….
4. К основным принципам обеспечения информационной безопасности относится…
5. Основными субъектами информационной безопасности являются:
6. К основным функциям системы безопасности можно отнести
7. Принципом информационной безопасности является принцип недопущения
8. Принципом политики информационной безопасности является принцип:

9. К основным типам средств воздействия на компьютерную сеть относится:
10. Когда получен спам по e-mail с приложенным файлом, следует:
11. ЭЦП – это:
12. Наиболее распространены угрозы информационной безопасности корпоративной системы:
13. Наиболее распространены средства воздействия на сеть офиса:
14. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
15. Угроза информационной системе (компьютерной сети) – это:
16. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
17. Окончательно, ответственность за защищенность данных в компьютерной сети несет:
18. Политика безопасности в системе (сети) – это комплекс:
19. Наиболее важным при реализации защитных мер политики безопасности является:
20. Что такое тактическое планирование?

Задания на установление соответствия

1. Установите взаимно однозначное соответствие

1	Идентификация	А	Может быть охарактеризован тем, какой пользователь обращается
2	Аутентификация	Б	Процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации – за счѐт этого каждый субъект или объект системы должен быть однозначно идентифицируем.
3	Запрос на доступ к ресурсу	В	Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа к ресурсу)

2. Установите взаимно однозначное соответствие функции памяти

1	Proximity	А	Чтение/Запись
2	Стандарт ISO/IEC 14443	Б	Чтение/Запись
3	Стандарт ISO/IEC 15693	В	Только чтение

3. Установите взаимно однозначное соответствие

1	аутентификации Kerberos	А	Принимает от пользователей запросы на аутентификацию
2	аутентификации RADIUS	Б	Был разработан специально для того, чтобы обеспечить надежную аутентификацию пользователей
3	Клиент RADIUS	В	рассматривается как механизм аутентификации и авторизации удалѐнных пользователей в условиях распределѐнной сетевой инфраструктуры, предоставляющий централизованные услуги по проверке подлинности и учѐту для служб удалѐнного доступа
4	Сервер RADIUS	Г	Заключается в централизованной обработке информации, предоставленной клиентами

4. Установите взаимно однозначное соответствие методы реализации систем одноразовых паролей

1	Метод "запрос-ответ"	А	В качестве исходной строки в нем используется не время, а количество успешных процедур аутентификации, проведенных до текущей
2	Метод "только ответ"	Б	В начале процедуры аутентификации пользователь отправляет на сервер свой логин. В ответ на

			это последний генерирует некую случайную строку и посылает ее обратно.
3	Метод "синхронизация по времени"	В	При этом в процессе создания строки используется значение предыдущего запроса
4	Метод "синхронизация по событию"	Г	При этом обычно используется не точное указание времени, а текущий интервал с установленными заранее границами (например, 30 секунд).

5. Установите взаимно однозначное соответствие

1	Ядро безопасности	А	Является одним из элементов ядра системы и предназначена для управления регистрацией в журнале событий, связанных с работой системы защиты
2	Ядро системы защиты	Б	локализованная, чѐтко ограниченная, изолированная совокупность программных и аппаратных механизмов, правильно реализующих функцию диспетчера доступа
3	Подсистема регистрации	В	Предоставляет средства для настройки защитных механизмов системы
4	Подсистема управления	Г	Представляет собой программу, которая автоматически запускается на защищаемом компьютере при его включении и функционирует на протяжении всего времени работы компьютера

6. Установите взаимно однозначное соответствие

1	Замкнутая программная среда	А	Предназначен для обеспечения гарантии того,

			что к моменту завершения загрузки ОС все ключевые компоненты СЗИ загружены и функционируют. Функциональный контроль осуществляется перед входом пользователя в систему
2	Функциональный контроль	Б	Предназначена для комплексной защиты информационных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах
3	Подсистема контроля аппаратной конфигурации компьютера	В	Позволяет сформировать для любого пользователя компьютера программную среду, определив индивидуальный перечень программ, разрешенных для запуска
4	СЗИ «Страж NT 2.0»	Г	Предназначена для своевременного обнаружения изменений в аппаратной конфигурации компьютера и реагирования на эти изменения и поддержания в актуальном состоянии списка устройств компьютера.

7. Установите взаимно однозначное соответствие

1	Пофайловое шифрование	А	Если зашифрован весь диск целиком, то операционная система не сможет запуститься, пока какой-либо механизм не расшифрует файлы загрузки
2	Шифрование каталогов	Б	Пользователь сам выбирает файлы, которые следует зашифровать

3	Шифрование виртуальных дисков	В	Пользователь создает папки, все данные в которых шифруются автоматически
4	Защита процесса загрузки	Г	Концепция виртуальных дисков реализована в некоторых утилитах компрессии, например Stacker или Microsoft DriveSpace

8. Установите взаимно однозначное соответствие

1	Контроль входа на компьютер	А	Это не позволит злоумышленнику в ваше отсутствие изменить какие-либо данные.
2	Контроль целостности файлов операционной системы	Б	При включении ПК устройство требует от пользователя ввести персональную информацию (например, вставить дискету с ключами)
3	Блок управления	В	Через него осуществляется основной обмен данными между устройством и компьютером.
4	Контроллер системной шины ПК	Г	основной модуль шифратора, который управляет работой всех остальных

9. Установите взаимно однозначное соответствие

1	Энергонезависимое запоминающее устройство	А	набор регистров, сумматоров, блоков подстановки и прочих элементарных схем, связанных между собой шинами передачи данных
2	Шифропроцессор	Б	обычно на базе микросхем флэш-памяти
3	Вычислитель	В	аппаратно реализованная программа (комбинационная схема конечного автомата), управляющая вычислителем

4	Блок управления	Г	специализированная микросхема или микросхема программируемой логики PLD

10. Установите взаимно однозначное соответствие

1	Несанкционированные (сторонние) процессы	А	Процессы, содержащие ошибки, ставшие известными, использование которых позволяет осуществить НСД к информации.
2	Критичные процессы	Б	Это процессы, которые не требуются пользователю для выполнения своих служебных обязанностей и могут несанкционированно устанавливаться на компьютер (локально, либо удаленно) с различными целями, в том числе, и с целью осуществления НСД к информации
3	Скомпрометированные процессы	В	К этой группе мы отнесем процессы, являющиеся средой исполнения (виртуальные машины как среды исполнения скриптов и апплетов, и офисные приложения как среды исполнения макросов).
4	Процессы, обладающие недекларированными (документально не описанными) возможностями	Г	К ним относят две группы процессов: те, которые запускаются в системе с привилегированными правами, например, под учетной записью System, и те, которые наиболее вероятно могут быть подвержены атакам, например, сетевые службы.

11.Установить соответствие между терминами и определениями

1	Объект защиты	А	информация, носители информации, технические средства и технология их обработки, а также средства защиты информации
2	Объект информатизации	Б	совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены
3	Защищаемые помещения (ЗП)	В	помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.)
4	Утечка информации по техническому каналу	Г	неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации

12. Установить соответствие классификации угроз

1	Состояние источника угрозы	А	в самой системе, что приводит к ошибкам в работе и сбоям при реализации ресурсов АС; в пределах видимости АС, например, применение подслушивающей аппаратуры, похищение информации в распечатанном виде или кража записей с носителей данных

2	Степень влияния	Б	активная угроза безопасности, которая вносит коррективы в структуру системы и ее сущность, например, использование вредоносных вирусов или троянов; пассивная угроза – та разновидность, которая просто ворует информацию способом копирования, иногда скрытая. Она не вносит своих изменений в информационную систему.
3	Возможность доступа сотрудников к системе программ или ресурсов		вредоносное влияние, то есть угроза информационным данным может реализоваться на шаге доступа к системе (несанкционированного); вред наносится после согласия доступа к ресурсам системы.
4	Способ доступа к основным ресурсам системы	Г	применение нестандартного канала пути к ресурсам, что включает в себя несанкционированное использование возможностей операционной системы; использование стандартного канала для открытия доступа к ресурсам, например, незаконное получение паролей и других параметров с дальнейшей маскировкой под зарегистрированного в системе пользователя.

13. Установить соответствие угроз безопасности информации в локальных размерах

1	Компьютерные вирусы	А	нарушающие информационную безопасность. Они оказывают воздействие на информационную систему одного компьютера или сети ПК после попадания в программу и самостоятельного размножения. Вирусы способны остановить действие системы, но в

			основном они действуют локально;
2	«Черви»	Б	модификация вирусных программ, приводящая информационную систему в состояние блокировки и перегрузки. ПО активируется и размножается самостоятельно, во время каждой загрузки компьютера. Происходит перегрузка каналов памяти и связи
3	«Троянские кони»	В	программы, которые внедряются на компьютер под видом полезного обеспечения. Но на самом деле они копируют персональные файлы, передают их злоумышленнику, разрушают полезную информацию

14. Установить соответствие между терминами и определениями

1	Автоматизированная система (АС)	А	система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функции
2	Контролируемая зона (КЗ)	Б	пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных, технических и иных материальных средств
3	Специальные исследования (СИ)	В	выявление с использованием контрольно-измерительной аппаратуры возможных каналов утечки защищаемой информации от основных и вспомогательных технических средств и систем
4	Специальная проверка (СП)	Г	проверка технических средств и систем объекта защиты с целью выявления возможно внедренных электронных устройств съема

			информации (закладочных устройств)

15. Установить соответствие между

1	Перехват паролей	А	мошенничество возможно с участием специальных программ, которые имитируют на экране монитора окошко для ввода имени и пароля. Введенные данные попадают в руки злоумышленника, и далее на дисплее появляется сообщение о неправильной работе системы.
2	«Маскарад»	Б	действия в информационной системе от лица другого человека в сети компании. Существуют такие возможности реализации планов злоумышленников в системе -передача ложных данных в системе от имени другого человека
3	Незаконное использование привилегий	В	название разновидности хищения информации и подрыва безопасности информационной системы говорит само за себя

16. Установить соответствие между излучениями каналов

1	Побочные электромагнитные излучения и наводки (ПЭМИН)	А	паразитные и побочные электромагнитные излучения радиоэлектронного оборудования и средств вычислительной техники. В зависимости от среды распространения различают
2	Побочные электромагнитные излучения (ПЭМИ)	Б	нежелательные (паразитные) электромагнитные излучения, возникающие при функционировании технических средств обработки информации, и приводящие к утечке обрабатываемой информации
3	Информативными ПЭМИ	В	сигналы, представляющие собой ВЧ несущую, модулированную

			информацией обрабатываемой на СВТ (например, изображением, выводимым на экран монитора, данными, обрабатываемыми на устройствах ввода-вывода и т.д.)
4	Неинформативными ПЭМИ	Г	сигналы, анализ которых может дать представление только о режиме работы СВТ и никак не раскрывает характер информации, обрабатываемой на СВТ

17. Установить соответствие между основными принципы защиты информации

1	Принцип законности	А	необходимо нормативно- правовое регулирование этой области общественных отношений. Законодательно должны быть обозначены права различных субъектов в области защиты информации
2	Принцип защиты информации	Б	основополагающие идеи, важнейшие рекомендации по организации и осуществлению этой деятельности на различных этапах решения задач сохранения секретов
3	Принцип приоритета	В	объектом засекречивания не могут быть сведения, которые государство обнародует или сообщает согласно конвенциям или соглашениям
4	Принцип собственности и экономической целесообразности	Г	право собственникам информации принимать меры к защите этой информации, а также оценивать ее потребительские свойства

18. Установить соответствие между терминами и определениями

1	Специальные обследования помещений	А	комплекс мер в области защиты информации в части проведения работ по выявлению электронных устройств,

			предназначенных для негласного получения сведений в помещениях, где циркулирует информация ограниченного пользования
2	Аттестация объекта защиты	Б	официальное подтверждение наличия на объекте защиты необходимых и достаточных условий, обеспечивающих выполнение установленных требований РД по ЗИ
3	Основные технические средства и системы	В	технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации
4	Нормирование показателей защищенности	Г	установление нормативными документами численных значений показателей защищенности информации

19. Установить соответствие между элементами и функциями

1	Дробление	А	знание какой-то одной части информации не позволяет восстановить всю технологию в целом
2	Кодирование	Б	метод защиты информации, преследующий цель скрыть от соперника содержание защищаемой информации и заключающийся в преобразовании с помощью кодов открытого текста в условный при передаче информации по каналам связи
3	Шифрование	В	метод защиты информации, используемый при передаче сообщений с помощью различной радиоаппаратуры, направлении письменных сообщений и в других случаях, когда есть опасность перехвата этих сообщений соперником

20. Установить соответствие между элементами и функциями

1	Случайные антенны	А	вспомогательные технические средства, их соединительные линии, а также линии электропитания, посторонние проводники и цепи заземления, при непосредственном подключении к которым средств разведки ПЭМИН возможен перехват информационных сигналов
2	Сосредоточенные	Б	телефонный аппарат, громкоговоритель радиотрансляционной сети, датчик пожарной сигнализации и т. д., подключенные к линии, выходящей за пределы КЗ
3	Распределенные	В	кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы КЗ

Задания на установление правильной последовательности

1. 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

2. 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

3. 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

4. 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

5. 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

6. 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

7. 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

8. 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»

9. 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

10. 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

11. 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

12. 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

13. Расположите в правильном порядке объекты защиты

1. __класс. Ценность данных определяется их собственником (коммерческая тайна)
2. __класс. Данные имеют ограниченный доступ на основании федеральных законов (персональные данные, банковская тайна)
3. __класс — государственная тайна.
Информационные объекты, имеющие ценность, присутствуют в жизни организации в виде

14. Расположить этапы процесса комплекса превентивных мер

1.подача и рассмотрение заявки;
2. предварительное ознакомление специалистов с аттестуемыми объектами;
3.разработка программы и методики испытаний;
4. запрос и получение специалистами необходимой технической документации;
5. проведение испытаний;
6. оформление, регистрация и выдача аттестата (сертификата соответствия) на оборудование и помещения.

15. Восстановите алгоритм испытаний

1. анализ информационных потоков, информационной системы в целом и отдельных объектов, технических средств, программного обеспечения, технической документации на внедренную систему защиты ИС в целом и от утечек по техническим каналам (ТКУИ);
2.оценка правильности классификации информационных объектов, выбора и применения технических средств защиты для блокирования опасных ТКУИ, возможных угроз несанкционированного доступа к информации и специальных воздействий на информацию (носители);
3. проверка сертификатов на программное обеспечение и техническое оборудование для защиты информации;
4. проведение аттестационных испытаний и оформление протоколов;
5.оформление заключения по результатам проверок.

16. Расположите этапы применения фреймворка управления рисками (NIST SP 800-37)
1. оценка внедренных мер защиты для определения корректности их применения, работоспособности и продуцирования ими результатов, удовлетворяющих требованиям безопасности и конфиденциальности
2. подготовка, т.е. определение целей и их приоритизация с точки зрения организации и ИТ-систем
3. внедрение мер защиты и описание того, как именно применяются меры защиты

4. категоризация систем и информации на основе анализа возможного негативного влияния от потери информации
5. выбор базового набора мер защиты и их уточнение (адаптация) для снижения риска до приемлемого уровня на основе оценки риска
6. непрерывный мониторинг систем и примененных мер защиты для оценки эффективности примененных мер, документирования изменений, проведения оценки рисков и анализа негативного влияния, создания отчетности по состоянию безопасности и конфиденциальности.
7. формальное согласование/утверждение использования систем или мер защиты на основе заключения о приемлемости рисков

17. Установить этапы реализации в ОС механизмов безопасности в порядке их внедрения:

1. Создание кольцевой системы защиты процессора
2. Реализация аутентификации пользователя
3. Реализация многозадачности
4. Создание виртуальных контейнеров для запуска приложений

18. Выберите правильную последовательность этапов по созданию системы защиты персональных данных:

1. Опытная и промышленная эксплуатация
2. Проектный этап
3. Аттестация или декларирование
4. Предпроектный этап

19. Выберите правильную последовательность этапов разработки профиля защиты.

1. Анализ среды применения ИТ-продукта с точки зрения
2. безопасности.
3. Выбор профиля-прототипа.
4. Синтез требований.

20.Последовательность слов для понятия Компьютерная сеть – это

1. Обеспечивающего передачу
2. Устройства связи
3. Связанных с помощью
4. Данных между ними
5. Группа компьютеров

Шкала оценивания результатов тестирования: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения

составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 баллов (установлено положением П 02.016).

Максимальный балл за тестирование представляет собой разность двух чисел: максимального балла по промежуточной аттестации для данной формы обучения (36) и максимального балла за решение компетентностно-ориентированной задачи (6).

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

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

Соответствие 100-балльной и 5-балльной шкал

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

2.2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

1.Для передачи сообщений по телеграфу каждая буква русского алфавита (Е и Ё отождествлены) представляется в виде пятизначной комбинации из нулей и единиц, соответствующих двоичной записи номера данной буквы в алфавите (нумерация букв начинается с нуля). Например, буква А представляется в виде 00000, буква Б - 00001, буква Ч - 10111, буква Я - 11111. Передача пятизначной комбинации производится по кабелю, содержащему пять проводов. Каждый двоичный разряд передается по отдельному проводу. При приеме сообщения перепутали провода, поэтому вместо переданного слова получен набор букв ЭАВЬЩО. Найдите переданное слово. «ПАРОЛЬ»

2.При шифровании открытый текст разбивается на блоки одинаковой длины и в каждом блоке осуществляется перестановка букв по одной и той же схеме. Восстановите исходное сообщение по криптограмме.

ПЬОКМ РХТЮЕ ШИРОО МОПЙО ККНЩИ ТОИРП ФАРГА

(45213) (45213) ….

КОМПЬЮТЕР ХОРОШИЙ ПОМОЩНИК КРИПТОГРАФА

3.Коммерсант для передачи цифровой информации с целью контроля передачи разбивает строчку передаваемых цифр на пятерки и после каждых двух пятерок приписывает две последние цифры от суммы чисел, изображенных этими пятерками. Затем процесс шифрования осуществляется путем прибавления к шифруемым цифрам членов арифметической прогрессии с последующей заменой сумм цифр остатками от деления на 10. Прочитайте зашифрованное сообщение:

6. 4 2 3 4 6 1 4 0 5 3 1 3.

4.Буквы русского алфавита занумерованы в соответствии с таблицей: Для зашифровки сообщения, состоящего из n букв, выбирается ключ K - некоторая последовательность из n букв приведенного выше алфавита. Шифрование каждой буквы сообщения состоит в сложении ее номера в таблице с номером соответствующей буквы ключевой последовательности и замене полученной суммы на букву алфавита, номер которой имеет тот же остаток от деления на 30, что и эта сумма. Прочтите шифрованное сообщение: РБЬНПТСИТСРРЕЗОХ, если известно, что шифрующая последовательность не содержала никаких букв, кроме А, Б и В.

5.Тридцати двум буквам русского алфавита А, Б, В, ..Э, Ю, Я приписаны соответственно числа 1, 2, 3, ..30, 31, 0 (буквы Е и Ё отождествляются). Выбрано некоторое нечетное число k (секретный ключ). Шифрование текста осуществляется побуквенно следующим образом:

1) число a, соответствующее данной букве, умножается на k,

2) вычисляется остаток r от деления a*k на 32

3) выписывается буква, соответствующая числу r.

Расшифруйте криптограммы:

1. ЕЦВ РФЗФЧНЙОЯ ЗМСФЦМ АМХХЛЭ

2. ЦОДШФДЮ ПКЫМЙМЯ

3. ЁРЪЫШРЫЪЩДБ ПЪДЛЪКООВЪДАКЩВБ

6.Рассмотрим модель шифра для цифрового текста, в котором каждая цифра заменяется остатком от деления значения многочлена

f(x) = b(x3 + 7x7 + 3x + a) на число 10, где a, b — фиксированные натуральные числа. Выяснить, при каких значениях a и b возможно однозначное расшифрование.

А-00000 З-01000 Р-10000 Ш-11000

Б-00001 И-01001 С-10001 Щ-11001

В-00010 К-01010 Т-10010 Ъ-11010

Г-00011 Л-01011 У-10011 Ы-11011

Д-00100 М-01100 Ф-10100 Ь-11100

Е-00101 Н-01101 Х-10101 Э-11101

Ё-00110 О-01110 Ц-10110 Ю-11110

Ж-00111 П-01111 Ч-10111 Я-11111

7.Найти хеш–образ своей Фамилии, используя хеш–функцию $H_i = (H_{i-1} + M_i)^2 \bmod n$, гдеn = pq

8.Используя хеш-образ своей Фамилии, вычислите электронную цифровую подпись по схеме RSA.\

9.Зашифровать, используя алгоритм - RSA.

Шумит дубравушка к непогодушке

10. Зашифровать, используя алгоритм - RSA.

Утром вороны каркают к дождю

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.