**Тамбовское государственное автономное профессиональное**

**образовательное учреждение «Тамбовский бизнес-колледж»**

**Предметно-цикловая комиссия информационных технологий**

Утверждаю:

Директор ТОГАПОУ

«Тамбовский бизнес-колледж»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Н.В. Астахова

«30» августа 2017 г.

**Фонд оценочных средств**

текущего контроля и промежуточной аттестации по учебной дисциплине

**ПМ.02 «Разработка, внедрение и адаптация программного обеспечения отраслевой направленности»**

среднее профессиональное образование

(программа подготовки специалистов среднего звена)

09.02.05 Прикладная информатика (по отраслям)

Тамбов 2017

**Лист согласования**

**программы фонда оценочных средств учебной дисциплины**

**ПМ.02 «Разработка, внедрение и адаптация программного обеспечения отраслевой направленности»**

Рабочая программа является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности 09.02.05 Прикладная информатика (по отраслям) входящей в состав укрупненной группы специальностей 09.00.00 Информатика и вычислительная техника, в части освоения основного вида профессиональной деятельности: обработка отраслевой информации изучаемой в учреждениях среднего профессионального образования при подготовке квалифицированных специалистов среднего звена.

**Организация разработчик:**

Тамбовское областное государственное автономное профессиональное образовательное учреждение «Тамбовский бизнес-колледж»

**Разработчики:**

Туляков Д.В.. преподаватель ТОГАПОУ «Тамбовский бизнес-колледж».

Программа рассмотрена и рекомендована ПЦК информационных технологий ТОГАПОУ «Тамбовский бизнес-колледж»

Протокол № 1 от «28» августа 2017 г.

СОГЛАСОВАНО:

Коммерческий директор ИЦ «НАШ ГОРОД»

\_\_\_\_\_\_\_\_\_\_\_\_\_ В.А. Колесов

«28» августа 2017 г.

**АННОТАЦИЯ**

**программы фонда оценочных средств учебной дисциплины**

**ПМ.02 «Разработка, внедрение и адаптация программного обеспечения отраслевой направленности»**

ФОС является составной частью образовательной программы - ППССЗ по специальности 09.02.05 Прикладная информатика (по отраслям) и предназначен для оценки качества подготовки обучающихся и выпускников ППССЗ по специальности 09.02.05 Прикладная информатика (по отраслям).

Объектами оценки являются знания, умения и практический опыт как элементы общих и профессиональных компетенций.

В результате изучения дисциплины обучающийся должен иметь практический опыт:

* сбора и анализа информации для определения потребностей клиента;
* разработки и публикации программного обеспечения отраслевой направленности со статическим и динамическим контентом на основе готовых спецификаций и стандартов;
* отладки и тестирования программного обеспечения отраслевой направленности;
* адаптации программного обеспечения отраслевой направленности:
* разработки и ведения проектной и технической документации;
* измерения и контроля характеристик программного продукта.

Обучающийся в ходе освоения профессионального модуля **должен уметь:**

* проводить анкетирование и интервьюирование:
* строить структурно-функциональные схемы;
* анализировать бизнес-информацию с использованием различных методик;
* формулировать потребности клиента в виде четких логических конструкций;
* участвовать в разработке технического задания;
* идентифицировать, анализировать и структурировать объекты информационного контента;
* разрабатывать информационный контент с помощью языков разметки;
* разрабатывать программное обеспечение с помощью языков программирования информационного контента;
* разрабатывать сценарии;
* размещать информационный контент в глобальных и локальных сетях;
* использовать инструментальные среды поддержки разработки, системы управления контентом;
* создавать анимации в специализированных программных средах;
* работать с мультимедийными инструментальными средствами;
* осуществлять выбор метода отладки программного обеспечения;
* формировать отчеты об ошибках;
* составлять наборы тестовых заданий;
* адаптировать и конфигурировать программное обеспечение для решения поставленных задач;
* осуществлять адаптивное сопровождение программного продукта или информационного ресурса;
* использовать системы управления контентом для решения поставленных задач;
* программировать на встроенных алгоритмических языках;
* составлять техническое задание;
* составлять техническую документацию;
* тестировать техническую документацию;
* выбирать характеристики качества оценки программного продукта;
* применять стандарты и нормативную документацию по измерению и контролю качества;
* оформлять отчет проверки качества.

В результате освоения учебной дисциплины студент **должен знать:**

* отраслевую специализированную терминологию;
* технологии сбора информации;
* методики анализа бизнес-процессов;
* нотации представления структурно-функциональных схем;
* стандарты оформления результатов анализа;
* специализированное программное обеспечение проектирования и разработки информационного контента;
* технологические стандарты проектирования и разработки информационного контента;
* принципы построения информационных ресурсов;
* основы программирования информационного контента на языках высокого уровня;
* стандарты и рекомендации на пользовательские интерфейсы;
* компьютерные технологии представления и управления данными;
* основы сетевых технологий;
* языки сценариев;
* основы информационной безопасности;
* задачи тестирования и отладки программного обеспечения;
* методы отладки программного обеспечения:
* методы тестирования программного обеспечения;
* алгоритмизацию и программирование на встроенных алгоритмических языках;
* архитектуру программного обеспечения отраслевой направленности;
* принципы создания информационных ресурсов с помощью систем управления контентом;
* архитектуру и принципы работы систем управления контентом;
* основы документооборота;
* стандарты составления и оформления технической документации;
* характеристики качества программного продукта;
* методы и средства проведения измерений;
* основы метрологии и стандартизации.

В результате освоения дисциплины формируются компетенции:

OK 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес. проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество

ОК 3. Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации

ОК 9. Быть готовым к смене технологий в профессиональной деятельности.

ПК 2.1. Осуществлять сбор и анализ информации для определения потребностей клиента.

ПК 2.2.Разрабатывать и публиковать программное обеспечение и информационные ресурсы отраслевой направленности со статическим и динамическим контентом па основе готовых спецификаций и стандартов.

ПК 2.3.Проводить отладку и тестирование программного обеспечения отраслевой направленности.

ПК 2.4. Проводить адаптацию отраслевого программного обеспечения.

ПК 2.5. Разрабатывать и вести проектную и техническую документацию.

ПК 2.6. Участвовать в измерении и контроле качества продуктов.

Использование фонда оценочных средств направлено на достижение общеобразовательных, воспитательных и практических задач, на дальнейшее развитие личностных способностей и дальнейшего профессионального роста выпускника – будущего специалиста.

**СОДЕРЖАНИЕ**

|  |  |
| --- | --- |
|  | Стр. |
| 1. Паспорт фонда оценочных средств | 6 |
| 1.1. Область применения | 6 |
| 1.1.1 Карта компетенций | 6 |
| Показатели оценивания планируемых результатов обучения | 9 |
| 2. Контроль и оценка освоения теоретического и практического курса учебной дисциплины «Разработка, внедрение и адаптация программного обеспечения отраслевой направленности» | 9 |
| 2.1. Общие положения освоения учебной дисциплины по темам | 9 |
| 2.2. Задания для оценки освоения теоретического и практического курса учебной дисциплины | 9 |
| 3. Материалы для промежуточной аттестации по учебной дисциплине | 36 |
| 4. Критерии оценки | 39 |
| 5. Список рекомендуемой литературы. | 40 |

**1. Паспорт фонда оценочных средств**

**1.1. Область применения**

Комплект фонда оценочных средств предназначен для проверки результатов освоения учебной дисциплины ПМ.02 «Разработка, внедрение и адаптация программного обеспечения отраслевой направленности» программы подготовки специалистов среднего звена по специальности СПО 09.02.05 Прикладная информатика (по отраслям).

**1.1.1 Карта компетенций**

Таблица 1

|  |  |
| --- | --- |
| Контролируемые компетенции (шифр компетенции) | Планируемые результаты обучения (знает, умеет, владеет, имеет навык) |
| ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес. | **Знать:** возможности трудоустройства и варианты построения трудовой карьеры на базе профессии обучения; видов и типов предприятий, форм занятости для трудоустройства по профессии обучения |
| **Уметь:** обосновывать выбор своей будущей профессии, ее преимущества и значимость на современном рынке труда России |
| **Владеть:** возможностями использования умений и навыков, приобретенных в ходе изучения учебного курса (дисциплины), в будущей профессионально-трудовой деятельности |
| ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество | **Знать:** виды и типы проблем в профессиональной деятельности, обобщенные способы их разрешения; типов и видов планирования работ, построения планов-графиков профессиональной деятельности; возможности повышения профессиональной квалификации |
| **Уметь:** планировать профессиональную деятельность, самообразование и организовывать их выполнение в соответствии с планом; выбирать эффективный способ решения проблем при наличии альтернативы и обосновывать его |
| **Владеть:** практическим опытом планирования работ, исходя из целей и задач деятельности, определенных руководителем; выбора средств реализации целей и задач, поставленных руководителем |
| ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личного развития | **Знать:** типы и виды источников информации в профессиональной области, их особенности и способы получения, способов работы с информацией при разрешении профессионально-трудовых проблем. |
| **Уметь:** осуществлять поиск, обработку и представление информации в различных форматах (таблицы, графики, диаграммы, текст и т.д.), в том числе – с использованием компьютерных программ; выделять существенное содержание в технических инструкциях и регламентах |
| **Владеть:** практическим опыта самостоятельного поиска информации из различных источников (в том числе – профессиональных изданий, Интернета и т.д.), необходимой для решения профессионально- трудовых задач; обработки и представления информации в различных форматах для разных групп пользователей (в том числе – администрации, коллег, клиентов и т.д.) |
| ОК 5. Владеть информационной культурой, анализировать и оценивать информацию с использованием информационно-коммуникативных технологий | **Знать:** основы работы с текстовыми редакторами, электронными таблицами, электронной почтой, мультимедийным оборудованием; способов работы с информацией при разрешении профессионально-трудовых проблем. |
| **Уметь:** осуществлять поиск, обработку и представление информации в различных форматах, с использованием компьютерных программ; (электронные таблицы, графики, диаграммы, текст и т.д.) |
| **Владеть:** практическим опытом самостоятельного поиска информации с использованием информационно-коммуникационных технологий, необходимой для решения профессионально-трудовых задач; обработки и представления информации в различных форматах для разных групп пользователей (в том числе – администрации, коллег, клиентов и т.д.) |
| ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями. | **Знать:** основные профессиональные технические термины и определения профессиональной области |
| **Уметь:** грамотно разъясняться с коллегами на профессиональные темы; сформулировать задачу |
| **Владеть:** практическим опытом коллективного решения задач в профессиональной области |
| ОК 7. Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий. | **Знать:** ответственность за работу членов команды (подчиненных), результат выполнения заданий |
| **Уметь:** нести ответственность за работу членов команды (подчиненных), результат выполнения заданий |
| **Владеть:** практическим опытом несенияответственности за работу членов команды (подчиненных), результат выполнения заданий |
| ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься само-образованием, осознанно планировать повышение квалификации | **Знать:** принципы определения задачи профессионального и личностного развития |
| **Уметь:** самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации. |
| **Владеть:** навыками самостоятельного определения задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации. |
| ОК 9. Быть готовым к смене техно-логий в профессиональной деятельности. | **Знать:** основополагающие принципы функционирования технологий в профессиональной деятельности |
| **Уметь:** ориентироваться в условиях частой смены технологий в профессиональной деятельности |
| **Владеть:** навыками самостоятельного освоения новых методов и технологий в профессиональной деятельности |
| ПК 2.1. Осуществлять сбор и анализ информации для определения потребностей клиента. | **Знать:** принципы сбор и анализ информации. |
| **Уметь** выполнять сбор и анализ информации для определения потребностей клиента |
| **Владеть:** навыками сбор и анализ информации |
| ПК 2.2.Разрабатывать и публиковать программное обеспечение и информационные ресурсы отраслевой направленности со статическим и динамическим контентом па основе готовых спецификаций и стандартов. | **Знать:** теоретические основы работы с основными средами разработки кода программного продукта |
| **Уметь:** разрабатывать и публиковать программное обеспечение и информационные ресурсы отраслевой направленности па основе готовых спецификаций и стандартов |
| **Владеть:** практическими навыками программирования |
| ПК 2.3.Проводить отладку и тестирование программного обеспечения отраслевой направленности. | **Знать:** специализированные программные средства для отладки и тестирования программных модулей |
| **Уметь:** протестировать и отладить программное обеспечение |
| **Владеть:** практическими навыками отладки и тестирования программных модулей |
| ПК 2.4. Проводить адаптацию отраслевого программного обеспечения. | **Знать:** основные принципы адаптации отраслевого программного обеспечения |
| **Уметь:** адаптировать отраслевое программное обеспечение. |
| **Владеть:** навыкамиадаптации отраслевого программного обеспечения |
| ПК 2.5. Разрабатывать и вести проектную и техническую документацию. | **Знать:** принципы разработки и ведения проектной и технической документацию |
| **Уметь:** разрабатывать и вести проектную и техническую документацию. |
| **Владеть:** практическими навыками разработки и ведения проектной и технической документацию |
| ПК 2.6. Участвовать в измерении и контроле качества продуктов. | **Знать:** основные принципы измерения и контроля качества продуктов |
| **Уметь:** определить качество программного обеспечения |
| **Владеть:** навыкомизмерения и контроля качества продуктов |

1.1.2 Показатели оценивания планируемых результатов обучения

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Семестр | Шкала оценивания | | | |
| 2 | 3 | 4 | 5 |
| 5 семестр | ОК1-ОК9 | ОК1-ОК9, ПК2.1 | ОК1-ОК9, ПК2.1-2.3 | ОК1-ОК9,  ПК2.1-2.4 |
| 6 семестр | ОК1-ОК9, | ОК1-ОК9, ПК2.1, ПК2.2 | ОК1-ОК9, ПК2.1-2.4 | ОК1-ОК9,  ПК2.1-2.6. |

**2. Контроль и оценка освоения теоретического и практического курса учебной дисциплины «Разработка, внедрение и адаптация программного обеспечения отраслевой направленности»**

**2.1. Общие положения освоения учебной дисциплины по темам**

Основной целью оценки учебной дисциплины ПМ.02 «Разработка, внедрение и адаптация программного обеспечения отраслевой направленности» является оценка знаний и умений.

Оценка теоретического, практического курса учебной дисциплины ПМ.02 «Разработка, внедрение и адаптация программного обеспечения отраслевой направленности» осуществляется с использованием следующих форм и методов контроля: индивидуального и фронтального опроса, выполнения ситуационных заданий, тестирования.

**2.2. Задания для оценки освоения теоретического и практического** **курса учебной дисциплины:**

В процессе домашней подготовки к занятиям по соответствующей теме студенты должны:

- изучить конспект лекции;

- изучить рекомендованные по соответствующей теме учебники, учебные пособия, а также по своему усмотрению выбрать дополнительную литературу;

- подготовить ответы на вопросы, сформулированные в задании.

**3. Материалы для промежуточной аттестации по учебной дисциплине**

**ЗАДАНИЕ ДЛЯ СТУДЕНТОВ № 1**

**КОМПЛЕКТ ЗАДАНИЙ ДЛЯ тестирования**

1. ... - это элементы экономического потенциала, которыми располагает общество и которые могут быть использованы для достижения конкретной цели хозяйственной деятельности?

1. Объекты
2. **Ресурсы**
3. Имущество

2. Отдельные документы и отдельные массивы документов в ИС называются … ?

1. Энергические ресурсы
2. Материальные ресурсы
3. **Информационные ресурсы**
4. Все ответы верны

3. Что относится к целям защиты информации в условиях конкурентной борьбы рыночной экономике за информационные ресурсы?

1. Сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством
2. Обеспечение правого режима документированной информации как объекта собственности
3. Предотвращение разглашения, утечки и несанкционированный доступ к охраняемым сведениям
4. **Все ответы верны**

4. В чем заключалась основная задачи ИБ в I этапе ее развития (до 1816 года), который характеризуется использованием естественно возникавших средств информационных коммуникаций?

1. **Защита сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих для человека лично или сообщества жизненно важное значение**
2. Решались, в основном, методами и способами ограничения физического доступа к оборудованию средств добывания, переработки и передачи информации
3. Применение помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала).

5. В чем заключалась основная задачи ИБ в IV этапе ее развития (начиная с 1946 года), который характеризуется использованием и внедрением в практическую деятельность ЭВМ?

1. Защита сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих для человека лично или сообщества жизненно важное значение
2. **Решались, в основном, методами и способами ограничения физического доступа к оборудованию средств добывания, переработки и передачи информации**
3. Применение помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала).

6. В чем заключалась основная задачи ИБ в II этапе ее развития (начиная с 1816 года), который характеризуется началом использования искусственно создаваемых технических средств электро- и радиосвязи?

1. Защита сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих для человека лично или сообщества жизненно важное значение
2. Решались, в основном, методами и способами ограничения физического доступа к оборудованию средств добывания, переработки и передачи информации
3. **Применение помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала).**

7. Дайте определение ИБ, исходя из свойств информации (полнота, достоверность, своевременность).

1. Защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб.
2. **Состояние информационной среды, обеспечивающее удовлетворение информационных потребностей субъектов информационных отношений, безопасность информации и защиту субъектов от негативного информационного воздействия.**

8. Дайте определение защите информации согласно ГОСТу 350922-96?

1. **Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.**
2. Защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб.

9. Какими свойствами должна обладать информации для обеспечения ее эффективной безопасности?

1. Информация должна быть полной
2. Информация должна быть достоверной
3. Информация должна быть своевременной
4. **Все ответы верны**

10. Как трактуется понятие ИБ в Доктрине ИБ РФ?

1. **Состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности , общества и государства.**
2. Защита душевного здоровья телезрителя.
3. Выпуск бронированных коробочек для дискет.

11. Что из перечисленного не относится к числу основных задач(аспектов) информационной безопасности?

1. Доступность
2. **Масштабируемость**
3. Целостность
4. Конфиденциальность

12. Что из перечисленного относится к числу основных задач(аспектов) информационной безопасности?

1. Защита от копирования
2. **Доступность**
3. Масштабируемость
4. Правдивое отражение действительности

13. Что из перечисленного относится к числу основных задач(аспектов) информационной безопасности?

1. Защита от копирования
2. Масштабируемость
3. **Целостность**
4. Правдивое отражение действительности

14. Что из перечисленного относится к числу основных задач(аспектов) информационной безопасности?

1. Защита от копирования
2. Правдивое отражение действительности
3. Масштабируемость
4. **Конфиденциальность**

15. Что подразумевает под собой обеспечение доступности информации?

1. Предотвращением несанкционированного ознакомления с информацией
2. Предотвращение несанкционированной модификации или разрушение информации
3. **Возможность за приемлемое время получить требуемую информационную услугу, а также предотвращение несанкционированного отказа в получении информации**

16. Что подразумевает под собой обеспечение целостности информации?

1. Предотвращением несанкционированного ознакомления с информацией
2. **Предотвращение несанкционированной модификации или разрушение информации**
3. Возможность за приемлемое время получить требуемую информационную услугу, а также предотвращение несанкционированного отказа в получении информации

17. Что подразумевает под собой обеспечение конфиденциальности информации?

1. **Предотвращением несанкционированного ознакомления с информацией**
2. Предотвращение несанкционированной модификации или разрушение информации
3. Возможность за приемлемое время получить требуемую информационную услугу, а также предотвращение несанкционированного отказа в получении информации

18. Что относится к субъектам ИБ, отличающиеся друг от друга правовым, техническим, финансовым, организационным и иным ресурсным обеспечением?

1. **Отдельные граждане**
2. **Государство в целом**
3. Транспортные средства

19. Что не относится к субъектам ИБ, отличающиеся друг от друга правовым, техническим, финансовым, организационным и иным ресурсным обеспечением?

1. Коммерческие структуры
2. **Имущество**
3. Государственные организации

20. Что из перечисленного относится к числу уровней обеспечения ИБ?

1. Законодательный
2. Административный
3. Программно-технический
4. **Все ответы верны**

21. Чем характеризуется концептуально-политический уровень обеспечения ИБ?

1. **Принимаются документы, определяющие основные направления государственной политики в области ИБ, формулируются цели и задачи обеспечения ИБ в отношении субъектов ИБ и намечаются пути и средства реализации поставленных целей**
2. Принимаются нормативно-правовые акты, призванные инициировать создание и функционирование системы правового регулирования обеспечения ИБ

22. Чем характеризуется законодательный уровень обеспечения ИБ?

1. Принимаются документы, определяющие основные направления государственной политики в области ИБ, формулируются цели и задачи обеспечения ИБ в отношении субъектов ИБ и намечаются пути и средства реализации поставленных целей
2. **Принимаются нормативно-правовые акты, призванные инициировать создание и функционирование системы правового регулирования обеспечения ИБ**

23. Чем характеризуется нормативно-технический уровень обеспечения ИБ?

1. **Осуществляется разработка стандартов, руководящих и методических материалов и документов регламентирующих процессы разработки, внедрения и эксплуатации средств обеспечения ИБ**
2. Осуществление мероприятий по обеспечению безопасности проводится в рамках конкретного предприятия, учреждения, организации; руководство организации реализует конкретные меры по обеспечению ИБ

24. Чем характеризуется административный уровень обеспечения ИБ?

1. Осуществляется разработка стандартов, руководящих и методических материалов и документов регламентирующих процессы разработки, внедрения и эксплуатации средств обеспечения ИБ
2. **Осуществление мероприятий по обеспечению безопасности проводится в рамках конкретного предприятия, учреждения, организации; руководство организации реализует конкретные меры по обеспечению ИБ**

25. Чем характеризуется программно-технический уровень обеспечения ИБ?

1. **Предполагает использование нескольких механизмов обеспечения информационной безопасности: идентификация, криптография, протоколирование и аудит, экранирование, обеспечение высокой доступности, управление доступом к информации**
2. Поддержание работоспособности персонала и оборудования предприятия, физическая защита имущества и работников предприятия, управление персоналом предприятия

**Пакет преподавателя**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № задания | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| Правильный ответ | 2 | 3 | 4 | 1 | 2 | 3 | 2 | 1 | 4 | 1 | 2 | 2 | 3 | 4 | 3 | 2 | 1 | 1,2 | 2 | 4 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № задания | 21 | 22 | 23 | 24 | 25 |
| Правильный ответ | 1 | 2 | 1 | 2 | 1 |

**ЗАДАНИЕ ДЛЯ СТУДЕНТОВ № 2**

**КОМПЛЕКТ ЗАДАНИЙ ДЛЯ тестирования**

1. Объектно-ориентированный подход помогает справляться с ...?

* 1. **Сложностью системы**
  2. Недостаточной реактивностью систем
  3. Некачественным пользовательским интерфейсом

2. Объектно-ориентированный подход содержит … ?

* 1. Семантическую декомпозицию
  2. **Объектную декомпозицию**
  3. Алгоритмическую декомпозицию

3. \*\*\* - это абстракция множества сущностей реального мира, объединенных общностью структуры и поведения.

* 1. **Класс**
  2. Объект
  3. Символ

4. \*\*\* - это элемент класса, то есть абстракция определенной сущности.

* 1. Класс
  2. **Объект**
  3. Символ

5. Понятие "..." может трактоваться как способность объекта принадлежать более чем одному классу.

* 1. Наследование
  2. Инкапсуляция
  3. **Полиморфизм**

6. \*\*\* - означает построение новых классов на основе существующих с возможностью добавления или переопределения данных и методов.

* 1. **Наследование**
  2. Инкапсуляция
  3. Полиморфизм

7. Любой разумный метод борьбы со сложностью опирается на принцип:

* 1. Не следует умножать сущности сверх необходимости
  2. Отрицания отрицания
  3. **Разделяй и властвуй**

8. В число основных понятий объектного подхода не входят?

1. Инкапсуляция
2. Наследование
3. **Класс**

9. Структурный подход опирается на:

* 1. Семантическую декомпозицию
  2. **Алгоритмическую декомпозицию**
  3. Декомпозицию структур данных

10. Контейнеры в компонентах объектных средах предоставляют:

* 1. **Общий контекст взаимодействия с другими компонентами и окружением**
  2. Средства для сохранения компонентов
  3. Механизмы транспортировки компонентов

11. Требование безопасности повторного использования объектов противоречит:

1. **Инкапсуляции**
2. Наследованию
3. Полиморфизму

12. Предположим, что при разграничении доступа учитывается семантика программ. В таком случае на игровую программу могут быть наложены следующие ограничения:

1. Запрет на чтение каких-либо файлов, кроме конфигурационных
2. **Запрет на изменение каких-либо файлов, кроме конфигурационных**
3. Запрет на установление сетевых соединений

**Пакет преподавателя**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № задания | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Правильный ответ | 1 | 2 | 1 | 2 | 3 | 1 | 3 | 3 | 2 | 1 | 1 | 2 |

**ЗАДАНИЕ ДЛЯ СТУДЕНТОВ № 3**

**КОМПЛЕКТ ЗАДАНИЙ ДЛЯ тестирования**

1. Потенциальная возможность определенным образом нарушить информационную безопасность это …

1. Бомба
2. **Угроза**
3. Атака

2. Попытка реализации угрозы называется …

1. Бомба
2. Угроза
3. **Атака**

3. По каким критериям можно классифицировать угрозы?

1. **По аспекту ИБ**
2. По внутренним отказам ИС
3. **По способу осуществления**
4. **По компонентам ИС, на которые угрозы нацелены**

4. Окно опасности - это …

1. Плохо закрепленная деталь строительной конструкции.
2. **Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется.**
3. Часть пространства.

5. По отношению к поддерживающей инфраструктуре рассматриваются следующие угрозы:

1. Нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования
2. Разрушение или повреждение помещений
3. Невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности
4. **Все ответы верны**

6. Melissa - это

1. Бомба
2. **Вирус**
3. Червь

7. Код, обладающий способностью к распространению путем внедрения в другие программы называется …

1. "Червь"
2. Бомба
3. **Вирус**

8. Код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение называется …

1. **"Червь"**
2. Бомба
3. Вирус

9. Что относится к граням вредоносного программного обеспечения?

1. **Вредоносная функция**
2. **Способ распространения**
3. Агрессивного потребления ресурсов
4. **Внешнее представление**
5. Получения контроля над атакуемой системой

10. Самыми опасными источниками внутренних угроз являются:

1. Некомпетентные руководители
2. **Обиженные сотрудники**
3. Любопытные администраторы

11. Melissa - это

1. **Макровирус для файлов MS-Word**
2. Макровирус для файлов PDF
3. МСакровирус для файлов Postscript

12. Основными источниками внутренних отказов являются:

1. **Отступление (случайное или умышленное) от установленных правил эксплуатации**
2. Разрушение или повреждение помещений
3. **Отказы программного и аппаратного обеспечения**
4. Удаленные данные
5. **Разрушение данных**

13. Вредоносный код, который выглядит как функционально полезная программа, называется

1. "Червь"
2. Вирус
3. **Троянская программа**

**Пакет преподавателя**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № задания | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| Правильный ответ | 2 | 3 | 1,3,4 | 2 | 4 | 2 | 3 | 1 | 1,2,4 | 2 | 1 | 1,3,5 | 3 |

**ЗАДАНИЕ ДЛЯ СТУДЕНТОВ № 4**

**КОМПЛЕКТ ЗАДАНИЙ ДЛЯ тестирования**

1. Какие меры относятся к мерам защиты информации?

1. **правовые (законодательные)**
2. физиологические
3. **физические**
4. математические
5. **морально-этические**

2. Выберите из предложенного списка наиболее подходящий вместо звездочек (\*\*\*) термин. К (\*\*\*) защиты относятся действующие в стране законы, указы и другие нормативно-правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее получения, обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей.

1. **правовым (законодательным) мерам**
2. морально-этическим мерам
3. технологическим мерам
4. организационным (административным и процедурным) мерам
5. технические меры

3. Выберите из предложенного списка наиболее подходящий вместо звездочек (\*\*\*) термин. К (\*\*\*) защиты относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе.

1. правовым (законодательным) мерам
2. **морально-этическим мерам**
3. технологическим мерам
4. организационным (административным и процедурным) мерам

4. Выберите из предложенного списка наиболее подходящий вместо звездочек (\*\*\*) термин. К (\*\*\*) защиты относятся разного рода технологические решения и приемы, основанные обычно на использовании некоторых видов избыточности и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

1. морально-этическим мерам
2. организационным мерам
3. физическим мерам
4. **технологическим мерам**
5. технические меры

5. Выберите из предложенного списка наиболее подходящий вместо звездочек (\*\*\*) термин. (\*\*\*) защиты - это меры административного и процедурного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей и обслуживающего персонала с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

1. морально-этические меры
2. **организационные меры**
3. физические меры
4. технические меры
5. правовые меры

6. Выберите из предложенного списка наиболее подходящий вместо звездочек (\*\*\*) термин. (\*\*\*) защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также средств визуального наблюдения, связи и охранной сигнализации.

1. правовые меры
2. морально-этические меры
3. технические меры
4. организационные меры
5. **физические меры**

7. Выберите из предложенного списка наиболее подходящий вместо звездочек (\*\*\*) термин. (\*\*\*) защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав АС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты.

1. правовые меры
2. морально-этические меры
3. **технические меры**
4. организационные меры
5. физические меры

8. Что относится к основным принципам построения системы защиты?

1. **законность**
2. принципиальность
3. **системность**
4. наглость
5. **комплексность**

9. Что относится к основным принципам построения системы защиты?

1. **специализация и профессионализм**
2. **взаимодействие и координация**
3. уравновешенность
4. застенчивость
5. **обязательность контроля**

10. Что предполагает принцип "персональная ответственность"?

1. Предполагает создание благоприятной атмосферы в коллективах подразделении.
2. Предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения.
3. Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите АС и реализацию мер обеспечения безопасности информации на ранних стадиях разработки АС в целом и ее системы защиты информации, в частности.
4. **Предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого сотрудника в пределах его полномочий.**

11. Что предполагает принцип "обязательность контроля"?

1. Предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого сотрудника в пределах его полномочий.
2. **Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.**
3. Предполагает создание благоприятной атмосферы в коллективах подразделении.
4. Предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения.

12. В чем смысл принципа "простота применения средств защиты"?

1. Защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем.
2. Предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью.
3. **Механизмы зашиты должны быть интуитивно понятны и просты в использовании.**
4. Соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения.

13. В чем смысл принципа "открытость алгоритмов и механизмов защиты"?

1. **Защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем.**
2. Предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью.
3. Механизмы зашиты должны быть интуитивно понятны и просты в использовании
4. Соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения.

14. В чем смысл принципа "взаимодействие и сотрудничество"?

1. Предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью.
2. Механизмы зашиты должны быть интуитивно понятны и просты в использовании.
3. Предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого сотрудника в пределах его полномочий.
4. **Предполагает создание благоприятной атмосферы в коллективах подразделении.**
5. Предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения.

**Пакет преподавателя**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № задания | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| Правильный ответ | 1,3,4 | 1 | 2 | 4 | 2 | 5 | 3 | 1,3,5 | 1,2,5 | 4 | 2 | 3 | 1 | 4 |

**ЗАДАНИЕ ДЛЯ СТУДЕНТОВ № 5**

**КОМПЛЕКТ ЗАДАНИЙ ДЛЯ тестирования**

1. Идентификация и аутентификация - это …

1. **первая линия обороны, "проходная" информационного пространства организации**
2. программный продукт, разработанный в середине 1980-х годов
3. совокупность автоматизированных методов поведения

2. Перечислите виды аутентификации:

1. пользовательская
2. **односторонняя**
3. многосторонняя
4. **двусторонняя**

3. Субъект может подтвердить свою подлинность, предъявив одну из следующих сущностей:

1. нечто, что засекречено
2. **нечто, что он знает**
3. **нечто, чем он владеет**
4. **нечто, что есть часть его самого**

4. Какая компания является генератором одноразовых паролей системы S/KEY?

1. intuit
2. биометрия
3. kekberos
4. **Bellcore**

5. Что такое Kerberos?

1. **программный продукт, разработанный в середине 1980-х годов в Массачусетском технологическом институте и претерпевший с тех пор ряд принципиальных изменений**
2. нечто, что есть часть его самого
3. средство, устойчивое к пассивному прослушиванию сети

6. Что такое логическое управление доступом?

1. доверенная третья сторона
2. **основной механизм многопользовательских систем**
3. основный механизм многопользовательских систем

7. Каково основное достоинство произвольного управления?

1. разделенность
2. **гибкость**
3. доступность
4. мобильность

8. Каковы недостатки произвольного управления?

1. **рассредоточенность управления**
2. ввод пароля можно подсмотреть
3. **права доступа существуют отдельно от данных**
4. распространение пароля коллегам

9. Перечислите три категории функций, необходимых для администрирования РУД:

1. ликвидирующие функции
2. **информационные функции**
3. **вспомогательные функции**
4. **административные функции**

10. В чем различие между динамическим и статическим разделением обязанностей?

1. рассматриваются задачи
2. рассматриваются объекты
3. **рассматриваются роли, одновременно активные для данного пользователя**

11. Виды разделения обязанностей:

1. серверное
2. **динамическое**
3. клиентское
4. **статическое**

**Пакет преподавателя**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № задания | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| Правильный ответ | 1 | 2,4 | 2,3,4 | 4 | 1 | 2 | 2 | 1,3 | 2,3,4 | 3 | 2,4 |

**ЗАДАНИЕ ДЛЯ СТУДЕНТОВ № 6**

**КОМПЛЕКТ ЗАДАНИЙ ДЛЯ тестирования**

1. Какие функции выполняет экран?

* 1. **разграничение доступа**
  2. облегчение доступа
  3. усложнения доступа

2. На межсетевой экран целесообразно возложить функции:

1. активного аудита
2. анализа защищенности
3. **идентификации/аутентификации удаленных пользователей**

3. Экранирование на сетевом уровне может обеспечить?

1. **разграничение доступа по сетевым адресам**
2. выборочное выполнение команд прикладного протокола
3. контроль объема данных, переданных по TCP-соединению

4. Экран — это …?

1. средство, устойчивое к пассивному прослушиванию сети
2. **средство разграничения доступа клиентов из одного множества систем**
3. первая линия обороны, "проходная" информационного пространства организации

5. Какие функции выполняет экран?

1. ускорение обмена информацией
2. **протоколирование обмен информацией**
3. замедление обмена информацией

6. Демилитаризованная зона располагается

1. перед внешним межсетевым экраном
2. **между межсетевыми экранами**
3. за внутренним межсетевым экраном

7. Экранирование на сетевом и транспортном уровнях может обеспечить?

1. разграничение доступа по сетевым адресам
2. выборочное выполнение команд прикладного протокола
3. **контроль объеме данных, переданных по TCP-соединению**

8.Экран выполняет функции:

1. очистки некоторых элементов передаваемых данных
2. пополнении некоторых элементов передаваемых данных
3. **преобразование некоторых элементов передаваемых данных**

9. К межсетевым экранам целесообразно применить следующие принципы архитектурной безопасности6

1. усиление самого слабого звена
2. **эшелонированность обороны**
3. невозможность перехода в небезопасное состояние

10. Экранирование на сетевом и транспортном уровнях может обеспечить?

1. разграничение доступа по сетевым адресам
2. **выборочное выполнение команд прикладного протокола**
3. контроль объеме данных, переданных по TCP-соединению

**Пакет преподавателя**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № задания | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Правильный ответ | 1 | 3 | 1 | 2 | 2 | 2 | 3 | 3 | 2 | 2 |

**ЗАДАНИЕ ДЛЯ СТУДЕНТОВ № 7**

**КОМПЛЕКТ ЗАДАНИЙ ДЛЯ тестирования**

1. Информационный сервис считается недоступным, если:

1. **его эффективность не удовлетворяет наложенным ограничениям**
2. подписка на него стоит дорого
3. не удается найти подходящий сервис

2. Среднее время наработки на отказ:

1. пропорционально интенсивности отказов
2. **обратно пропорционально интенсивности отказов**
3. не зависит от интенсивности отказов

3. Достоинство синхронного тиражирования являются:

1. **идейная простота**
2. простота реализации
3. устойчивость к отказам сети

4. Эффективность информационного сервиса может измеряться как:

1. рентабельность работы сервиса
2. **максимальное время обслуживания запроса**
3. количество одновременно обслуживаемых пользователей

5. Интенсивности отказов независимых компонентов:

1. **складываются**
2. умножаются
3. возводятся в квадрат и складываются

6. Достоинствами асинхронного тиражирования являются:

1. идейная простота
2. простота реализации
3. **устойчивость к отказам сети**

7. Обеспечение высокой доступности можно ограничить:

1. критически важными серверами
2. сетевым оборудованием
3. **всей цепочкой от пользователя до серверов**

8. В число основных угроз доступности входит:

1. **отказ пользователя**
2. повышение цен на услуги связи
3. **отказ поддерживающей инфраструктуры**

9. Основными функциями ПО промежуточного слоя, существенными для высокой доступности, являются:

1. **маршрутизация запросов**
2. **балансировка загрузки**
3. доступность свободно распространяемых реализаций

10. Туннелирование может использоваться на следующих уровнях эталонной семиуровневой модели:

1. **канальном**
2. транспортном
3. сеансовом

11. Согласно стандарту Х.700, в число функций управления конфигурацией входит:

1. запуск и остановка компонентов
2. выбор закупаемой конфигурации
3. **изменение конфигурации системы**

12. Каркас необходим системе управления для придания:

1. гибкости
2. **жесткости**
3. устойчивости

13. Туннелирование может использоваться на следующих уровнях эталонной семиуровневой модели:

1. **сетевом**
2. сеансовом
3. уровне представления

14. Согласно стандарту Х.700, в число функций управления отказами входит:

1. предупреждение отказов
2. **выявления отказов**
3. **устранение отказов**

15. Выявление неадекватного поведения выполняется системами управления путем применения методов, типичных для:

1. систем анализ защищенности
2. **систем активного аудита**
3. систем идентификации

16. Согласно стандарту Х.700, в число функций управления безопасностью входит:

1. создание инцидентов
2. **реагирование на инциденты**
3. устранение инцидентов

17. Архитектурными элементами систем управления являются:

1. **агенты**
2. клиенты
3. **менеджеры**

**Пакет преподавателя**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № задания | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| Правильный ответ | 1 | 2 | 1 | 2 | 1 | 3 | 3 | 1,3 | 1,2 | 1 | 3 | 2 | 1 | 2,3 | 2 | 2 | 1,3 |

**ЗАДАНИЕ ДЛЯ СТУДЕНТОВ № 8**

**КОМПЛЕКТ ЗАДАНИЙ ДЛЯ тестирования**

1.Что такое операционная система?

1. программная оболочка, обеспечивающая взаимодействие пользователя с компьютером
2. программная оболочка, обеспечивающая взаимодействие пользователя с компьютером, доступ к принтерам, Интернет и другим сетевым устройствам
3. комплекс программ, который обеспечивает управление физическими устройствами компьютера
4. **комплекс программ, который обеспечивает управление физическими устройствами компьютера, доступ к файлам, ввод и вывод данных, выполнение и взаимодействие пользовательских программ**

2. Что такое вредоносная программа?

1. последовательность инструкций (команд), результат которых непредсказуем
2. **это программа, наносящая какой-либо вред компьютеру,на котором она запускается, или другим подключённым к нему компьютерам**
3. это программа, способная создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и /или файлы, системные области компьютера и прочие выполняемые объекты

3. Что такое локальная сеть?

1. **это компьютерная сеть, покрывающая относительно небольшую территорию - дом, школу, институт, микрорайон**
2. это компьютерная сеть, покрывающая большие территории - города, страны, континенты.
3. всемирная система объединенных компьютерных сетей.

4. Что такое компьютерная программа?

1. **последовательность инструкций (команд) для выполнения компьютером определенных действий**
2. последовательность действий, которые должен выполнить пользователь для получения от компьютера нужного ему результата
3. файл, при запуске которого компьютер начинает взаимодействовать с пользователем

5. Какой тип вирусов не относится к классу файловых вирусов?

1. макровирусы
2. **загрузочные вирусы**
3. скрипт-вирусы
4. классические файловые вирусы

6. Троян (троянский конь) – это программа… (продолжите фразу, выбрав наиболее точный вариант)

1. основной целью которой является незаметное проникновение в другую компьютерную систему
2. **основной целью которой является вредоносное воздействие по отношению к компьютерной системе**
3. основной целью которой является кража конфиденциальной информации
4. основной целью которой является обеспечение незаметного заражения вирусом или червем другой компьютерной системы

7. Утилиты скрытого удаленного управления относятся к классу:

1. файловых вирусов
2. макровирусов
3. сетевых червей
4. **троянов**

8. Чем занимаются клавиатурные шпионы?

1. **постоянно находясь в оперативной памяти, записывают все данные, поступающие от клавиатуры с целью последующей их передачи своему автору**
2. находясь в оперативной памяти следят за вводимой информацией. Как только пользователь вводит некое кодовое слово, клавиатурный шпион начинает выполнять вредоносные действия, заданные автором
3. находясь в оперативной памяти следят за вводимой пользователем информацией и по команде хозяина производят нужную ему замену одних символов (или групп символов) другими
4. передают хозяину марку и тип используемой пользователем клавиатуры

9. На какой тип делятся червь в зависимости от способа проникновения в систему?

1. сетевой червь
2. почтовый червь
3. IM-червь
4. IRC-червь
5. **Все ответы верны**

10. Что такое компьютерный вирус?

1. последовательность инструкций (команд), результат которых непредсказуем
2. это распространение на другие ресурсы компьютера и выполнение специальных действий при определенных событиях или действиях пользователя
3. **это программа, способная создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению**
4. Нет верных ответов

11. Какая группа не относится к проявлению вредоносных программ?

1. явная
2. скрытая
3. косвенная
4. **материальная**

12. К скрытым проявлениям вирусного заражения относятся:

1. наличие в оперативной памяти подозрительных процессов
2. наличие на компьютере подозрительных файлов
3. подозрительная сетевая активность
4. Наличие подозрительных ключей в системном реестре Windows
5. **Все ответы верны**

13. Для чего предназначена утилита netstat?

1. для просмотра текущей конфигурации сети
2. для получения отчета о посещенных пользователем сайтах
3. **для получения списка активных подключений, в который входят установленные соединения и открытые порты**
4. для получения отчета о сетевой активности за последний месяц (период с помощью ключей можно изменить)

14. Для чего предназначена системная утилита "Настройка системы" (msconfig.exe)?

1. для удаления троянов
2. **для настройки параметров автозагрузки**
3. для настройки сетевых параметров
4. для настройки внешнего вида окна

15. Выберите свойство вируса, позволяющее называться ему загрузочным

1. **способность заражать загрузочные сектора жестких дисков и мобильных носителей**
2. способность заражать загрузочные дискеты и компакт-диски
3. способность вызывать перезагрузку компьютера-жертвы
4. способность подсвечивать кнопку Пуск на системном блоке

16. Какой тип не выделяют среди троянов?

1. клавиатурные шпионы
2. похитители паролей
3. **шутки**
4. логические бомбы

17. В каком году произошла глобальная эпидемия червя Морриса?

1. **В 1988**
2. В 1989
3. В 1990
4. В 1991

18. Как назывался первый вирус для смартфонов?

1. LoveLetter (5 мая 2000 год)
2. **Cabir (июнь 2004 год)**
3. CodeRed (12 июля 2001 год)
4. Melissa (26 марта 1999 год)

19. Какой из перечисленных вирусов попал в Книгу Рекордов Гиннеса?

1. **LoveLetter (5 мая 2000 год)**
2. Cabir (июнь 2004 год)
3. CodeRed (12 июля 2001 год)
4. Melissa (26 марта 1999 год)

20. К явным проявлениям вредоносных программ относятся:

1. Изменение настроек браузера
2. Всплывающие и другие сообщения
3. Несанкционированный дозвон в Интернет
4. **Все ответы верны**

21. К косвенным проявлениям вредоносных программ относятся:

1. Блокирование антивируса и антивирусных сайтов
2. Сбои в системе или в работе других программ
3. Почтовые уведомления
4. **Все ответы верны**

22. Из скольких стадий состоит жизненный цикл червей?

1. двух
2. трех
3. четырех
4. **пяти**

23. Из скольких стадий состоит жизненный цикл троянов?

1. двух
2. **трех**
3. четырех
4. пяти

24. К каким вирусным программам относятся похитители паролей?

1. Файловые вирусы
2. Черви
3. **Трояны**
4. Загрузочные вирусы

25. Что такое файл?

1. **это логический блок информации, хранимой на носителях информации**
2. это совокупность правил, определяющих систему хранения информации
3. это последовательность инструкций (команд) для выполнения компьютером определенных действий.

**Пакет преподавателя**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № задания | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Правильный ответ | 3 | 2 | 1 | 1 | 2 | 2 | 4 | 1 | 5 | 4 | 4 | 5 | 3 | 2 | 1 |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № задания | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| Правильный ответ | 3 | 1 | 2 | 1 | 4 | 4 | 4 | 2 | 3 | 1 |

**ЗАДАНИЕ ДЛЯ СТУДЕНТОВ № 9**

**КОМПЛЕКТ ЗАДАНИЙ ДЛЯ ОПРОСА**

1. Дайте определение термину «система защиты от копирования (система защита авторского права)».
2. Что понимается под нелегальным распространением программного продукта?
3. Что понимается под нелегальным использованием программного продукта?
4. Что понимается под нелегальным изменении программного продукта?
5. Назовите три основные ситуации, связанные с распространением программного обеспечения.
6. Охарактеризуйте следующую ситуацию, связанную с распространением программного обеспечения: распространение (рассылка или передача) программного продукта на магнитных носителях (дискетках) и установка самим пользователем.
7. Охарактеризуйте следующую ситуацию, связанную с распространением программного обеспечения: установка программного продукта представителем фирмы.
8. Охарактеризуйте следующую ситуацию, связанную с распространением программного обеспечения: использование программного продукта лицами, не заинтересованными в его дальнейшем распространении.
9. Дайте определение надежности системы защиты от копирования.
10. Чем нужно руководствоваться при создании и использовании средств защиты?
11. При выполнении каких требований существенно повышается надежность системы защиты от копирования?
12. Из каких компонентов состоит система защиты от копирования?
13. Что подразумевается под копированием дискет?
14. Что означает обеспечить некопируемость информации с дискеты?
15. Дайте определение некопируемой метке.
16. Какие существуют способы формирования некопируемых меток?
17. Перечислите способы нанесения магнитной метки.
18. Опишите способы нанесения магнитной метки: вынос метки за пределы стандартного поля копирования.
19. Опишите способы нанесения магнитной метки: нестандартная разметка дорожки (дорожек) дискеты.
20. Опишите способы нанесения магнитной метки: привязка к временным параметрам чтения/записи.
21. Опишите способы нанесения магнитной метки: комбинированные методы.
22. В чем состоит идея метода простановки физической метки?
23. Приведите алгоритм работы с лазерной меткой.
24. Назовите основной метод создания некопируемой метки на жестких магнитных дисках (ЖМД).
25. Какие требования должны выполняться при форматировании дорожек за пределами рабочего поля?
26. В чем состоит идея метода создания некопируемой метки на жестких магнитных дисках (ЖМД): применение операций длинного чтения и длинной записи?

**ЗАДАНИЕ ДЛЯ СТУДЕНТОВ № 10**

**КОМПЛЕКТ ЗАДАНИЙ ДЛЯ ОПРОСА**

1. Перечислите основные методы защиты от программных средств отладки и дисассемблирования.
2. В чем заключался метод защита от средств отладки и дисассемблирования:построение антитрассировочных средств на основе учета аппаратных особенностей микропроцессоров Intel семейства 80х86?
3. В чем заключался метод защита от средств отладки и дисассемблирования: противодействие работе программных отладчиков, использующих прерывания ONE STEP и BREAK POINT?
4. В чем заключался метод защита от средств отладки и дисассемблирования: динамическое преобразования кода программы в процессе ее выполнения?
5. Какие основные цели преследует преобразование кода программы во время ее выполнения?
6. Перечислите основные способы организации преобразования кода программы. Дайте характеристику данным способам.
7. В чем заключался метод защита от средств отладки и дисассемблирования: построение антиотладочных средств на основе противодействия процессу общения с пользователем?
8. В чем заключался метод защита от средств отладки и дисассемблирования: учет временных зависимостей работы программы, создание псевдопараллельных процессов на базе таймерного прерывания?
9. В чем заключается метод трассировки программы по заданному прерыванию?
10. Дайте определение термину «трассировка прерывания».
11. Сколько прерываний можно использовать при работе с гибкими дисками?
12. Какие приемы используются для защиты от трассировки по int 13h и int 40h прерываниям?
13. Какие используются методы защиты о трассировки по прерыванию при работе с жесткими дисками?
14. Опишите метод защиты от трассировки прерывания DOS.
15. Опишите возможные ситуации при защите нерезидентных программ.
16. Дайте характеристику следующей ситуации при защите нерезидентных программ: нападение на дополнительный модуль к защищаемой программе.
17. Дайте характеристику следующей ситуации при защите нерезидентных программ: нападение на защищенную программу после отработки антиотладочных средств и передача на нее управления.
18. Какие возможны виды нападений при защите резидентных программ.

**ЗАДАНИЕ ДЛЯ СТУДЕНТОВ № 11**

**КОМПЛЕКТ ЗАДАНИЙ ДЛЯ ОПРОСА**

1. Дайте определение криптологии.
2. Какие три основных периода криптологии вы знаете?
3. Объясните понятие «криптологический алгоритм».
4. Что такое криптография?
5. Приведите основную классификацию криптографических методов.
6. Какова суть преобразований перестановки и замены?
7. Что собой представляет шифрование и дешифрование?
8. Дайте определение аналитическому преобразованию, гаммированию и комбинированному шифрованию.
9. Что такое системы с открытыми ключами?
10. Приведите структурную схему процесса шифрования с открытым ключом.
11. Дайте определение стойкости криптосистемы.
12. Приведите основные программно-аппаратные реализации шифров.
13. В чем заключается суть DES-алгоритмов? Каковы его особенности?
14. В каких режимах может работать DES-алгоритмов?
15. Дайте определение отечественного алгоритма криптографического преобразования данных (ГОСТ 28147-89) и его отличительных особенностей.
16. Какие режимы имеет отечественный алгоритм криптографического преобразования данных (ГОСТ 28147-89)?
17. Чем отличаются поточные симметричные криптографические системы?
18. Какими характеристиками оценивается стойкость криптографических систем?
19. Что такое ключевая система шифра и как организуется протоколирование связи и распределение ключей?
20. В чем заключается суть электронной цифровой подписи?
21. Как проверяется целостность сообщений?

**ЗАДАНИЕ ДЛЯ СТУДЕНТОВ № 12**

**КОМПЛЕКТ ЗАДАНИЙ ДЛЯ ОПРОСА**

1. Каким образом вирус заражает компьютер?
2. Каким образом действуют компьютерные вирусы?
3. Какие вы знаете источники заражения компьютерным вирусом?
4. По каким признакам можно обнаружить факт заражения компьютерным вирусом?
5. Какие вы знаете типы вирусов? Какие деструктивные действия они осуществляют?
6. Какие действия предпринимают для предотвращения заражения компьютерным вирусом?
7. На какие основные классы можно разделить компьютерные вирусы?
8. Какие вредоносные программные закладки кроме вирусов вам известны?
9. Что такое компьютерный вирус?
10. Что такое стелс-вирус?
11. Что такое boot-вирус?
12. Что такое макровирусы?
13. Какие методы борьбы с компьютерными вирусами вы знаете?
14. Какие средства борьбы с компьютерными вирусами вы знаете?
15. Какие технологии борьбы с компьютерными вирусами вы знаете?
16. Приведите классификацию компьютерных вирусов по среде обитания.
17. Дайте характеристику файловым вирусам.
18. Дайте характеристику загрузочным вирусам.
19. Дайте характеристику сетевым вирусам.
20. Какие стадии жизненного цикла выделяются у компьютерных вирусов?
21. Какие этапы включаются в стадию исполнения компьютерных вирусов?
22. Что такое полиморфные вирусы?
23. Что такое резидентные вирусы?
24. Каковы особенности заражения файловыми вирусами?
25. Каковы особенности заражения загрузочными вирусами?
26. Каковы особенности заражения макровирусами?
27. Могут ли вирусы помимо самокопирования выполнять деструктивные функции?
28. Приведите классификацию вирусов по деструктивным возможностям.
29. Что такое троянские программы?
30. Объясните понятие «логическая бомба».
31. Каковы основные каналы распространения вирусов и вредоносных программ?

**ЗАДАНИЕ ДЛЯ СТУДЕНТОВ № 13**

**КОМПЛЕКТ ЗАДАНИЙ ДЛЯ ОПРОСА**

1. Что такое антивирус? Какие типы антивирусов вы знаете?
2. Какие методы обнаружения компьютерных вирусов вы знаете?
3. Что такое эвристический анализатор? Какие функции он выполняет?
4. Приведите примеры антивирусных программ. Коротко охарактеризуйте их.
5. Какие образом производится лечение зараженных дисков?
6. Что такое программа — полиграф?
7. Что такое программа — детектор?
8. Приведите внешние признаки проявления деятельности вируса.
9. Дайте характеристику методу обнаружения вирусов «метод сравнения с этанолом».
10. Дайте характеристику методу обнаружения вирусов «антивирусный мониторинг».
11. Дайте характеристику методу обнаружения вирусов «метод обнаружения изменений».
12. Дайте характеристику методу обнаружения вирусов «встраивание антивирусов в BIOS компьютера».
13. Что такое программа — фаги (сканеры)?
14. Что такое программа — ревизоры (CRC – сканеры)?
15. Что такое программа — блокировщики?
16. Что такое программа — иммунизаторы?
17. Каковы критерии качества антивирусной программы?
18. Относится ли Doctor Wed к программам-фагам (сканерам)?
19. Какие профилактические действия необходимо совершать для уменьшения вероятности заражения вирусом?
20. Перечислите наиболее распространенные антивирусные программные комплексы.

**ЗАДАНИЕ ДЛЯ СТУДЕНТОВ № 14**

**КОМПЛЕКТ ЗАДАНИЙ ДЛЯ ОПРОСА**

Раскройте содержание основных принципов доктрины ИБ.

1. Какие основные направления обеспечения ИБ в мировой практике вы знаете?
2. Сформулируйте основные задачи обеспечения ИБ РФ.
3. Приведите основные функции государственной системы обеспечения ИБ РФ.
4. Назовите задачи обеспечения безопасности функционирования информации в КС.
5. Каковы основные отечественные и зарубежные стандарты в области ИБ?
6. Какая система называется безопасной, а какая — надежной?
7. Что такое политика безопасности?
8. Каковы основные предметные направления защиты процессов переработки информации?
9. Что такое государственная тайна?
10. Дайте определение коммерческий тайны?
11. Что такое служебная тайна?
12. Что включает в себя понятие «профессиональная тайна»?
13. Что такое персональные данные?
14. Что такое источники права на доступ к информации?
15. Каковы уровни доступа к информации с точки зрения законодательства РФ?
16. Что такое информация ограниченного распространения?
17. Каковы виды доступа к информации?
18. В чем заключается ответственность за нарушение законодательства РФ в информационной сфере?
19. Перечислите основные недостатки запретов процессов переработки информации в АСОД и назовите пути их преодоления.

**ЗАДАНИЕ ДЛЯ СТУДЕНТОВ № 15**

**КОМПЛЕКТ ЗАДАНИЙ ДЛЯ АУДИТОРНОЙ САМОСТОЯТЕЛЬНОЙ РАБОТЫ**

Перечень контрольных вопросов:

1. Что такое аудит?
2. Что понимается под протоколированием?
3. Какие задачи решает реализация протоколирования и аудита?
4. Какую информацию рекомендуется записывать при протоколировании события?
5. Что такое выборочное протоколирование?
6. В чем заключается задача активного аудита?
7. Что понимается под сигнатурой атаки?
8. Каковы достоинства и недостатки сигнатурного метода атаки?
9. Каковы достоинства и недостатки статического подхода атаки?
10. Какие компоненты входят в состав средств активного аудита?

**ЗАДАНИЕ ДЛЯ СТУДЕНТОВ № 16**

**КОМПЛЕКТ ЗАДАНИЙ ДЛЯ АУДИТОРНОЙ САМОСТОЯТЕЛЬНОЙ РАБОТЫ**

**Шифрование, контроль целостности.**

Перечень контрольных вопросов:

1. Что такое шифрование?
2. Какие методы шифрования различают?
3. В чем заключается метод симметричного шифрования?
4. В чем заключается метод асимметричного шифрования?
5. Сколько ключей используется при асимметричном шифровании? Как они используются?
6. Какие понятия лежат в основе контроля целостности?
7. Что понимается пол хэш-функцией?
8. Для чего используются удостоверяющие центры?
9. Какую структуру имеет цифровой сертификат?
10. Для чего применяется цифровой сертификат?
11. Какими свойствами обладает цифровой сертификат?

**ЗАДАНИЕ ДЛЯ СТУДЕНТОВ № 17**

**КОМПЛЕКТ ЗАДАНИЙ ДЛЯ АУДИТОРНОЙ САМОСТОЯТЕЛЬНОЙ РАБОТЫ**

Перечень контрольных вопросов:

1. В чем заключается главная задача стандартов информационной безопасности?
2. Какова роль потребителей при создании стандартов информационной безопасности?
3. Какова роль производителей при создании стандартов информационной безопасности?
4. Какова роль экспертов по квалификации и специалистов по сертификации при создании стандартов информационной безопасности?
5. Какой документ стал первым из стандартов в рассмотрении информационной безопасности?
6. Какие уровни безопасности отражены в Оранжевой книге?
7. Что предполагается седлать для обеспечения информационной безопасности компании в соответствии с международными и национальными стандартами?
8. Какие вопросы в обеспечении информационной безопасности рассматриваются в международном стандарте ISO/IEC 17799:2002 (BS 7799:2000) “Управление информационной безопасностью — Информационные технологии”?
9. Какие вопросы в обеспечении информационной безопасности рассматриваются в германском стандарте BSI “Руководство по защите информационных технологий для базового уровня защищенности”?
10. Какие вопросы в обеспечении информационной безопасности рассматриваются в международном стандарте ISO 15408 “Общие критерии безопасности информационных технологий”?
11. Какие существуют стандарты для беспроводных сетей?
12. Каковы особенности каждого из стандартов для беспроводных сетей: IEEE 802.11, IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11i?
13. Какие существуют стандарты информационной безопасности в Интернете?
14. В чем особенность каждого протокола безопасной передачи данных в интернете: SSL, SET, IPSec?
15. Какие существуют отечественные стандарты безопасности информационных технологий?
16. Какие вопросы в обеспечении безопасности рассматриваются в ГОСТ Р ИСО/МЭК 15408-2002 «Критерии оценки безопасности информационных технологий»?

**ЗАДАНИЕ ДЛЯ СТУДЕНТОВ № 18**

**КОМПЛЕКТ ЗАДАНИЙ ДЛЯ защиты реферата**

Темы рефератов:

1. Понятие информационной безопасности и защиты информации.
2. Аспекты информационной безопасности. Системы защиты информации.
3. Угрозы. Классификация.
4. Вредоносное программное обеспечение. Виды. Примеры.
5. Программные закладки.
6. Троянские программы.
7. Вирусы. Определение. Классификация.
8. Основные виды вирусов и схемы их функционирования.
9. Антивирусы.
10. Управление рисками.
11. Организационный уровень защиты информации.
12. Процедурный уровень защиты информации.
13. Инженерно-техническая защита.
14. Защита от утечки по техническим каналам.
15. Защита от утечки по акустическим каналам.
16. Защита от утечки по материально-вещественным каналам.
17. Защита от утечки по визуально-оптическим каналам.
18. Защита от утечки по электромагнитным каналам.
19. Системы контроля вскрытия аппаратуры.
20. Защита информации на носителях. Способы уничтожения информации.
21. Сетевые атаки. Классификация.
22. Технологии защиты от сетевых атак.
23. Межсетевые экраны.
24. Способы контроля и разграничения доступа к информации.
25. Контроль целостности ПО и информации
26. Защита операционных систем.
27. Методы идентификации и аутентификации. ЭСИА.
28. Криптографические средства защиты. Требования к криптографическому закрытию информации.
29. Криптографические протоколы аутентификации.
30. Криптографические протоколы голосования.
31. Стандарт шифрования данных DES.
32. Отечественный стандарт шифрования данных ГОСТ 28147-89.
33. Криптографические системы с открытым ключом.
34. Протоколы разделения секрета.
35. Законодательный *уровень* информационной безопасности.
36. Стандарты в области информационной безопасности. Основные определения.
37. «Оранжевая книга».
38. Европейские критерии безопасности.
39. Руководящие документы Гостехкомиссии России
40. Федеральные критерии безопасности
41. Единые критерии безопасности.

**ЗАДАНИЕ ДЛЯ СТУДЕНТОВ № 19**

**Комплект заданий для тестирования**

**(рубежный контроль)**

1**.** Что из перечисленного не относится к числу основных аспектов информационной безопасности?

* 1. Доступность
  2. Целостность
  3. Конфиденциальность
  4. **Правдивое отношение действительности**

2. Что такое защита информации?

* 1. Защита от несанкционированного доступа к информации
  2. Выпуск бронированных коробочек для дискет
  3. **Комплекс мероприятий, направленных на обеспечение информационной безопасности**

3.Как трактуется понятие ИБ в Доктрине ИБ РФ?

* 1. **Состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности , общества и государства.**
  2. Защита душевного здоровья телезрителя.
  3. Выпуск бронированных коробочек для дискет.

4. Что из перечисленного не относится к числу основных составляющих информационной безопасности?

* 1. Доступность
  2. **Масштабируемость**
  3. Целостность
  4. Конфиденциальность

5. Что из перечисленного относится к числу основных составляющих информационной безопасности?

* 1. Защита от копирования
  2. **Доступность**
  3. Масштабируемость
  4. Правдивое отражение действительности

6. Что из перечисленного относится к числу основных составляющих информационной безопасности?

* 1. Защита от копирования
  2. Масштабируемость
  3. **Целостность**
  4. Правдивое отражение действительности

7. Что из перечисленного относится к числу основных составляющих информационной безопасности?

* 1. Защита от копирования
  2. Правдивое отражение действительности
  3. Масштабируемость
  4. **Конфиденциальность**

8. \*\*\* - это возможность за приемлемое время получить требуемую информационную услугу?

* 1. **Доступность**
  2. Конфиденциальность
  3. Целостность

9. \*\*\* - это актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения?

* 1. Доступность
  2. Конфиденциальность
  3. **Целостность**

10. \*\*\* - это защита от несанкционированного доступа к информации?

* 1. Доступность
  2. **Конфиденциальность**
  3. Целостность

11. На какие составляющие делится целостность?

* 1. **Динамическая**
  2. Эстетическая
  3. **Статическая**

12. Какую сумму потеряла студентка Мичиганского университета из-за того, что ее соседка по комнате воспользовалась их общим системным входом и отправила от имени своей жертвы электронное письмо с отказом от стипендии?

* 1. 100 тысяч долларов
  2. 45 тысяч долларов
  3. **18 тысяч долларов**

13. Средний ущерб от компьютерного преступления в США составляет примерно:

* 1. **Сотни тысяч долларов**
  2. Десятки долларов
  3. Копейки

14. Компьютерная преступность в мире:

* 1. Остается на одном уровне
  2. Снижается
  3. **Растет**

15. Какая сумма была похищена из Центрального банка России в 1995 году?

* 1. 100 миллионов рублей
  2. **250 миллиардов рублей**
  3. Миллион рублей

16. Объектно-ориентированный подход содержит … ?

* 1. Семантическую декомпозицию
  2. **Объектную декомпозицию**
  3. Алгоритмическую декомпозицию

17. \*\*\* - это абстракция множества сущностей реального мира, объединенных общностью структуры и поведения.

* 1. **Класс**
  2. Объект
  3. Символ

18. \*\*\* - это элемент класса, то есть абстракция определенной сущности.

* 1. Класс
  2. **Объект**
  3. Символ

19. Понятие "..." может трактоваться как способность объекта принадлежать более чем одному классу.

* 1. Наследование
  2. Инкапсуляция
  3. **Полиморфизм**

20. \*\*\* - означает построение новых классов на основе существующих с возможностью добавления или переопределения данных и методов.

* 1. **Наследование**
  2. Инкапсуляция
  3. Полиморфизм

21. Любой разумный метод борьбы со сложностью опирается на принцип:

* 1. Не следует умножать сущности сверх необходимости
  2. Отрицания отрицания
  3. **Разделяй и властвуй**

22. В число основных понятий объектного подхода не входят?

* 1. Инкапсуляция
  2. Наследование
  3. **Полиморфизм**

23. Структурный подход опирается на:

* 1. Семантическую декомпозицию
  2. **Алгоритмическую декомпозицию**
  3. Декомпозицию структур данных

24. Контейнеры в компонентах объектных средах предоставляют:

* 1. **Общий контекст взаимодействия с другими компонентами и окружением**
  2. Средства для сохранения компонентов
  3. Механизмы транспортировки компонентов

25. Потенциальная возможность определенным образом нарушить информационную безопасность - это …?

* 1. Бомба
  2. **Угроза**
  3. Атака

26. Попытка реализации угрозы называется …?

* 1. Бомба
  2. Угроза
  3. **Атака**

27. По каким критериям можно классифицировать угрозы?

* 1. **По аспекту ИБ**
  2. По внутренним отказам ИС
  3. **По способу осуществления**
  4. **По компонентам ИС, на которые угрозы нацелены**

28. Окно опасности - это …?

* 1. Плохо закрепленная деталь строительной конструкции.
  2. **Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется.**
  3. Часть пространства.

29. По отношению к поддерживающей инфраструктуре рассматриваются следующие угрозы:

* 1. Нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования
  2. Разрушение или повреждение помещений
  3. Невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности
  4. **Все ответы верны**

30. Melissa – это …?

* 1. Бомба
  2. **Вирус**
  3. Червь

31. Код, обладающий способностью к распространению путем внедрения в другие программы называется …?

* 1. Червь
  2. Бомба
  3. **Вирус**

32. Код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение называется …?

* 1. **Червь**
  2. Бомба
  3. Вирус

33. Что относится к граням вредоносного программного обеспечения?

* 1. **Вредоносная функция**
  2. **Способ распространения**
  3. Агрессивного потребления ресурсов
  4. **Внешнее представление**

34. Самыми опасными источниками внутренних угроз являются:

* 1. Некомпетентные руководители
  2. **Обиженные сотрудники**
  3. Любопытные администраторы

35. Melissa – это …?

* 1. **Макровирус для файлов MS-Word**
  2. Макровирус для файлов PDF
  3. Макровирус для файлов Postscript

36. Основными источниками внутренних отказов являются:

* 1. **Отступление (случайное или умышленное) от установленных правил эксплуатации**
  2. Разрушение или повреждение помещений
  3. **Отказы программного и аппаратного обеспечения**
  4. **Разрушение данных**

37. Вредоносный код, который выглядит как функционально полезная программа, называется … ?

* 1. Червь
  2. Вирус
  3. **Троянская программа**

38. Основным законом Российской Федерации является …?

* 1. Семейное право
  2. Пиратский кодекс
  3. **Конституция**

39. Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон ... ?

* 1. **"Об информации, информационных технологиях и о защите информации"**
  2. "Об информации"
  3. "Преступления в сфере компьютерной информации"

40. Что обязан предоставить импортер при ввозе информационного продукта, и информационных услуг?

* 1. **Сертификат**
  2. Визу
  3. Паспорт
  4. Все ответы верны

41. Что такое электронная цифровая подпись?

* 1. Это документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.
  2. Это уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, …
  3. **Это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки…**

42. Физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи это ...?

* 1. Владелец сертификата ключа подписи
  2. **Пользователь сертификата ключа подписи**
  3. Пользователь сертификата ключа расписки

43. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя это … ?

* 1. Запретная информация
  2. **Конфиденциальность информации**
  3. Секретная информация

44. Согласно Закону "Об информации, информационных технологиях и о защите информации", документированная информация - это …?

* 1. Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.
  2. Процессы сбора, обработки, накопления, хранения, поиска и распространения информации.
  3. **Зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.**

45. Согласно Закону "О лицензировании отдельных видов деятельности", лицензия - это … ?

* 1. Вид деятельности, на осуществление которого на территории Российской Федерации требуется получение лицензии в соответствии с настоящим Федеральным законом.
  2. **Специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.**
  3. Юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности.

46. Согласно Закону "О лицензировании отдельных видов деятельности", лицензиат - это …?

* 1. Вид деятельности, на осуществление которого на территории Российской Федерации требуется получение лицензии в соответствии с настоящим Федеральным законом.
  2. Специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.
  3. **Юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности.**

47. Уголовный кодекс РФ не предусматривает наказания за:

* 1. Увлечение компьютерными играми в рабочее время
  2. **Неправомерный доступ к компьютерной информации**
  3. **Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети**

48. При каких условиях электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе?

* 1. Сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания
  2. Подтверждена подлинность электронной цифровой подписи в электронном документе
  3. Электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи
  4. **Все ответы верны**

49. Когда была принята Конституция РФ?

* 1. **12 декабря 1993**
  2. 15 марта 1991
  3. 21 сентября 1998

50. В каком году была впервые опубликована "Оранжевая книга"?

* 1. **1983 году**
  2. 1984 году
  3. 1985 году

51. Какими качествами НЕ обладает монитор обращений?

* 1. **Изолированность**
  2. Безопасность
  3. Верифицируемость

52. Ядро безопасности – это … ?

* 1. **Основа, на которой строятся все защитные механизмы.**
  2. Способ убедиться в том, что архитектура системы и ее реализация действительно реализуют избранную политику безопасности
  3. Код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение

53. Операционная гарантированность - это … ?

* 1. Весь жизненный цикл ИС, то есть периоды проектирования, реализации, тестирования, продажи и сопровождения.
  2. **Способ убедиться в том, что архитектура системы и ее реализация действительно реализуют избранную политику безопасности**

54. Какие классы безопасности определяются в «Оранжевой книге»?

* 1. С1, С2, С3, В1, В2, А1
  2. С1, С2, А1, В1, В2
  3. **A1, C1, C2, B1, B2, B3**

55. Какие требования включает в себя показательный класс функциональных требований - "Использование ресурсов", содержащий требования доступности?

* 1. **Распределение ресурсов**
  2. Анонимность
  3. **Отказоустойчивость**

56. Сколько всего оценочных уровней доверия?

* 1. Пять
  2. Шесть
  3. **Семь**

57. Дайте определение «системы» относительно Европейских критерий?

* 1. Аппаратно-программный "пакет", который можно купить и по своему усмотрению встроить в ту или иную систему.
  2. **Конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении.**

58. Какой оценочный уровень доверия предусматривает формальную верификацию проекта объекта оценки. Он применим к ситуациям чрезвычайно высокого риска?

* 1. Оценочный уровень доверия 6
  2. Оценочный уровень доверия 5
  3. **Оценочный уровень доверия 7**

59. Главная цель мер административного уровня:

* 1. **Сформировать программу работ в области ИБ и обеспечить ее выполнение.**
  2. Противостоять административным правонарушениям.
  3. Обезопасить администрацию организации.
  4. Администрировать цели организации.

60. Политика безопасности строится на основе …?

* 1. На предпочтениях организации
  2. **Анализа рисков**
  3. Политической безопасности
  4. На сервисах

61. После того, как риски проанализированы, и стратегия защиты определена, составляется … ?

* 1. Телевизионная программа
  2. Смета
  3. **Программа обеспечения информационной безопасности**
  4. Отчёт

62. Под политикой безопасности понимается:

* 1. Соблюдение законов
  2. Обеспечение политической неприкосновенности
  3. Безопасность оборудования и ПО
  4. **Совокупность документированных решений**

63. К верхнему уровню ИБ можно отнести решения, затрагивающие … ?

* 1. **Организацию в целом**
  2. Персонал
  3. Оборудование и ПО
  4. Отдельный аспекты ИБ

64. Политика безопасности нижнего уровня относится … ?

* 1. К общим аспектам
  2. К организации в целом
  3. **К конкретным информационным сервисам**
  4. Правильного ответа нет

65. В жизненном цикле информационного сервиса НЕТ такого этапа, как:

* 1. Инициация
  2. Закупка
  3. Установка
  4. **Разработка**

66. Для борьбы с эффектом медленных изменений приходится прибегать … ?

* 1. **К периодическим проверкам сервиса**
  2. К постоянным модификациям сервиса
  3. К обновлению правил безопасности
  4. К уничтожению старой информации

67. В число этапов жизненного цикла информационного сервиса входят:

* 1. **Закупка**
  2. Продажа
  3. **Выведение из эксплуатации**
  4. **Установка**

68. Какой вид деятельности включает в себя управление рисками?

* 1. Оценка рисков
  2. Нейтрализация рисков
  3. **Ликвидация рисков**

69. Какие действия возможны к выявленным рискам?

* 1. **Ликвидация риска**
  2. **Уменьшение риска**
  3. Анализ риска
  4. Переадресация риска

70. Что необходимо сделать с рисками для получения наибольшего эффекта?

* 1. **Интегрировать в жизненный цикл ИС**
  2. Определить этапы жизненного цикла
  3. Инициировать известные риски

71. На каком этапе жизненного цикла управление рисками должно сопровождать все существенные изменения в системе?

* 1. Установки
  2. **Эксплуатации**
  3. Разработки

72. Первый шаг в оценке рисков – это … ?

* 1. Создание карты информационной системы
  2. **Выбор анализируемых объектов и уровня детализации**
  3. Детализация рисков

73. Типичная оптимизационная задача – это … ?

* 1. **Управление рисками**
  2. Миссия организации
  3. Идентификация активов

74. Первый шаг в анализе угроз – это … ?

* 1. **Их идентификация**
  2. Их детализация
  3. Их локализация

75. При оценке вероятности осуществления угрозы допустимо использовать … ?

* 1. Десятибалльную шкалу
  2. Пятибалльную шкалу
  3. **Трехбалльную шкалу**

76. В число классов мер процедурного уровня входят:

* 1. Логическая защита
  2. **Физическая защита**
  3. **Планирование восстановительных работ**

77. В число принципов управления персоналом входят:

* 1. "Разделяй и властвуй"
  2. **Разделение обязанностей**
  3. Инкапсуляция наследования

78. В число этапов процесса планирования восстановительных работ входят:

* 1. **Выявление критически важных функций организации**
  2. **Определение перечня возможных аварий**
  3. Проведение тестовых аварий

79. В число этапов процесса планирования восстановительных работ входят:

* 1. Идентификации персонала
  2. Проверка персонала
  3. **Идентификация ресурсов**

80. В число принципов физической защиты входят:

* 1. Беспощадный отпор
  2. **Непрерывность защиты в пространстве и времени**
  3. Минимизация защитных средств

81. В число основных принципов архитектурной безопасности входят:

* 1. Применение наиболее передовых технических решений
  2. **Применение простых апробированных решений**
  3. Сочетание простых и сложных защитных средств

82. Что понимается под протоколированием?

* 1. **Сбор и накопление информации о событиях, происходящих в информационной системе.**
  2. Анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день).
  3. Совокупность условий, при выполнении которых атака считается имеющей место, что вызывает заранее определенную реакцию.

83. Что понимается под аудитом?

* 1. Сбор и накопление информации о событиях, происходящих в информационной системе.
  2. **Анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день).**
  3. Совокупность условий, при выполнении которых атака считается имеющей место, что вызывает заранее определенную реакцию.

84. Что понимается под сигнатурой атаки?

* 1. Сбор и накопление информации о событиях, происходящих в информационной системе.
  2. Анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день).
  3. **Совокупность условий, при выполнении которых атака считается имеющей место, что вызывает заранее определенную реакцию.**

85. Какие задачи решает реализация протоколирования и аудита?

* 1. Обеспечение подотчетности пользователей и администраторов
  2. Предоставление информации для выявления и анализа проблем
  3. Обнаружение попыток нарушений информационной безопасности
  4. **Все ответы верны**

86. Какую информацию рекомендуется записывать при протоколировании события?

* 1. Дата и время события
  2. Уникальный идентификатор пользователя – инициатора действия
  3. Тип события
  4. **Все ответы верны**

87. Сигнатурный метод выявления атак хорош тем, что он:

* 1. **Поднимает мало ложных тревог**
  2. Способен обнаруживать неизвестные атаки
  3. **Имеет высокую производительность**

88. Цифровой сертификат содержит:

* 1. **Открытый ключ пользователя**
  2. Секретный ключ пользователя
  3. **Имя пользователя**

89. Статический метод выявления атак хорош тем, что он:

* 1. Поднимает мало ложных тревог
  2. **Способен обнаруживать неизвестные атаки**
  3. **Имеет универсальность и обоснованность решений**

90. Идентификация и аутентификация - это …?

* 1. **Первая линия обороны, "проходная" информационного пространства организации**
  2. Программный продукт, разработанный в середине 1980-х годов
  3. Совокупность автоматизированных методов поведения

91. Перечислите виды аутентификации:

* 1. Пользовательская
  2. **Односторонняя**
  3. Многосторонняя
  4. **Двусторонняя**

92. Субъект может подтвердить свою подлинность, предъявив одну из следующих сущностей:

* 1. Нечто, что засекречено
  2. **Нечто, что он знает**
  3. **Нечто, чем он владеет**
  4. **Нечто, что есть часть его самого**

93. Какая компания является генератором одноразовых паролей системы S/KEY?

* 1. Intuit
  2. Биометрия
  3. Kekberos
  4. **Bellcore**

94. Что такое Kerberos?

* 1. **Программный продукт, разработанный в середине 1980-х годов в Массачусетском технологическом институте и претерпевший с тех пор ряд принципиальных изменений**
  2. Нечто, что есть часть его самого
  3. Средство, устойчивое к пассивному прослушиванию сети

95. Что такое логическое управление доступом?

* 1. Доверенная третья сторона
  2. **Основной механизм многопользовательских систем**

96. Каково основное достоинство произвольного управления?

* 1. Разделенность
  2. **Гибкость**
  3. Доступность
  4. Мобильность

97. Каковы недостатки произвольного управления?

* 1. **Рассредоточенность управления**
  2. Ввод пароля можно подсмотреть
  3. Права доступа существуют отдельно от данных
  4. Распространение пароля коллегам

98. Перечислите три категории функций, необходимых для администрирования РУД:

* 1. Ликвидирующие функции
  2. **Информационные функции**
  3. **Вспомогательные функции**
  4. **Административные функции**

99. В чем различие между динамическим и статическим разделением обязанностей?

* 1. Рассматриваются задачи
  2. Рассматриваются объекты
  3. **Рассматриваются роли, одновременно активные для данного пользователя**

100. Виды разделения обязанностей:

* 1. Серверное
  2. **Динамическое**
  3. Клиентское
  4. **Статическое**

**Пакет преподавателя**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № задания | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| Правильный ответ | 4 | 3 | 1 | 2 | 2 | 3 | 4 | 1 | 3 | 2 | 1,3 | 3 | 1 | 3 | 2 | 2 | 1 | 2 | 3 | 1 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № задания | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| Правильный ответ | 3 | 3 | 2 | 1 | 2 | 3 | 1,3,4 | 2 | 4 | 2 | 3 | 1 | 1,2,4 | 2 | 1 | 1,3,4 | 3 | 3 | 1 | 1 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № задания | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 |
| Правильный ответ | 3 | 2 | 2 | 3 | 2 | 3 | 2,3 | 4 | 1 | 1 | 1 | 1 | 2 | 3 | 1,3 | 3 | 2 | 3 | 1 | 2 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № задания | 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 |
| Правильный ответ | 3 | 41 | 3 | 4 | 4 | 1 | 1,3,4 | 3 | 1,2,4 | 1 | 2 | 2 | 1 | 1 | 3 | 2,3 | 2 | 1,2 | 3 | 2 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № задания | 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 | 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 |
| Правильный ответ | 2 | 1 | 2 | 3 | 4 | 4 | 1,3 | 1,3 | 2,3 | 1 | 2,4 | 2,3,4 | 4 | 1 | 2 | 2 | 1 | 2,3,4 | 3 | 2,4 |

**ЗАДАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ № 20**

**ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕРКИ**

**ТЕОРЕТИЧЕСКОГО МАТЕРИАЛА**

1. Понятие информационной безопасности и защиты информации.
2. Основные составляющие ИБ.
3. Важность и сложность проблемы ИБ.
4. Основные понятия объектно-ориентированного подхода ИБ.
5. Основные определения и критерии классификации угроз.
6. Наиболее распространенные угрозы доступности.
7. Вредоносное программное обеспечение.
8. Основные угрозы целостности.
9. Основные угрозы конфиденциальности.
10. Что такое законодательный уровень ИБ и почему он важен.
11. Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт. Основные понятия.
12. Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт. Механизмы безопасности.
13. Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт. Классы безопасности.
14. Административный уровень ИБ. Основные понятия.
15. Управление рисками. Основные понятия.
16. Подготовительные этапы управления рисками.
17. Основаны этапы управления рисками.
18. Основные классы мер процедурного уровня ИБ.
19. Основные понятия программно-технического уровня ИБ.
20. Идентификация и аутентификация.
21. Управление доступом.
22. Протоколирование и аудит.
23. Шифрование, контроль целостности.
24. Экранирование. Основные понятия
25. Экранирование. Классификация межсетевых экранов.
26. Основные понятия обеспечения высокой доступности.
27. Основные меры обеспечения высокой доступности.
28. Туннелирование и управление.
29. Компьютерный вирус: классификация, свойства.
30. История компьютерных вирусов по1998 год.
31. История компьютерных вирусов с 1999 по 2005 года.
32. Пути проникновения вирусов в компьютер.
33. Признаки заражения компьютера вирусом.
34. Способы заражения программ вирусами.
35. Резидентные вирусы. Характеристика. Особенности функционирования.
36. Опишите отличия вирусов-репликаторов и стелс-вирусов.
37. Опишите отличительные особенности вирусов мутантов и «троянских» программ.
38. Принципы функционирования загрузочного вируса.
39. Принципы функционирования файлового вируса.
40. Принципы функционирования загрузочно-файлового вируса.
41. Дайте характеристику полиморфного вируса. Опишите особенности его функционирования.
42. Методы защиты от вредоносных программ. Организационные методы
43. Методы защиты от вредоносных программ. Технические методы.
44. Опишите назначение антивирусных программ различных типов.
45. Программы-детекторы и программы-доктора или фаги.
46. Программы-ревизоры и программы фильтры.
47. Программы вакцины или иммунизаторы.
48. Опишите особенности использования антивирусных программ различных типов.
49. Современные антивирусные программы: DrWEB.
50. Современные антивирусные программы: NOD32.
51. Современные антивирусные программы: антивирус Касперского.
52. Основные меры по защите от вирусов.

**ЗАДАНИЕ ДЛЯ ОБУЧАЮЩИХСЯ № 21**

**ПЕРЕЧЕНЬ практических ЗАДАЧ**

Решить задачи по оценке стойкости парольных систем.

* 1. В таблице 1 найти для вашего билета значения характеристик P,V,T, а также группы символов, используемых при формировании пароля.
  2. Вычислить мощность алфавита паролей A, соответствующую Вашему варианту.
  3. Вычислить по формуле мощность пространства паролей S для заданных P,V,T.
  4. Зная мощность алфавита паролей A, вычислить минимальную длину пароля L, при котором выполняется условие.

Таблица 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер билета | *P* | *V* | *T* | *Используемые группы символов пароля* |
| 1 | 10-4 | 15 паролей/мин | 2 недели | 1. Цифры (0-9)  2. Латинские строчные буквы (a-z) |
| 2 | 10-5 | 3 паролей/мин | 10 дней | 1. Латинские прописные буквы (A-Z)  2. Русские строчные буквы (а-я) |
| 3 | 10-6 | 10 паролей/мин | 5 дней | 1. Русские прописные буквы (А-Я)  2. Специальные символы. (10 символов) |
| 4 | 10-7 | 11 паролей/мин | 6 дней | 1. Цифры (0-9)  2. Латинские прописные буквы (A-Z) |
| 5 | 10-4 | 100 паролей/день | 12 дней | 1. Русские прописные буквы (А-Я)  2. Латинские строчные буквы (a-z) |
| 6 | 10-5 | 10 паролей/день | 1 месяц | 1. Русские строчные буквы (а-я)  2. Специальные символы. (7 симолов) |
| 7 | 10-6 | 20 паролей/мин | 3 недели | 1. Цифры (0-9)  2. Русские строчные буквы (а-я) |
| 8 | 10-7 | 15 паролей/мин | 20 дней | 1. Латинские строчные буквы (a-z)  2. Латинские прописные буквы (A-Z) |
| 9 | 10-4 | 3 паролей/мин | 15 дней | 1. Русские прописные буквы (А-Я)  2. Русские строчные буквы (а-я) |
| 10 | 10-5 | 10 паролей/мин | 1 неделя | 1. Цифры (0-9)  2. Специальные символы. (15 символ) |
| 11 | 10-6 | 11 паролей/мин | 2 недели | 1. Цифры (0-9)  2. Русские прописные буквы (А-Я) |
| 12 | 10-7 | 100 паролей/день | 10 дней | 1. Латинские строчные буквы (a-z)  2. Русские прописные буквы (А-Я) |
| 13 | 10-4 | 10 паролей/день | 5 дней | 1. Цифры (0-9)  2. Латинские строчные буквы (a-z) |
| 14 | 10-5 | 20 паролей/мин | 6 дней | 1. Латинские прописные буквы (A-Z)  2. Русские строчные буквы (а-я) |
| 15 | 10-6 | 15 паролей/мин | 12 дней | 1. Русские прописные буквы (А-Я)  2. Специальные символы. (11 символов) |
| 16 | 10-7 | 3 паролей/мин | 1 месяц | 1. Цифры (0-9)  2. Латинские прописные буквы (A-Z) |
| 17 | 10-4 | 10 паролей/мин | 3 недели | 1. Русские прописные буквы (А-Я)  2. Латинские строчные буквы (a-z) |
| 18 | 10-5 | 11 паролей/мин | 20 дней | 1. Русские строчные буквы (а-я)  2. Специальные символы. (9 символов) |
| 19 | 10-6 | 100 паролей/день | 15 дней | 1. Цифры (0-9)  2. Русские строчные буквы (а-я) |
| 20 | 10-7 | 10 паролей/день | 1 неделя | 1. Латинские строчные буквы (a-z)  2. Латинские прописные буквы (A-Z) |
| 21 | 10-4 | 20 паролей/мин | 2 недели | 1. Русские прописные буквы (А-Я)  2. Русские строчные буквы (а-я) |
| 22 | 10-5 | 15 паролей/мин | 10 дней | 1. Цифры (0-9)  2. Специальные символы. (17 символов) |
| 23 | 10-6 | 3 паролей/мин | 5 дней | 1. Цифры (0-9)  2. Русские прописные буквы (А-Я) |
| 24 | 10-7 | 10 паролей/мин | 6 дней | 1. Латинские строчные буквы (a-z)  2. Русские прописные буквы (А-Я) |
| 25 | 10-4 | 11 паролей/мин | 12 дней | 1. Цифры (0-9)  2. Латинские строчные буквы (a-z) |
| 26 | 10-5 | 100 паролей/день | 1 месяц | 1. Латинские прописные буквы (A-Z)  2. Русские строчные буквы (а-я) |
| 27 | 10-6 | 10 паролей/день | 3 недели | 1. Русские прописные буквы (А-Я)  2. Специальные символы. (13 символов) |
| 28 | 10-7 | 20 паролей/мин | 20 дней | 1. Цифры (0-9)  2. Латинские прописные буквы (A-Z) |
| 29 | 10-4 | 15 паролей/мин | 15 дней | 1. Русские прописные буквы (А-Я)  2. Латинские строчные буквы (a-z) |
| 30 | 10-5 | 3 паролей/мин | 1 неделя | 1. Русские строчные буквы (а-я)  2. Специальные символы. (14 символов) |

**4. Критерии оценки**

**4.1. Практическая работа:**

«5» – все задания выполнены

«4» – наблюдались неточности при выполнении работы

«3» – наблюдались ошибки при выполнении работы

«2» – работа выполнена менее 50 %

**4.2. Тестовые задания:**

|  |  |  |
| --- | --- | --- |
| Процент результативности (правильных ответов) | Качественная оценка индивидуальных образовательных достижений | |
| балл (отметка) | вербальный аналог |
| 86 ÷ 100 | 5 | отлично |
| 70 ÷ 85 | 4 | хорошо |
| 55 ÷ 69 | 3 | удовлетворительно |
| менее 55 | 2 | не удовлетворительно |

**4.3 Теоретические вопросы**

|  |  |
| --- | --- |
| Оценка | Критерии |
| *«отлично»* | Дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний по дисциплине, доказательно раскрыты основные положения вопросов; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знания по предмету демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ изложен литературным языком с использованием современной технической терминологии. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа. |
| *«хорошо»* | Дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен литературным языком с использованием современной технической терминологии. Могут быть допущены некоторые неточности или незначительные ошибки, исправленные студентом с помощью преподавателя. |
| *«удовлетвори-тельно*» | Дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. В ответе отсутствуют выводы. Умение раскрыть значение обобщенных знаний не показано. Речевое оформление требует поправок, коррекции. |
| *«неудовлетворительно»* | 1) Ответ представляет собой разрозненные знания с существенными ошибками по вопросу. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь обсуждаемого вопроса по билету с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная, техническая терминология не используется. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента.  2) Ответ на вопрос полностью отсутствует.  3) Отказ от ответа. |

# 5. Информационное обеспечение обучения

**Основная литература:**

1. Гагарина, Л. Г. Введение в инфокоммуникационные технологии: учебное пособие / Л.Г. Гагарина, А.М. Баин и др.; под ред. д.т.н., проф. Л.Г.Гагариной. - М.: ФОРУМ: ИНФРА-М, 2013.
2. Гагарина, Л. Г. Технология разработки программного обеспечения: учебное пособие/ Л.Г.Гагарина, Е.В.Кокорева, Б.Д.Виснадул; под ред. проф. Л.Г.Гагариной. - М.: ФОРУМ: Инфра-М, 2013.
3. Гагарина, Л.Г. Введение в теорию алгоритмических языков и компиляторов: учебное пособие / Л.Г. Гагарина, Е.В. Кокорева. - М.: Форум, 2012.
4. Гуриков, С. Р. Введение в программирование на языке Visual C#: учебное пособие. - М.: Форум: ИНФРА-М, 2013.
5. Гуриков, С. Р. Информатика: учебник. - М.: Форум: ИНФРА-М, 2014.
6. Дьяконов, В.П. MATLAB. Полный самоучитель. - М.: ДМК Пресс, 2014.
7. Зиборов, В В. MS Visual C++ 2010 в среде .NET. Библиотека программиста.- СПб. : Питер, 2011.
8. Ковалевская, Е.В. Методы программирования: учебное пособие. - М.: Евразийский открытый институт, 2011.
9. Колдаев, В. Д. Структуры и алгоритмы обработки данных: учебное пособие. - М.: РИОР: ИНФРА-М, 2014.
10. Котельников, Е.В. Введение во внутреннее устройство Windows. - М.: Интернет- Университет Информационных Технологий (ИНТУИТ), 2013.
11. Культин, Н. С# в задачах и примерах. - СПб. : БХВ-Петербург, 2010.
12. Липаев, В.В. Тестирование компонентов и комплексов программ. - М.: СИНТЕГ, 2010.
13. Молчанов, А. Ю. Системное программное обеспечение: учебник для вузов. - СПб. : Питер, 2010.
14. Орлов, С. А. Технологии разработки программного обеспечения: учебник для вузов/ С.А.Орлов, Б.Я.Цилькер. - СПб. : Питер, 2012.
15. Павловская, Т. А. C#. Программирование на языке высокого уровня: учебник для вузов. - СПб.: Питер, 2012.
16. Партыка, Т. Л. Операционные системы, среды и оболочки: учебное пособие для студ. учрежд. СПО / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2013.
17. Подбельский, В.В. Язык Си# Базовый курс: учебное пособие. - М.: Финансы и статистика, 2011.
18. Смоленцев Н. К. MATLAB: Программирование на Visual C#, Borland C#, JBuilder, VBA: учебный курс. - М.: ДМК Пресс, 2015.
19. Собель, М. Linux. Администрирование и системное программирование. - СПб. : Питер, 2011.
20. Сузи, Р.А. Python. - СПб.: БХВ-Петербург, 2010.
21. Ташков, П. Веб-мастеринг на 100 %: HTML, CSS, JavaScript, PHP, CMS, AJAX, раскрутка.- СПб. : Питер, 2010.
22. Фленов, М. Библия C#. - СПб.: БХВ-Петербург, 2011.
23. Черников, Б.В. Оценка качества программного обеспечения: практикум: учебное пособие / Б.В. Черников, Б.Е. Поклонов; под ред. Б.В. Черникова. – М.: ФОРУМ: Инфра-М, 2012.

**Дополнительная литература:**

1. Алексеев, А.А. Основы параллельного программирования с использованием Visual Studio 2010. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2013.
2. Антамошкин О. А. Программная инженерия. Теория и практика: учебник. - Красноярск: Сиб. федер. ун-т, 2012.
3. Биллиг, В.A. Основы объектного программирования на С# (C# 3.0, Visual Studio 2008). - М.: БИНОМ. Лаборатория знаний, Интернет-Университет Информационных Технологий (ИНТУИТ), 2010.
4. Васильев, А. Java. Объектно-ориентированное программирование: учебное пособие. - СПб. : Питер, 2011.
5. Гоше, Х. Д.HTML5. Для профессионалов. - СПб. : Питер, 2012.
6. Дуванов, А.А. Web-конструирование. DHTML. - СПб.: БХВ-Петербург, 2010.
7. Дунаев, В. В. HTML, скрипты и стили. — 3-е изд., перераб. и доп. - СПб.: БХВ- Петербург, 2011.
8. Дунаев, В. В. Самоучитель JavaScript. - СПб. : Питер, 2010.
9. Котеров, Д. В. PHP 5/Д. В. Котеров, А. Ф. Костарев. - СПб.: БХВ-Петербург, 2010.
10. Лав, Р. Linux. Системное программирование. - СПб.: Питер, 2014.
11. Литвиненко Н. Технология программирования на С++. Win32 API-приложения. - СПб.: БХВ-Петербург, 2010.
12. Мартемьянов, Ю.Ф. Операционные системы. Концепции построения и обеспечения безопасности: учебное пособие/ Ю.Ф.Мартемьянов, Ал.В.Яковлев, Ан.В.Яковлев. - М.: Горячая линия - Телеком, 2011.
13. Орлов, С. Теория и практика языков программирования: учебник для вузов. - СПб. : Питер, 2013.

**Интернет-ресурсы:**

1. Мультипортал http://www.km.ru

2. Интернет-Университет Информационных технологий http://www.intuit.ru/

3. Образовательный портал http://claw.ru/

4. Свободная энциклопедия http://ru.wikipedia.org

5. «Мультимедиа для всех» статьи И.Р.Кузнецова

http://inftech.webservis.ru/it/multimedia

6. «Мультимедийные технологии» лекционный курс. Якушин А.В.

http://www.tula.net/tgpu/resouces/yakushin/html\_doc/doc08/doc08index.htm

7. Информационный сайт http://informika.ru

8. Сайт рефератов http://www.bankreferatov.ru

9. fepo - "Федеральный Интернет-экзамен в сфере профессионального

образования"

10. http://www.dreamspark.ru/ - Бесплатный для студентов, аспирантов,

школьников и преподавателей доступ к полным лицензионным версиям

инструментов Microsoft для разработки и дизайна.