ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Проректор по УМР
_____ И.А. Дибиров
«31» ____мая_____2023г

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ ОПЦ.13 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки 09.02.01 Компьютерные системы и комплексы
Квалификация: специалист по компьютерным системам
Срок обучения по ОП: 3г 10м (очное обучение)
Форма обучения: очная
Образовательный стандарт (ФГОС) N 362 от 25.05.2022

Махачкала 2023

Автор (ы)-составитель(и): Магомедов З.М.

Программа утверждена на заседании учебно-методического совета ДГПУ (протокол №3 от «28» апреля 2023г.

Председатель УМС д.ф.н, профессор
Дибиров И.А. _____ _____
подпись дата

СОДЕРЖАНИЕ

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств (ФОС) разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования (ФГОС СПО) по специальности *09.02.01 Компьютерные системы и комплексы*, утвержденного Приказом Минпросвещения России *от 25 мая 2022 г. № 362* и в соответствии с рабочей программой дисциплины *ОПЦ.13 Информационная безопасность и защита информации.*

ФОС включает контрольные материалы для проведения текущего контроля и промежуточной аттестации в форме зачета и дифференцированного зачета, которые позволяют оценить уровень достижения, запланированных результатов обучения по учебной дисциплине.

Текущий контроль успеваемости осуществляется с целью регулярного наблюдения за ходом поэтапного освоения обучающимися материалом учебной дисциплины, оптимизации управления образовательной деятельностью обучающихся, своевременной корректировки персональных образовательных результатов, обучающихся педагогическими средствами.

Текущему контролю успеваемости подлежат все обучающиеся, осваивающие учебную дисциплину.

Текущий контроль проводится в пределах учебного времени, отведенного на изучение дисциплины традиционными и инновационными методами с использованием современных технологий.

Результаты текущего контроля успеваемости обучающихся в виде оценки в балльном выражении («5», «4», «3», «2») записываются в журнале учебных занятий.

Промежуточная аттестация по учебной дисциплине проводится с целью оценки уровня освоения теоретических знаний, умений, приобретенного практического опыта.

Формы и периодичность промежуточной аттестации по дисциплине определяются учебным планом образовательной программы: зачет в 5, 6 семестрах, 7 семестр – дифференцированный зачет.

Зачет проводится непосредственно после завершения освоения дисциплины, в сроки, установленные календарным учебным графиком.

Вопросы и задания составляются на основе рабочей программы дисциплины. Вопросы и задания должны соответствовать проверяемым результатам обучения и доводятся до сведения обучающихся в течение первых двух месяцев от начала обучения.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОПЦ.13 Информационная **безопасность и защита информации** направлена на формирование следующих общих и профессиональных компетенций:

- **ОК 0**4. Эффективно взаимодействовать и работать в коллективе и команде;
- **ОК 05.** Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;
- **ОК 09**. Пользоваться профессиональной документацией на государственном и иностранном языках.

В результате освоения учебной дисциплины обучающийся должен овладеть профессиональными компетенциями:

- **ПК 1.3** Оформлять техническую документацию на проектируемые устройства
- **ПК 2.1.** Проектировать, разрабатывать и отлаживать программный код

модулей

- **ПК 2.2**. Владеть методами командной разработки программных продуктов. разработки алгоритмов решения поставленных задач в соответствии с требованиями технического задания или других принятых в организации нормативных документов.

В результате освоения дисциплины обучающийся должен:

уметь:

- формулировать тему, проблему, ставить цель и задачи, обосновывать актуальность проблемы, определять гипотезу, доказывать или опровергать ее.
- изготовлять продукт исследовательской деятельности.
- составлять содержание работы и план своих действий на каждом этапе.
- составлять структуру своего исследования.
- проводить исследование и делать вывод по его результатам.
- работать с различными источниками информации, используя разные формы защиты информации.
- выявлять вирусы.
- использовать современные средства защиты информации.

знать:

- современные методы защиты информации;
- основные виды угроз;
- виды продуктов вирусов;
- формы защиты информации в сети ЭВМ;
- требования к защите информации, критерии оценки угроз.

Общие компетенции:

Код компетенции	Формулировка компетенции	Знания, умения
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде	**Умения:** • организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности
		Знания: • психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	**Умения:** грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе
		Знания: • особенности социального и культурного контекста; правила оформления документов и построения устных сообщений.
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках	**Умения:** • понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые); • понимать тексты на базовые профессиональные темы; • участвовать в диалогах на знакомые общие и профессиональные темы;

		• строить простые высказывания о себе и о своей профессиональной деятельности; • кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы
		Знания: • правила построения простых и сложных предложений на профессиональные темы; • основные общеупотребительные глаголы (бытовая и профессиональная лексика); • лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности

Профессиональные компетенции:

Код и наименование компетенции	**Показатели освоения компетенции**
ПК.1.3. Оформлять техническую документацию на проектируемые устройства	**Умения:** • применять рекомендуемые нормативные и руководящие материалы на разрабатываемую техническую документацию; • пользоваться стандартным программным обеспечением при оформлении документации; • разрабатывать рабочие чертежи в соответствии с требованиями стандартов организации, национальных стандартов и технических регламентов; • применять имеющиеся шаблоны для составления технической документации; • использовать прикладные программы для разработки конструкторской документации.
	Знания: • основные требования Единой системы конструкторской документации (далее - ЕСКД); • правила оформления и внесения изменений в техническую и эксплуатационную документацию; • специальные пакеты прикладных программ для разработки конструкторской документации: наименования, возможности и порядок работы в них; • прикладные компьютерные программы для создания графических документов: • наименования, возможности и порядок работы в них
ПК 2.1. Проектировать, разрабатывать и отлаживать программный код модулей	**Практический опыт в:** • разработка программных модулей различной сложности в рамках учебных проектов; • участие в командной разработке программного обеспечения; • использование различных инструментов разработки; применение методов модульного тестирования и отладки программного кода.
	Умения: • проектировать структуру модулей в соответствии с требованиями технического задания; • разрабатывать программный код модулей на выбранном языке программирования; • использовать IDE и другие инструменты для написания, компиляции и

	отладки кода; • выполнять тестирование модулей для выявления и устранения ошибок; • оптимизировать программный код модулей для повышения производительности и эффективности; интегрировать разработанные модули в единое приложение.
	Знания: • принципы модульного программирования (инкапсуляция, абстракция, полиморфизм); • языки программирования высокого уровня, используемые для разработки прикладных приложений (например, C#, Java, Python); интегрированные среды разработки (IDE) и инструменты для работы с кодом (отладчики, системы контроля версий); Методы проектирования модулей (UML, блок-схемы); Алгоритмы и структуры данных, используемые в разрабатываемых модулях; Технологии доступа к данным (например, базы данных, веб-сервисы).
ПК 2.2. Размещать и обновлять информационный материал через систему управления контентом .	**Практический опыт в:** • размещении и обновлении информационных материалов через систему управления контентом (CMS); • преобразовании и перекомпоновки контента, связанная с изменением структуры контента, форм и требований к оформлению; • заполнении служебной информации (названий и идентификаторов страниц, ключевых слов, мета-тегов); настройки внутренних связей между информационными блоками/страницами в системе управления контентом; размещении новостей на веб-ресурсе и в социальных сетях.
	Умения: • заполнять веб-формы; • размещать мультимедийные объекты на веб-страницах; владеть функциональными особенностями популярных социальных сетей и форумов; создавать и обмениваться письмами электронной почты.
	Знания: • технологии организации и ведения новостных лент, рассылок по электронной почте; • нормы общения в социальных сетях, чатах и форумах (веб-этикета); принципы работы CMS и систем хранения файлов, информационных блоков.

ОПЦ.13 Информационная безопасность и защита информации

Наименование темы	ПК, ОК	Текущий контроль успеваемости	Промежуточная аттестация
Раздел 1. Общие вопросы информационный безопасности	ОК 04, ОК 05, ОК 09 ПК 1.3, ПК 2.1 ПК 2.2	Устный опрос, тестирование	Зачет Диф.зачет
Тема 1.1. Международные стандарты информационного обмена			
Тема 1.2. Понятия и угрозы.			
Раздел 2. Государственная система информационной безопасности			
Тема 2.1. Информационная безопасность в условиях функционирования в России глобальных сетей.			
Раздел 3. Угрозы безопасности			
Тема 3.1. Угрозы безопасности**.**			
Раздел 4. Теоретические основы методов защиты информационных систем			
Тема 4.1. Теоретические основы методов защиты информационных систем			
Раздел 5. Методы защиты средств вычислительной техники			
Тема 5.1. Методы защиты средств вычислительной техники			
Раздел 6. Основы криптографии			
Тема 6.1. Основы криптографии			
Раздел 7.Архитектура защитных экономических систем			
Тема 7.1. Архитектура защитных экономических систем			
Раздел 8. Алгоритмы и привязки программного обеспечения к аппаратному окружению			
Тема 8.1. Алгоритмы и привязки программного обеспечения к аппаратному окружению			
Раздел 9. Алгоритмы и привязки программного обеспечения к аппаратному окружению			
Тема 9.1. Алгоритмы безопасности в компьютерных сетях			

3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

3.1. Формы и методы оценивания

Формы текущего контроля по дисциплине*:*

- устный опрос (фронтальный, индивидуальный, комбинированный);
- тестирование (письменное или компьютерное);
- письменная проверка (ответы на вопросы, решение задач и примеров, составление тезисов, рефератов, выполнение схем, выполнение заданий для самостоятельной работы и др.);
- самоконтроль и взаимопроверка.

Возможны и другие формы текущего контроля успеваемости, в том числе инновационные на основе информационно-коммуникационных технологий.

Преподаватель на одном учебном занятии может использовать одну или несколько форм текущего контроля.

Промежуточная аттестация оценивает результаты учебной деятельности обучающихся за семестр (полугодие).

Основными формами промежуточной аттестации являются:

− зачёт;

- дифференцированный зачет.

3.2.Фонд оценочных средств для текущего контроля

Вопросы для устного опроса

1. Основные понятия защиты информации и информационной безопасности.
2. Классификация угроз информационной безопасности автоматизированных систем.
3. Непосредственные виды угроз для автоматизированных систем: угроза нарушения конфиденциальности, угроза нарушения целостности информации, угроза нарушения работоспособности. Угроза раскрытия параметров автоматизированной системы.
4. Назначение и структура стека протоколов TCP/IP. Характеристика протокола TCP/IP с точки зрения информационной безопасности.
5. Основные цели и характерные особенности сетевых атак. Виды сетевых атак: подслушивание (sniffing), подмена доверенного субъекта (IP – spoofing), посредничество в обмене незашифрованными ключами (Man-in-the-Middle).
6. Основные цели и характерные особенности сетевых атак. Виды сетевых атак: перехват сеанса (Session hijacking), отказ в обслуживании (Denial of Service, DoS), парольная атака полного перебора (brute force attack).
7. Основные цели и характерные особенности сетевых атак. Виды сетевых атак: угадывание ключа, атаки на уровне приложений, сетевая разведка, злоупотребление доверием.
8. Основные характеристики спама и методы борьбы с ним.
9. Виды интернет - мошенничества: фишинг и фарминг и методы борьбы с ними.
10. Угрозы и уязвимости проводных корпоративных сетей.
11. Особенности построения и актуальность защиты беспроводных сетей. Виды сетевых атак: вещание радиомаяка, обнаружение WLAN, подслушивание, ложные точки доступа в сеть.
12. Особенности построения и актуальность защиты беспроводных сетей. Виды сетевых атак: отказ в обслуживании, атаки типа “ человек в середине”, атака подмены ARP-записей, анонимный доступ в Интернет.
13. Способы обеспечения информационной безопасности компьютерных сетей. Фрагментарный и комплексный подходы.
14. Пути решения проблем защиты информации в сети Интернет. Информационная безопасность электронного бизнеса.

15. Основные понятия политики безопасности. Верхний, средний и нижний уровни политики безопасности.
16. Структура политики безопасности организации. Базовая и специализированные политики безопасности. Процедуры безопасности.
17. Основные этапы разработки политики безопасности
18. Аутентификация, авторизация и администрирование действий пользователей. Аутентификация на основе паролей.
19. Аутентификация на основе PIN-кода.
20. Строгая аутентификация. Примеры протоколов аутентификации.
21. Биометрическая аутентификация пользователя.
22. Электронные системы идентификации и аутентификации.
23. Комбинированные системы идентификации и аутентификации.
24. Понятие компьютерного вируса. Классификация вирусов.
25. Специализированные утилиты для борьбы с вредоносным ПО: анти шпионы, антируткиты и антикейлоггеры.
26. Троянские программы. Виды троянских программ.
27. Компьютерные черви. Виды компьютерных червей.
28. Методы борьбы с вирусами: обнаружение, основанное на сигнатурах, обнаружение программ подозрительного поведения, метод “белого списка”.
29. Методы борьбы с вирусами: обнаружение вирусов при помощи эмуляции работы программы, эвристический анализ, метод резидентных мониторов.
30. Антивирусные программы: утилита Dr. Web Curelt, программа Dr. Web., антивирус Avira AntiVir Personal, антивирус Avast! Home Edition.

3.3.Критерии оценивания

Критерии оценки для тестирования:

- «5» - 85-100% верных ответов
- «4» - 69-84% верных ответов
- «3» - 51-68% верных ответов
- «2» - 50% и менее

Критерии оценивания практической/лабораторной работы:

Оценка «5» ставится, если учащийся выполняет работу в полном объеме с соблюдением необходимой последовательности, все этапы работы проводит в условиях и режимах, обеспечивающих получение правильных результатов и выводов, соблюдает требования правил техники безопасности, правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, правильно выполняет анализ погрешностей.

Оценка «4» ставится, если выполнены все требования к оценке «5», но было допущено два-три недочета, не более одной негрубой ошибки и одного недочета

Оценка «3» ставится, если работа выполнена не полностью, но объем выполненной ее части позволяет получить правильный результат и вывод, или если в ходе проведения опыта и измерения были допущены ошибки

Оценка «2» ставится, если работа выполнена не полностью, или объем выполненной части работы не позволяет сделать правильных выводов, или если опыты, измерения, вычисления, наблюдения производились неправильно.

Критерии оценки результатов выполнения
внеаудиторной (самостоятельной) работы

Работа выполнена полностью, демонстрируются глубокие знания теоретического материала и умение их применять, последовательно и правильно выполнены все задания, сделаны выводы.

Оценка «5» - «отлично» выставляется, если работа выполнена полностью; демонстрируются глубокие знания теоретического материала и умение их применять; последовательно, правильно выполнены все задания; демонстрируется умение обоснованно излагать свои мысли, делать необходимые выводы.

Оценка «4» - «хорошо» выставляется, если работа выполнена полностью; демонстрируются глубокие знания теоретического материала и умение их применять; последовательно, правильно выполнены все задания; возможны единичные ошибки, исправляемые самим студентом после замечания преподавателя; демонстрируется умение обоснованно излагать свои мысли, делать необходимые выводы.

Оценка «3» - «удовлетворительно» выставляется, если студент демонстрирует затруднения с комплексным выполнением работы; неполное теоретическое обоснование, требующее наводящих вопросов преподавателя; выполняет задания при подсказке преподавателя; затрудняется в формулировке выводов.

Оценка «2» - «неудовлетворительно» выставляется, если работа не выполнена или выполнена неправильно; дана неправильная оценка предложенной ситуации; отсутствует теоретическое обоснование выполнения заданий.

3.4.Фонд оценочных средств для промежуточной аттестации
ТЕСТОВЫЕ ЗАДАНИЯ

1. Под информационной безопасностью понимается…

А) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации, и поддерживающей инфраструктуре.

Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия

В) нет правильного ответа

2. Защита информации – это..

А) комплекс мероприятий, направленных на обеспечение информационной безопасности.

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей

В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность?

А) от компьютеров

Б) от поддерживающей инфраструктуры

В) от информации

4. Основные составляющие информационной безопасности:

А) целостность

Б) достоверность

В) конфиденциальность

5. Доступность – это…
А) возможность за приемлемое время получить требуемую информационную услугу.
Б) логическая независимость
В) нет правильного ответа

6. Целостность – это..
А) целостность информации
Б) непротиворечивость информации
В) защищенность от разрушения

7. Конфиденциальность – это..
А) защита от несанкционированного доступа к информации
Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
В) описание процедур

8. Для чего создаются информационные системы?
А) получения определенных информационных услуг
Б) обработки информации
В) все ответы правильные

9. Целостность можно подразделить:
А) статическую
Б) динамичную
В) структурную

10. Где применяются средства контроля динамической целостности?
А) анализе потока финансовых сообщений
Б) обработке данных
В) при выявлении кражи, дублирования отдельных сообщений

11. Какие трудности возникают в информационных системах при конфиденциальности?
А) сведения о технических каналах утечки информации являются закрытыми
Б) на пути пользовательской криптографии стоят многочисленные технические проблемы
В) все ответы правильные

12. Угроза – это…
А) потенциальная возможность определенным образом нарушить информационную безопасность
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

13. Атака – это…
А) попытка реализации угрозы
Б) потенциальная возможность определенным образом нарушить информационную безопасность
В) программы, предназначенные для поиска необходимых программ.

14. Источник угрозы – это..
А) потенциальный злоумышленник
Б) злоумышленник
В) нет правильного ответа

15. Окно опасности – это…
А) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.
Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

16. Какие события должны произойти за время существования окна опасности?
А) должно стать известно о средствах использования пробелов в защите.
Б) должны быть выпущены соответствующие заплаты.
В) заплаты должны быть установлены в защищаемой И.С.

17. Угрозы можно классифицировать по нескольким критериям:
А) по спектру И.Б.
Б) по способу осуществления
В) по компонентам И.С.

18. По каким компонентам классифицируется угрозы доступности:
А) отказ пользователей
Б) отказ поддерживающей инфраструктуры
В) ошибка в программе

19. Основными источниками внутренних отказов являются:
А) отступление от установленных правил эксплуатации
Б) разрушение данных
В) все ответы правильные

20. Основными источниками внутренних отказов являются:
А) ошибки при конфигурировании системы
Б) отказы программного или аппаратного обеспечения
В) выход системы из штатного режима эксплуатации

21. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:
А) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности
Б) обрабатывать большой объем программной информации
В) нет правильного ответа

22. Какие существуют грани вредоносного П.О.?
А) вредоносная функция
Б) внешнее представление
В) способ распространения

23. По механизму распространения П.О. различают:
А) вирусы
Б) черви
В) все ответы правильные

24. Вирус – это…
А) код обладающий способностью к распространению путем внедрения в другие программы
Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
В) небольшая программа для выполнения определенной задачи

25. Черви – это…
А) код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения
Б) код обладающий способностью к распространению путем внедрения в другие программы
В) программа действий над объектом или его свойствами

26. Конфиденциальную информацию можно разделить:
А) предметную
Б) служебную
В) глобальную

27. Природа происхождения угроз:
А) случайные
Б) преднамеренные
В) природные

28. Предпосылки появления угроз:
А) объективные
Б) субъективные
В) преднамеренные

29. К какому виду угроз относится присвоение чужого права?
А) нарушение права собственности
Б) нарушение содержания
В) внешняя среда

30. Отказ, ошибки, сбой – это:
А) случайные угрозы
Б) преднамеренные угрозы
В) природные угрозы

31. Отказ - это…
А) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
Б) некоторая последовательность действий, необходимых для выполнения конкретного задания
В) структура, определяющая последовательность выполнения и взаимосвязи процессов

32. Ошибка – это…
А) неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния
Б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
В) негативное воздействие на программу

33. Сбой – это…
А) такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
Б) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния
В) объект-метод

34. Побочное влияние – это…
А) негативное воздействие на систему в целом или отдельные элементы
Б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
В) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

35. СЗИ (система защиты информации) делится:
А) ресурсы автоматизированных систем
Б) организационно-правовое обеспечение
В) человеческий компонент

36. Что относится к человеческому компоненту СЗИ?
А) системные порты
Б) администрация
В) программное обеспечение

37. Что относится к ресурсам А.С. СЗИ?
А) лингвистическое обеспечение
Б) техническое обеспечение
В) все ответы правильные

38. По уровню обеспеченной защиты все системы делят:
А) сильной защиты
Б) особой защиты
В) слабой защиты

39. По активности реагирования СЗИ системы делят:
А) пассивные
Б) активные
В) полупассивные

40. Правовое обеспечение безопасности информации – это…
А) совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) нет правильного ответа

41. Правовое обеспечение безопасности информации делится:
А) международно-правовые нормы
Б) национально-правовые нормы
В) все ответы правильные

42. Информацию с ограниченным доступом делят:
А) **государственную тайну**
Б) конфиденциальную информацию
В) достоверную информацию

43. Что относится к государственной тайне?
А) сведения, защищаемые государством в области военной, экономической … деятельности
Б) документированная информация
В) нет правильного ответа

44. Вредоносная программа - это…
А) программа, специально разработанная для нарушения нормального функционирования систем
Б) упорядочение абстракций, расположение их по уровням
В) процесс разделения элементов абстракции, которые образуют ее структуру и поведение

45. Основополагающие документы для обеспечения безопасности внутри организации:
А) трудовой договор сотрудников
Б) должностные обязанности руководителей
В) коллективный договор

46. К организационно - административному обеспечению информации относится:
А) взаимоотношения исполнителей
Б) подбор персонала
В) регламентация производственной деятельности

47. Что относится к организационным мероприятиям:
А) хранение документов
Б) проведение тестирования средств защиты информации
В) пропускной режим

48. Какие средства используется на инженерных и технических мероприятиях в защите информации:
А) аппаратные
Б) криптографические
В) физические

49. Программные средства – это…
А) специальные программы и системы защиты информации в информационных системах различного назначения
Б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла
В) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

50. Криптографические средства – это…
А) средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования
Б) специальные программы и системы защиты информации в информационных системах различного назначения
В) механизм, позволяющий получить новый класс на основе существующего

3.5.Ключи к тестам

№ Вопроса	Ответ	№ Вопроса	Ответ
1	А	**26**	А Б
2	А	**27**	А Б
3	А Б	**28**	А Б
4	А Б В	**29**	А
5	А	**30**	А
6	А Б В	**31**	А
7	А	**32**	А
8	А	**33**	А
9	А Б	**34**	А
10	А В	**35**	А Б В
11	В	**36**	А Б
12	А	**37**	В
13	А	**38**	А Б В
14	А	**39**	А Б
15	А	**40**	А
16	А Б В	**41**	В
17	А Б В	**42**	А Б
18	А Б	**43**	А
19	В	**44**	А
20	А Б В	**45**	А Б В
21	А	**46**	А Б В
22	А Б В	**47**	А В
23	В	**48**	А Б В
24	А	**49**	А
25	А	**50**	А

3.6. Критерии оценивания

Критерии оценки экзамена/зачета с оценкой

Оценка «5» - «отлично» выставляется обучающемуся, если демонстрируются всестороннее, систематическое и глубокое знание учебного программного материала, самостоятельно выполнивший все предусмотренные программой задания, глубоко усвоивший основную и дополнительную литературу, рекомендованную программой, активно работавший на практических, семинарских, лабораторных занятиях, разбирающийся в основных научных концепциях по изучаемой дисциплине, проявивший творческие способности и научный подход в понимании и изложении учебного программного материма, ответ отличается богатством и точностью использованных терминов, материал излагается последовательно и логично.

Оценка «4» - «хорошо» выставляется обучающемуся, если демонстрируются достаточно полное знание учебно-программного материала, не допускающий в ответе существенных неточностей, самостоятельно выполнивший все предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, активно работавший на практических, семинарских, лабораторных занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы, а также способность к их самостоятельному пополнению.

Оценка «3» - «удовлетворительно» выставляется обучающемуся, если демонстрируются знания основного учебно-программного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по профессии, не отличавшийся активностью на практических (семинарских) и лабораторных занятиях, самостоятельно выполнивший основные предусмотренные программой задания, однако допустивший погрешности при их выполнении и в ответе на экзамене, но обладающий необходимыми знаниями для устранения под руководством преподавателя наиболее существенных погрешностей.

Оценка «2» - «неудовлетворительно» выставляется обучающемуся, если обнаруживаются пробелы в знаниях или отсутствие знаний по значительной части основного учебно- программного материала, не выполнившему самостоятельно предусмотренные программой основные задания, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий, не отработавшему основные практические, семинарские, лабораторные занятия, допускающему существенные ошибки при ответе, и который не может продолжить обучение или приступить к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.

Критерии оценки для тестирования:

- «5» - 85-100% верных ответов
- «4» - 69-84% верных ответов
- «3» - 51-68% верных ответов
- «2» - 50% и менее

4. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Основные источники:

1) Криптография и безопасность в технологии .NET [Электронный ресурс] / П. Торстейнсон, Г. А. Ганеш ; пер. с англ. - 3-е изд. (эл.). - М. : БИНОМ, 2015. - (Программисту). - http://www.studentlibrary.ru/book/ISBN9785996329526.html Электронное издание на основе: Криптография и безопасность в технологии .NET [Электронный ресурс] / П. Торстейнсон, Г. А. Ганеш ; пер. с англ.-3-е изд. (эл.).-Электрон. текстовые дан. (1 файл pdf : 482 с.).-тМ. : БИНОМ. Лаборатория знаний, 2015.- (Программисту).-Систем. требования: Adobe Reader XI ; экран 10". - ISBN 978-5-9963-2952-6.

2) Интеллектуальные системы защиты информации [Электронный ресурс] : учеб. пособие/ Васильев В.И. - 2-е изд., испр. и доп. - М.: Машиностроение, 2013. - http://www.studentlibrary.ru/book/ISBN9785942756673.html Электронное издание на основе: Интеллектуальные системы защиты информации: учеб. пособие/ В. И. Васильев. 2-е изд., испр. и доп. - М.: Машиностроение, 2013.- 172 с. - ISBN 978-5-94275-667-3.13

3) Информатика 2015 [Электронный ресурс] : учебное пособие / Алексеев А.П. - М. : СОЛОН-ПРЕСС, 2015. - http://www.studentlibrary.ru/book/ISBN9785913591586.html Электронное издание на основе: Информатика 2015: учебное пособие/ Алексеев А.П.- 2015. - 400 с., илл. - ISBN 978-5-91359-158-6.

Дополнительные источники:

1) Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных сетях. - Ростов-на-Дону: Издательство СКНЦ ВШ, 2012.

2) Соколов А. В., Степанюк О. М. Защита от компьютерного терроризма. Справоч-ное пособие. - СПб.: БХВ - Петербург, Арлит, 2012.- 496с.:ил.