Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 19.10.2022 13:21:09
Уникальный программный ключ:
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

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

Методы защиты программного обеспечения
(наименование учебной дисциплины)

10.03.01 Информационная безопасность, направленность (профиль) «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий»
(код и наименование ОПОП ВО)

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

Тема 1. Защита программного обеспечения.

1. Какие цели преследует защита ПО?
2. Перечислите способы защиты программных продуктов и БД.
3. Ключевые элементы, необходимые для выполнения программы.
4. Назовите средства исследования программ.

Тема 2. Методы защиты от исследования программ.

1. Перечислите виды отладочных механизмов.
2. Методы обнаружения модифицированного кода.
3. Основные категории требований к средствам обеспечения информационной безопасности
4. Эмуляторы процессора

Тема 3. Организационно-технические принципы защиты.

1. Структура синтеза системы защиты.
2. Что необходимо учитывать при формулировании требований к защите?
3. Какие этапы включает в себя процесс синтеза?
4. Опишем общую структуру синтеза системы защиты

Тема 4. Методы и средства защиты программ от компьютерных вирусов.

1. Определение компьютерного вируса.
2. Классификация компьютерных вирусов.
3. Троянские программы.
4. Процесс заражения программы.
5. Физическая структура вируса.

Тема 5. Методы защиты программного обеспечения от внедрения на этапе его эксплуатации и сопровождения программных закладок.

1. Перечислите методы защиты от компьютерных вирусов.
2. Каков основной принцип в основе разработки технологии защиты от вирусов?
3. Классификация средств исследования программ.
4. Методы защиты программ от исследования.
5. Компоненты защищаемой от исследования программы.
6. Дополнительные функции безопасности.
7. Назовите методы защиты программ от несанкционированных изменений.

Тема 6. Методы и средства обеспечения целостности и достоверности используемого программного кода..

1. Базовые криптографические понятия.
2. Почему в большинстве схем электронной подписи используются хэш-функции?
3. Внедрение РПС в авторскую программу
4. Эффективные методы защиты от злоумышленников

Тема 7. Основные подходы к защите программ от несанкционированного копирования.

1. Назовите основные функции средств защиты от копирования.
2. Каковы действия инсталлированной программы при запуске.
3. Назовите основные методы защиты от копирования.
5. Перечислите методы противодействия динамическим способам снятия защиты программ от копирования.

Критерии оценки:

- 2 балла по шкале БРС выставляется обучающемуся, если даны точные ответы, демонстрируется знание дополнительной литературы и материала, не раскрытого на лекции;

- 1 балла по шкале БРС выставляется обучающемуся, если имеется знание терминов и понятий, понимаются основные взаимосвязи процессов и явлений;

- 0 балла по шкале БРС выставляется обучающемуся, отсутствует знание базовых терминов и понятий, отсутствие понимания взаимосвязи понятий.

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ЛАБОРАТОРНЫХ РАБОТ

Лабораторная работа № 1 «Анализ структуры программных модулей с привязкой к архитектуре»

1. Какие понятия лежат в основе архитектурного проектирования?
2. Назовите факторы архитектурного решения
3. Что такое под уровни архитектуры программного обеспечения?
4. Какой признак является успешным в архитектуре ?

Лабораторная работа № 2 «Разработка адаптивного пользовательского интерфейса на базе web-технологий»

1. Зачем разрабатывают ТЗ?
2. Какими стандартами регулируется содержимое технического задания?
3. Какие существуют стадии и этапы разработки?
4. Раскройте понятие «время восстановления после отказа»

Лабораторная работа № 3 «Настройка интегрированной среды разработки и системы управления базами данных»

1. Сформулируйте определение интегрированной среды разработки программ.
2. Каковы основные компоненты интегрированной среды?
3. Назовите наиболее популярные интегрированные среды и их фирмы-разработчики.
4. Какую функциональность обеспечивала среда Турбо-Паскаль?

Лабораторная работа №4 «Разработка CRUD приложение на базе web-фреймворка»

1. Зачем нужная оптимизация
2. Основные технологии оптимизации
3. Основные психологические аспекты производительности
4. Основные стадии загрузки страницы

Лабораторная работа №5 «Реализация базового функционала API-сервера с применением системы контроля версий Git»

1. В чем заключается экономия времени при использовании системы контроля версий?
2. В чем преимущества использования системы контроля версий?
3. Что такое Git?
4. Как начать использовать git?

Лабораторная работа №6 «Подключение пользовательского интерфейса, контроль ошибок и отладка программы.»

1. Что такое трансляторы?
2. Перечислите стадии тестирования? (3шт)
3. Перечислите основные стадии тестирования?
4. При каком условии тест считается удачным?

Лабораторная работа №7 «Исследование защищенности и быстродействия работы API-функций на локальном сервере.»

1. Что такое тестирование API?
2. Каковы распространенные типы тестирования API?
3. Назовите некоторые из распространенных протоколов, используемых при тестировании API?
4. Какие архитектурные стили используются для создания веб-API?

Критерии оценки:

- 2 балла по шкале БРС выставляется обучающемуся, если даны точные ответы, демонстрируется знание дополнительной литературы и материала, не раскрытого на лекции;

- 1 балла по шкале БРС выставляется обучающемуся, если имеется знание терминов и понятий, понимаются основные взаимосвязи процессов и явлений;

- 0 балла по шкале БРС выставляется обучающемуся, отсутствует знание базовых терминов и понятий, отсутствие понимания взаимосвязи понятий.

1.3 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа № 1«Обзор pe-формата исполняемых файлов платформы win32»

1. Опишите структуру PE-файла.
2. Что такое DOS-заглушка?
3. Опишите формат заголовка PE-файла.
4. Что такое относительный виртуальный адрес?
5. Что такое точка входа? Почему при дизассемблировании необходимо правильно указывать еѐ адрес?
6. Как определить количество секций программы и характеристики каждой из них?
7. Что такое импортируемая функция? Где они расположены?

Практическая работа № 2«Изучение и отладка приложений win32 и способы изменения хода их выполнения с помощью отладчика уровня пользователя.»

1. Для чего необходима отладка программных средств?
2. Какие существуют методы и средства отладки программ?
3. Чем отличаются отладчики уровня пользователя от отладчиков уровня ядра?
4. Назовите выполняемые программными системами защиты информации машинные команды, которые являются наиболее критичными с точки зрения обеспечения информационной безопасности.
5. Назовите основные приѐмы изменения хода исполнения программ.
6. Что такое патч и каким образом происходит его создание?

Практическая работа № 3«Обнаружение ошибок и отладка программы.»

1. Перечислите виды ошибок, возникающих в процессе создания и эксплуатации программного обеспечения.
2. Как диагностируются ошибки, выявляемые компилятором VBA? В чем причина этих ошибок?
3. Какие ошибки могут возникнуть на этапе выполнения программы? В чем причина возникновения этих ошибок?

4. Что такое тест и как выполняется тестирование?
5. Каковы виды пошаговых режимов работы отладчика?
6. Какие существуют способы контроля над значениями переменных?
7. Как можно изменить значения переменных в процессе отладки программы?

Практическая работа № 4«Отладка параллельных MPI программ в среде Microsoft Visual Studio»

1. Как локально протестировать работоспособность параллельной
2. программы, разработанной для использования с библиотекой MS MPI до запуска ее на кластере?
3. Какое программное обеспечение должно быть установлено для этого на Вашей рабочей станции?
4. Перечислите и дайте краткое описание основным окнам среды
5. Microsoft Visual Studio 2005, используемым при отладке?
6. Что такое и для чего используются точки остановки? Что такое условные точки остановки?
7. Чем принципиальная особенность отладки параллельных MPI программ в среде Microsoft Visual Studio 2005?
8. Какие типичные ошибки при программировании с использованием технологии MPI Вы знаете?

Практическая работа № 5«Отладка программ и обработка ошибок»
1. Дайте определение тестированию.
2. Дайте определение отладки.
3. Назовите типы ошибок и дайте им определения.

Практическая работа № 6«Отладка программ с помощью GDB»
1. Что такое отладка программного обеспечения?
2. В каком режиме работает отладчик GDB?
3. Какие параметры командной строки использует GDB?
4. Каким образом должны быть подготовлены программы, чтобы их можно было исследовать с помощью GDB?
5. Как влияет уровень детализации отладочной информации на размер исполняемого файла?
6. Можно ли выделить отладочную информацию в отдельный файл? Если да, то каким образом?
7. Что такое «точка останова»? Сколько точек останова можно задать в процессе отладки программы? Можно ли задать условие срабатывания точки останова?
8. Какую информацию можно получить в процессе отладки программы?

Практическая работа № 7«Интеграция механизмов защиты с применением аппаратных ключей»

1. Электронные ключи Guardant. Электронный ключ Guardant Sign. Электронный ключ Guardant Code. Лицензирование сетевых приложений. Защищенные схемы продаж.
2. Электронные ключи Guardant. Guardant SP. Сервер активации. Принцип работы. Технические характеристики.
3. Электронные ключи Guardant. Выбор модели ключа. Защита Windows-приложений.
4. Электронные ключи Guardant. Выбор модели ключа. Удаленное обновление памяти ключа

Критерии оценки:

- 2 балла по шкале БРС выставляется обучающемуся, если даны точные ответы, демонстрируется знание дополнительной литературы и материала, не раскрытого на лекции;
- 1 балла по шкале БРС выставляется обучающемуся, если имеется знание терминов и понятий, понимаются основные взаимосвязи процессов и явлений;
- 0 балла по шкале БРС выставляется обучающемуся, отсутствует знание базовых терминов и понятий, отсутствие понимания взаимосвязи понятий.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 ТЕМЫ КУРСОВЫХ РАБОТ

1. Обеспечение доступа к ресурсам сети.
2. Анализ процедуры "быстрой" сортировки.
3. Обработка записей Базы Данных.
4. Редактирование строки на экране.
5. Автоматизация процессов подготовки документации на программное обеспечение.
6. Обработка текстов.
7. Клавиатурный тренажёр.
8. Графический редактор с ограниченным набором функций.
9. Редактирование текстов на экране.
10. Имитация электронной таблицы.
11. Игра в слова с компьютером.
12. Игра с компьютером. Составляем слова.
13. Игра с компьютером. "Города".
14. Игра "Пятнадцать".

15.Игра "Морской бой".

16.Игра "Ипподром".

17.Игра "Тезей".

18.Игра "Проще простого".

19.Игра в слова с компьютером "Балда".

20.Игра "Крисс - кросс".

Шкала оценивания курсовых работ (или курсовых проектов): 100-балльная.

Критерии оценивания:

85-100 баллов (или оценка «отлично») выставляется обучающемуся, если тема курсовой работы раскрыта полно и глубоко, при этом убедительно и аргументированно изложена собственная позиция автора по рассматриваемому вопросу; курсовая работа демонстрирует способность автора к сопоставлению, анализу и обобщению; структура курсовой работы четкая и логичная; изучено большое количество актуальных источников, включая дополнительные источники, корректно сделаны ссылки на источники; самостоятельно подобраны убедительные примеры; основные положения доказаны; сделан обоснованный и убедительный вывод; сформулированы мотивированные рекомендации; выполнены требования к оформлению курсовой работы.

70-84 баллов (или оценка «хорошо») выставляется обучающемуся, если тема курсовой работы раскрыта, сделана попытка самостоятельного осмысления темы; структура курсовой работы логична; изучены основные источники, правильно оформлены ссылки на источники; приведены уместные примеры; основные положения и вывод носят доказательный характер; сделаны рекомендации; имеются незначительные погрешности в содержании и (или) оформлении курсовой работы.

50-69 баллов (или оценка «удовлетворительно») выставляется обучающемуся, если тема курсовой работы раскрыта неполно и (или) в изложении темы имеются недочеты и ошибки; отмечаются отступления от рекомендованной структуры курсовой работы; количество изученных источников менее рекомендуемого, сделаны ссылки на источники; приведены самые общие примеры или недостаточное их количество; вывод сделан, но имеет признаки неполноты и неточности; рекомендации носят формальный характер; имеются недочеты в содержании и (или) оформлении курсовой работы.

0-49 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если тема курсовой работы не раскрыта и (или) в изложении темы имеются грубые ошибки; структура курсовой работы нечеткая или не определяется вообще; количество изученных источников значительно менее рекомендуемого, неправильно сделаны ссылки на источники или они отсутствуют; не приведены примеры или приведены неверные примеры;

отсутствует вывод или автор испытывает затруднения с выводами; не соблюдаются требования к оформлению курсовой работы.

2.2 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1. Из перечисленного аутентификация используется на уровнях:
1. Прикладном
2. сетевом
3. транспортном

2. Из перечисленного базовыми услугами для обеспечения безопасности компьютерных систем и сетей являются:
1. Аутентификация
2. контроль доступа
3. причастность
4. целостность

3. Из перечисленного в автоматизированных системах используется аутентификация по:

1. Паролю
2. Предмету
3. физиологическим признакам

4. Из перечисленного в обязанности сотрудников группы информационной безопасности входят:

1. расследование причин нарушения защиты
2. управление доступом пользователей к данным

5. Из перечисленного в ОС UNIX регистрационная запись средств аудита включает поля:
1. дата и время события
2. идентификатор пользователя
3. результат действия
4. тип события

6. Из перечисленного в ОС UNIX существуют администраторы:

1. Аудита
2. Печати
3. Системных утилит
4. Службы аутентификации

7. Из перечисленного в соответствии с видами объектов привилегии доступа подразделяются на:
1. базы данных
2. процедуры
3. сервер баз данных
4. события

8. Из перечисленного в файловых системах ОС UNIX права доступа к файлу определяются для:
1. Владельца
2. Всех основных пользователей
3. Членов группы владельца

9. Из перечисленного для аутентификации по личной подписи терминальных пользователей используются методы:
1. визуальное сканирование
2. исследование динамических характеристик движения руки

10. Из перечисленного для аутентификации по физиологическим признакам терминальных пользователей наиболее приемлемыми считаются:
1. Голос
2. Личная подпись
3. Отпечатки пальцев
4. Форма кисти

11. Из перечисленного для разграничения доступа к файлу применяются флаги, разрешающие
1. Выполнение
2. Запись
3. Чтение

12. Из перечисленного для СУБД важны такие аспекты информационной безопасности, как:

1. Доступность
2. Конфиденциальность
3. Целостность

13. Из перечисленного защита процедур и программ осуществляется на уровнях:

1. Аппаратуры
2. Данных
3. Программного обеспечения

14. Из перечисленного контроль доступа используется на уровнях:

1. Прикладном
2. Сетевом
3. Транспортном

15. Из перечисленного метка безопасности состоит из таких компонентов, как:
1. Категория
2. Области
3. Уровень секретности
16. Из перечисленного методами защиты потока сообщений являются:

1. Использование случайных чисел
2. Нумерация сообщений
3. Отметка времени

17. Из перечисленного на сетевом уровне рекомендуется применение услуг:

1. Аутентификация
2. Контроля доступа
3. Конфиденциальности
4. Целостности

18. Из перечисленного на транспортном уровне рекомендуется применение услуг:
1. Аутентификации
2. Контроля доступа
3. Конфиденциальности
4. Целостности

19. Из перечисленного объектами для монитора обращений являются:

1. Задания
2. Программы
3. Устройства
4. Файлы

20. Из перечисленного пользователи СУБД разбиваются на категории:

1. администратор базы данных
2. администратор сервера баз данных
3. конечные пользователи

21. Из перечисленного привилегии в СУБД могут передаваться:

1. Группам
2. Ролям
3. Субъектам

22. Из перечисленного привилегиями безопасности являются:

1. Createdb
2. Operator
3. Security; operator
4. Trace

23. Из перечисленного система брандмауэра может быть:

1. ПК
2. Маршрутизатором
3. Хостом

24. Из перечисленного структура ОС с точки зрения анализа ее безопасности включает уровни:

1. Внешний
2. Приложений
3. Сетевой
4. Системный

25. Из перечисленного субъектами для монитора обращений являются:

1. Порты
2. Программы
3. Терминалы

26. Из перечисленного функция подтверждения подлинности сообщения использует следующие факты:

1. доставка по адресу
2. неизменность сообщения при передаче
3. санкционированный отправитель

27. Из перечисленного электронная почта состоит из:

1. краткого содержания письма
2. прикрепленных файлов
3. тела письма

28. Из перечисленного, ГОСТ 28147-89 используется в режимах:

1. выработка имитовставки
2. гаммирование
3. гаммирование с обратной связью
4. простая замена

29. Из перечисленного, группами требований к документированию системы защиты информации являются:

1. обработка угроз
2. протоколирование
3. тестирование программ

32. Из перечисленного, группами требований к системам защиты информации являются:

1. Конкретные
2. Общие
3. Организационные

33. Из перечисленного, проблемами модели Белла-ЛаПадула являются:

1. завышение уровня секретности
2. запись вслепую
3. привилегированные субъекты
4. удаленная запись

34. Из перечисленного, различают модели воздействия программных закладок на компьютеры:

1. искажение
2. наблюдение и компрометация
3. перехват
4. уборка мусора

35. Из перечисленных категорий требований безопасности, в "Оранжевой книге" предложены:

1. аудит
2. корректность
3. политика безопасности

36. Из перечисленных множеств, модель безопасности Хартстона описывается множествами:

1. операции
2. пользователи
3. ресурсы
4. установленные полномочия

37. Из перечисленных программных закладок, по методу внедрения в компьютерную систему различают:

1. драйверные
2. загрузочные
3. прикладные
4. программно-аппаратные

38. Из перечисленных разделов, криптография включает:

1. криптосистемы с открытым ключом
2. симметричные криптосистемы
3. системы электронной подписи
4. управление ключами

39. Из перечисленных уровней безопасности, в "Европейских критериях" определены:

1. базовый
2. высокий
3. средний

40. Виды информационной безопасности:

1. Персональная, корпоративная, государственная
2. Клиентская, серверная, сетевая
3. Локальная, глобальная, смешанная

41. Основные объекты информационной безопасности:

1. Компьютерные сети, базы данных
2. Информационные системы, психологическое состояние пользователей
3. Бизнес-ориентированные, коммерческие системы

42. Основными рисками информационной безопасности являются:

1. Искажение, уменьшение объема, перекодировка информации
2. Техническое вмешательство, выведение из строя оборудования сети
3. Потеря, искажение, утечка информации

43. К основным принципам обеспечения информационной безопасности относится:

1. Экономической эффективности системы безопасности
2. Многоплатформенной реализации системы
3. Усиления защищенности всех звеньев системы

44. Принцип Кирхгофа:

1. Секретность ключа определена секретностью открытого сообщения
2. Секретность информации определена скоростью передачи данных
3. Секретность закрытого сообщения определяется секретностью ключа

45. ЭЦП – это

1. Электронно-цифровой преобразователь
2. Электронно-цифровая подпись
3. Электронно-цифровой процессор

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

1. Владелец сети
2. Администратор сети
3. Пользователь сети

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

1. Аудит, анализ затрат на проведение защитных мер
2. Аудит, анализ безопасности
3. Аудит, анализ уязвимостей, риск-ситуаций

48. Что такое процедура?

1. Правила использования программного и аппаратного обеспечения в компании
2. Пошаговая инструкция по выполнению задачи
3. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
4. Обязательные действия

49. Тактическое планирование – это:

1. Среднесрочное планирование
2. Долгосрочное планирование
3. Ежедневное планирование
4. Планирование на 6 месяцев

50. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?

1. Анализ связующего дерева
2. AS/NZS
3. NIST
4. Анализ сбоев и дефектов

Задания в открытой форме

1. Дизассемблирование - это получение из исполняемого …
2. Трассировка - это пошаговое …
3. Хвост - это часть вируса …
4. Термин "криптология" происходит от двух греческих слов …
5. Шифр (криптосистема) - способ, метод …
6. Шифрование - процесс применения …
7. Дешифрование - процесс, обратный …
8. Защита ПО преследует следующие цели …
9. Дизассемблер - программа, осуществляющая …
10. Отладчик - программа, предназначенная …
11. Эмулирующий отладчик - отладчик, который самостоятельно …
12. Первоначально исходя из общей архитектуры и назначения компьютерной системы определяют существенно важные элементы, связанные с …
13. MtE-вирусы делятся на …
14. stealth-*вирусы* - вирусы, пытающиеся быть …
15. Детекторы обеспечивают выявление вирусов посредством …
16. Фаги выполняют функции, свойственные …
17. Ревизоры обеспечивают слежение за состоянием …
18. Фильтрация. Заключается в использовании программ …

19. Вакцинация. Специальная обработка …
20. Статические методы предусматривают анализ текстов …

Задания на установление соответствия

1. Установить соответствие:

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

2. Установить соответствие:

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

3. Установить соответствие:

1) Точность результатов	a) Возможность совместного функционирования с некоторым оборудованием
2) Защищенность	b) Возможность совместного функционирования с другим программным обеспечением

3) Программная совместимость	c) Обеспечение конфиденциальности инф ормации;
4) Аппаратная совместимость	d) Обеспечение погрешности результатов не выше заданной;

4. Установить соответствие средства обеспечения информационной безопасности:

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

5. Установить соответствие:

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

6. Установить соответствие:

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

	секретного сообщения с целью его защиты.
3) Алфавит	c) Конечное множество используемых для кодирования информации символов.

7. Установить соответствие:

1) DES	a) Один из режимов использования блочного алгоритма шифрования.
2) ECB	b) Является блочным алгоритмом симметричного шифрования..
3) CBC	c) Режим сцепления блоков шифра.
4) BBS	d) Один из методов генерации псевдослучайных чисел.

8. Установить соответствие видов угроз:

1) Аппаратная	a) Когда возможен несанкционированный доступ к данным и их потеря.
2) Вероятность утечки	b) Когда существует вероятность нарушения работоспособности оборудования.
3) Нестабильность ПО	c) Когда есть вероятность некорректной работы программного обеспечения.

9. Установить соответствие оценки рисков в зависимости от факторов:

1) Высокий риск	a) Предполагается, что без снижения таких рисков обращение к информационной системе предприятия может оказать отрицательное влияние на бизнес;
2) Существенный риск	b) Здесь требуется эффективная стратегия управления рисками, которая позволит уменьшить или полностью исключить отрицательные последствия нападения;
3) Умеренный риск	c) Усилия по управлению рисками в данном случае не будут играть важной роли.

4) Незначительный риск	d) В отношении рисков, попавших в эту область, достаточно применить основные процедуры управления рисками;

10. Установить соответствие:

1) Правовая защита	a) Это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, которая исключает или ослабляет нанесение каких-либо убытков предприятию;
2) Организационная защита	b) Это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, которые обеспечивают защиту информации на правовой основе;
3) Инженерно-техническая защита	c) Это использование разнообразных технических средств, которые препятствуют нанесению убытков предприятию.

11. Установить соответствие средств информационной защиты:

1) Программы-антивирусы	a) Это специальные технологии, которые предотвращают потерю конфиденциальной информации. Как правило, данная технология используется большими предприятиями, так как требует больших финансовых и трудоресурсных затрат.
2) VPN	b) Борются с самыми распространенными вирусами, также способны восстанавливать поврежденные файлы.
3) DLP-решения	c) Это облачные решения для обеспечения антивирусной защиты вашего ресурса.

12. Установить соответствие каналов утечки:

1) Электрические	a) Электромагнитные излучения радиодиапазона

2) Оптические	b) Электромагнитные излучения в видимой, инфракрасной и ультрафиолетовой частях спектра
3) Акустические и виброакустические	c) Звуковые колебания в любом звукопроводящем материале или среде
4) Радиоканалы	d) Напряжение и ток в различных токопроводящих коммуникациях

13. Установить соответствие:

1) Программно-аппаратные (технические) методы	a) Для обеспечения безопасности используются приемы «перестраховки», с помощью которых исключается возможность ошибочного или несанкционированного проникновения в информационную систему
2) Физическая защита	b) Для осуществления информационной защиты используются специальные компьютерные технологии. С их помощью можно скрыть важные данные, не допустить утечки во время пересылки через интернет
3) Морально-этические методы	c) Профилактические действия, в основном, воспитательного характера
4) Технологические приемы	d) Мероприятия направлены на снижение риска потери данных и выявление лиц, пытающихся проникнуть на охраняемую территорию или в информационную систему

14. Установить соответствие степеней происхождения угрозы информационной безопасности:

1) Естественная	a) Данные угрозы, в свою очередь, делятся на 2 подкатегории: преднамеренная подкатегория — это действия хакеров, конкурентов, недобросовестных сотрудников и т. д., непреднамеренная — действия происходят из-за людей по их неосторожности.

2) Искусственная	b) Это те угрозы, которые не зависят от деятельности человека: землетрясения, ураганы, смерчи, дожди, молнии и т. д.
3) Внутренняя	c) Все угрозы, которые происходят вне системы.
4) Внешняя	d) Угроза исходит изнутри самой системы.

15. Установить соответствие:

1) OLE-automation или просто Automation	a) Технология, организующая доступ к данным разных компьютеров с учетом балансировки нагрузки сети.
2) ActiveX	b) Технология, обеспечивающая безопасность и стабильную работу распределенных приложений при больших объемах передаваемых данных.
3) MIDAS	c) Технология предназначена для создания программного обеспечения как сосредоточенного на одном компьютере, так и распределенного в сети.
4) MTS (Microsoft Transaction Server)	d) Технология создания программируемых приложений, обеспечивающая программируемый доступ к внутренним службам этих приложений

16. Установить соответствие каналов утечки:

1) Несанкционированное копирование, уничтожение или подделка информации	a) Ошибки персонала и пользователей
2) Перебои электропитания	b) Из-за некорректной работы программ
3) Случайное уничтожение или изменение данных	c) Потери информации, связанная с несанкционированным доступом
4) Потеря или изменение данных при ошибках по	d) Сбои оборудования, при котором теряется информация

17.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.

18. Установить соответствие между

1	Перехват паролей		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»		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		название разновидности хищения информации и подрыва безопасности информационной системы говорит само за себя

19. Установить соответствие между

	Процедуры управления операционным риском		анализ базы событий самооценка анализ динамики количественных показателей (ключевых индикаторов риска) анализ результатов регуляторных проверок анализ результатов внешнего аудита анализ поступающих сигналов от сотрудников.

	Сбор и регистрация информации о событиях операционного риска:		автоматизированное (из информационных систем), неавтоматизированное (экспертным методом), алгоритмизированное выявление информации о рисках классификация рисковых событий оценка потерь, стоимости возмещения потерь регистрация рисковых событий в базе событий обновление информации, актуализация источников информации.
	Мониторинг рисков:		анализ индикаторов риска и статистики контроль выполнения мероприятий мониторинг входящей информации.

20.Установите взаимно однозначное соответствие

1	Угрозы для безопасности	А	записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор.
2	Загрузочные вирусы	Б	угрозы, которые не соответствуют в точности определению вируса, троянского коня, червя и

			других категорий угроз, но могут представлять угрозы для компьютера и хранящихся на нем данных
3	Макро-вирусы	В	используют для своего распространения протоколы или команды компьютерных сетей и электронной почты
4	Сетевые вирусы	Г	заражают файлы-документы и электронные таблицы нескольких популярных редакторов

Задания на установление правильной последовательности

1. Установите последовательность Защита информации-

1. направленных на обеспечение целостности (неизменности), конфиденциальности
2.комплекс правовых, организационных и технических мер
3. доступности и сохранности информации

2. Установите последовательность Информация –

1. ведения о лицах, предметах, фактах, событиях
2. сведения о лицах, предметах, фактах, событиях
3. от формы их представления

3. Установите основные этапы оценки риска:
1. Сопоставление вероятности возникновения
2. Определение контрмер
3. Документирование
4. Идентификация угроз

4. Установите последовательность Система защиты информации-

1. установленным соответствующими нормативными правовыми актами в области защиты информации
2. информации, а также объектов защиты, функционирующих по правилам
3. совокупность органов и (или) исполнителей, используемой ими техники

4. в том числе техническими нормативными правовыми актами

5. 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

6. Установить этапы построения программы обеспечения безопасности:
1. Формирование политики безопасности организации
2. Проведение разъяснительных мероприятий и обучения персонала для поддержки требуемых мер безопасности
3. Регулярный контроль пошаговой реализации плана безопасности
4. Установление уровня безопасности
5. Определение ценности технологических и информационных активов организации

7. Установите последовательность Технические средства –

1. электрических, электромеханических,
2. реализуются в виде
3. электронных устройств

8. Установите последовательность Защиты программного обеспечения

1. изучить классификацию систем защиты программного обеспечения
2. проанализировать основные средства и методы защиты информации
3. проанализировать основные показатели эффективности системы защиты программного обеспечения
4. выявить достоинства и недостатки систем защиты программного обеспечения

9. Установить последовательность защиты от копирования

1. проверка расположения и содержимого «сбойных» секторов
2. запись информации в неиспользуемых секторах
3. проверка скорости чтения отдельных секторов

10. Установить последовательность Системы защиты ПО

1. системы, встраиваемые в исходный код ПО до компиляции\
2. системы, устанавливаемые на скомпилированные модули ПО

3. комбинированные

11. Установить последовательность механизмам защиты системы защиты можно классифицировать на

1. системы, использующие шифрование защищаемого ПО
2. комбинированные системы
3. системы, использующие сложные логические механизмы

12. Установить последовательность функционирования системы

1. упаковщики/шифраторы
2. системы защиты от несанкционированного копирования
3. системы защиты от несанкционированного доступа

13. Установить последовательность Локальная программная защита-

1. номера (ключа) при установке/запуске
2. требование ввода серийного
3. программного обеспечения

14. Установить последовательность Запутывание программного кода

1. внедряются ложные процедуры — «пустышки», холостые циклы, искажается
2. используются неупорядоченные переходы в различные части кода
3. количество реальных параметров процедур программы

15. Установить последовательность Технические средства защиты

1. аппаратные
2. программные
3. программно-аппаратные

16. Установите последовательность внутренней защиты

1. защита бд
2. защита ос
3. защита по

17. Установите последовательность обеспечения защиты

1. регистрация
2. контроль

3. уничтожение
4. имитация
5. сигнализация

18. Установите последовательность поражение вирусом

1. Активация вируса на пк
2. Выполнение пользователем некоторых действий
3. Заражение пк
4. Заражение удаленных пк

19. Установите последовательность этапов разработки профиля защиты.

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

20. Выберите правильную последовательность этапов защиты информации, информационных технологий и автоматизированных систем от атак:
1. Анализ рисков для активов организации, включающий в себя выявление ценных активов и оценку возможных последствий реализации атак с использованием скрытых каналов
2. Реализация защитных мер по противодействию скрытых каналов
3. Организация контроля за противодействием скрытых каналов.
4. Выявление скрытых каналов и оценка их опасности для активов организации

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

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

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

Общий балл по промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости

в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

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

2.2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

Компетентностно-ориентированная задача №1

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.

Компетентностно-ориентированная задача №2

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.

Компетентностно-ориентированная задача №3

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.

Компетентностно-ориентированная задача №4

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.

Компетентностно-ориентированная задача №5

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.

Компетентностно-ориентированная задача №6

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.

Компетентностно-ориентированная задача №7

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.

Компетентностно-ориентированная задача №8

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.

Компетентностно-ориентированная задача №9

Реализуйте автозагрузку правил файрвола при старте операционной системы. Запретите средствами операционной системы доступ к сетевым узлам по незащищённым протоколам

Компетентностно-ориентированная задача №10

Запретите доступ ко всем почтовым сервисам посредством браузера. Реализуйте запрет использования сервисов обмена мгновенным сообщениями средствами операционной системы

Компетентностно-ориентированная задача №11

Запретите незащищённые сетевые соединения средствами операционной системы

Компетентностно-ориентированная задача №12

Реализуйте доступ к почтовому сервису исключительно посредством почтовой программы (встроенной или сторонней)

Компетентностно-ориентированная задача №13

Реализуйте доступ к почтовому сервису только через браузер, исключив почтовые программы

Компетентностно-ориентированная задача №14

Установите возможность использования только регламентированного браузера

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.