

Приложение 2 к РПД Защита информации
09.03.02 Информационные системы и технологии
Направленность (профиль) – Программно-аппаратные комплексы
Форма обучения – очная
Год набора - 2019

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ
АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

1. Общие сведения

1.	Кафедра	Информатики и вычислительной техники
2.	Направление подготовки	09.03.02 Информационные системы и технологии
3.	Направленность (профиль)	Программно-аппаратные комплексы
4.	Дисциплина (модуль)	Защита информации
5.	Форма обучения	очная
6.	Год набора	2019

2. Перечень компетенций

- | |
|---|
| <ul style="list-style-type: none">– способность применять системный подход и математические методы в формализации решения прикладных задач, моделировать прикладные (бизнес) процессы и предметную область автоматизации организации (ПК-2);– способность эксплуатировать и сопровождать информационные системы и сервисы, осуществлять ведение информационных хранилищ для решения прикладных задач профессиональной деятельности (ПК-3). |
|---|

3. Критерии и показатели оценивания компетенций на различных этапах их формирования

Этап формирования компетенции (разделы, темы дисциплины)	Формируемая компетенция	Критерии и показатели оценивания компетенций			Формы контроля сформированности компетенций
		Знать:	Уметь:	Владеть:	
Понятие Информационной безопасности. Введение	ПК-2	математические методы и алгоритмы используемые в разработке программного обеспечения для информационной безопасности компьютерных систем	применять на практике собственные и классические алгоритмы криптографической защиты данных	навыками работы с алгоритмами криптографической защиты данных	тестовый экспресс-опрос
Законодательный уровень информационной безопасности	ПК-3	виды контента информационных ресурсов предприятия и Интернет-ресурсов	ставить и решать схемотехнические задачи, связанные с выбором системы элементов при заданных требованиях к параметрам (временным, мощностным, габаритным, надежностным)	методами проектирования, разработки и реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятия	тестовый экспресс-опрос, решение задач (в виде программы)
Наиболее распространенные угрозы информационной безопасности					тестовый экспресс-опрос
Распространение объектно-ориентированного подхода на ИБ					тестовый экспресс-опрос
Административный уровень информационной безопасности	ПК-3	основы безопасности жизнедеятельности в области профессиональной деятельности	проектировать, внедрять и организовать эксплуатацию ИС и ИКТ	основными методами защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий; иметь представление о моделях безопасности ИС	тестовый экспресс-опрос, решение задач (в виде программы)
Процедурный уровень информационной безопасности	ПК-2 ПК-3	базовые понятия и определения, используемые в сфере информационной безопасности;	моделировать, анализировать и совершенствовать бизнес-процессы разрабатывать конкретные предложения по результатам исследований, готовить справочно-аналитические материалы для принятия управленческих	навыками работы с алгоритмами криптографической защиты данных	тестовый экспресс-опрос

Этап формирования компетенции (разделы, темы дисциплины)	Формируемая компетенция	Критерии и показатели оценивания компетенций			Формы контроля сформированности компетенций
		Знать:	Уметь:	Владеть:	
			решений		
Основные программно-технические меры безопасности информации	ПК-3	основные угрозы безопасности информации и возможные способы их реализации, а также методы и средства противодействия этим угрозам.	ставить и решать схемотехнические задачи, связанные с выбором системы элементов при заданных требованиях к параметрам (временным, мощностным, габаритным, надежностным)	методами проектирования, разработки и реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятия	тестовый экспресс-опрос, решение задач (в виде программы)
Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом	ПК-2 ПК-3	базовые понятия и определения, используемые в сфере информационной безопасности;	моделировать, анализировать и совершенствовать бизнес-процессы разрабатывать конкретные предложения по результатам исследований, готовить справочно-аналитические материалы для принятия управленческих решений	навыками работы с алгоритмами криптографической защиты данных	тестовый экспресс-опрос
Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная цифровая подпись	ПК-2	математические методы и алгоритмы используемые в разработке программного обеспечения для информационной безопасности компьютерных систем	применять на практике собственные и классические алгоритмы криптографической защиты данных	навыками работы с алгоритмами криптографической защиты данных	тестовый экспресс-опрос, решение задач (в виде программы)
Основные программно-технические меры безопасности информации: Экранирование, Анализ защищенности	ПК-3	основы безопасности жизнедеятельности в области профессиональной деятельности	проектировать, внедрять и организовать эксплуатацию ИС и ИКТ	основными методами защиты производственного персонала и населения от возможных последствий аварий, катастроф,	тестовый экспресс-опрос

Этап формирования компетенции (разделы, темы дисциплины)	Формируемая компетенция	Критерии и показатели оценивания компетенций			Формы контроля сформированности компетенций
		Знать:	Уметь:	Владеть:	
				стихийных бедствий; иметь представление о моделях безопасности ИС	

4. Критерии и шкалы оценивания

4.1. Тестовый экспресс-опрос (в т.ч. терминологический срез)

Процент правильных ответов	До 60	61-80	81-100
Количество баллов за решенный тест	0	1	2

4.2. Решение задач (в виде программы)

10 баллов выставляется, если обучающийся выполнил все лабораторные работы, правильно изложил все варианты решения, аргументировав их, с обязательной ссылкой на соответствующие нормативы (если по содержанию это необходимо) в поставленные сроки.

7 баллов выставляется, если обучающийся решил не менее 85% рекомендованных задач, правильно изложил все варианты решения, аргументировав их, с обязательной ссылкой на соответствующие нормативы (если по содержанию это необходимо).

5 баллов выставляется, если обучающийся решил не менее 65% рекомендованных задач, правильно изложил все варианты их решения, аргументировав их, с обязательной ссылкой на соответствующие нормативы (если по содержанию это необходимо).

0 баллов - если обучающийся выполнил менее 50% задания, и/или неверно указал варианты решения.

5. Типовые контрольные задания и методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

5.1. Типовое тестовое задание

Цель: проведение оперативного контроля и промежуточной аттестации по итогам освоения разделов (тем) дисциплины, в т.ч. для контроля самостоятельной работы учащихся по отдельным разделам дисциплины.

Тема 00 "Введение. Понятие информационной безопасности "

Ментальная карта начального уровня:

Информационная безопасность

Безопасность информации

Защита информации

Тема 1 "Понятие Информационной безопасности"

Письменный ответ на вопросы:

- ментальная карта понятий

- тезисы

- связный текст

1. Что такое информационная безопасность?

2. Что является основными составляющими информационной безопасности?

3. Какие цели и задачи имеет информационная безопасность?

4. В чем заключается важность и сложность проблемы информационной безопасности?

Тема 02 "Законодательный уровень информационной безопасности"

Сформулировать вопросы по разделам Темы:

- первый вопрос по указанному разделу

- второй (и более) вопрос по любым выбранным разделам Темы

1. Что такое законодательный уровень информационной безопасности и почему он важен []

2. Обзор российского законодательства в области информационной безопасности

<p>3. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности []</p> <p>4. Другие законы и нормативные акты РФ</p> <p>5. Обзор зарубежного законодательства в области информационной безопасности</p> <p>6. О текущем состоянии российского законодательства в области информационной безопасности</p> <p>--- если вопрос не по теме, то объяснить почему и привести пример правильного вопроса</p>
<p>Тема №03 "Наиболее распространенные угрозы информационной безопасности"</p> <p>1. Основные определения и критерии классификации угроз [];</p> <p>2. Наиболее распространенные угрозы доступности [];</p> <p>2.1 Примеры угроз доступности;</p> <p>2.2 Программные атаки на доступность;</p> <p>3. Вредоносное программное обеспечение;</p> <p>4. Основные угрозы целостности [];</p> <p>5. Основные угрозы конфиденциальности [];</p>
<p>Тема 04 "Распространение объектно-ориентированного подхода на ИБ"</p> <p>1. Что означает "распространение объектно-ориентированного подхода на информационную безопасность"</p> <p>2. В чём проявляется "распространение объектно-ориентированного подхода на информационную безопасность"</p> <p>3. Какие преимущества и недостатки имеет "распространение объектно-ориентированного подхода на информационную безопасность"</p>
<p>Тема 05 Административный уровень информационной безопасности</p> <p>1. Административный уровень информационной безопасности: Основные понятия []</p> <p>2. Политика безопасности []</p> <p>3. Программа безопасности</p> <p>4. Синхронизация программы безопасности с жизненным циклом систем</p>
<p>Тема 06 "Процедурный уровень информационной безопасности"</p> <p>Вопросы по подразделам темы: [общие вопросы]</p> <p>1. В чем заключается и для чего предназначен "процедурный уровень информационной безопасности"?</p> <p>[вопросы по вариантам]</p> <p>2. Каковы цели и особенности реализации указанного класса мер процедурного уровня ИБ?</p> <p>а. Управление персоналом</p> <p>б. Физическая защита</p> <p>в. Поддержание работоспособности</p> <p>г. Реагирование на нарушения режима безопасности</p> <p>д. Планирование восстановительных работ</p>
<p>Тема 07 "Основные программно-технические меры безопасности информации"</p> <p>[общие вопросы]</p> <p>1. В чем заключается и для чего предназначен "программно-технический уровень информационной безопасности"?</p> <p>[вопросы по вариантам]</p> <p>2. Почему средства по обеспечению безопасности в информационных системах называются "сервисами"? Что такое "полный набор сервисов ИБ" и как можно классифицировать сервисы в нем?</p> <p>3. Какие особенности современных информационных систем являются существенными с точки зрения организации информационной безопасности на программно-</p>

<p>техническом уровне?</p> <p>4. Что означает и какое место в обеспечении информационной безопасности занимает архитектурная безопасность?</p>
<p>Тема 08 "Основные программно-технические меры безопасности информации" [вопросы по вариантам]</p> <p>1. Для чего предназначена и какую роль в ИБ играет сервис X?</p> <p>2. Какие существуют способы реализации сервиса X и в чем их особенности? [варианты X]</p> <p>а. пара сервисов "идентификация" и "аутентификация"; б. сервис "управление доступом".</p>
<p>Тема 09 "Основные программно-технические меры безопасности информации" [вопросы по вариантам]</p> <p>1. Для чего предназначена и какую роль в ИБ играет сервис X?</p> <p>2. Какие существуют способы реализации сервиса X и в чем их особенности?</p> <p>3. Почему пара сервисов X обычно рассматривается совместно друг с другом? [варианты X]</p> <p>а. пара сервисов "протоколирование" и "аудит"; б. пара сервисов "шифрование" и "контроль целостности". [доп. вопрос]</p> <p>д4. Что такое, как реализуется и где используется "электронная цифровая подпись"?</p>
<p>Тема 10 "Основные программно-технические меры безопасности информации" [вопросы по вариантам]</p> <p>1. Для чего предназначена и какую роль в ИБ играет сервис X?</p> <p>2. Как и с какими угрозами ИБ позволяет бороться сервис X? [варианты X]</p> <p>а. Экранирование; б. Анализ защищенности.</p>
<p>Тема 11 "Криптография: шифрование и обеспечение целостности"</p> <p>в1 = Базовые понятия и Терминология в3 = Криптографические примитивы в4 = Криптографические хэш-функции в5 = Криптографические генераторы псевдослучайных чисел в6 = Модели основных криптоаналитических атак в7 = Анализ стойкости криптографических примитивов</p> <p>Практические рекомендации по использованию шифрования Криптографическое преобразование информации: методы подстановки.</p> <p>в2.1 = Моноалфавитные подстановки. Шифр Цезаря в2.2 = Многоалфавитные подстановки. Шифр Вижинера в2.3 = Монофонические шифры в 2.4 = Частотный анализ</p>
<p>Тема 12 "Протоколирование и аудит, шифрование, контроль целостности"</p> <p>Протоколирование и аудит Активный аудит Шифрование Контроль целостности</p>
<p>Тема 13 " Антивирусная защита компьютерных систем "</p> <p>Антивирусная защита компьютерных систем Вирусы и средства борьбы с ними Основы информационной безопасности при работе на компьютере Инфраструктуры открытых ключей</p>

Ключ: все вопросы открытого типа, что позволяет снизить давление на учащихся

ограниченным списком вариантов ответов, и дать им максимально свободные и профессионально творческие ответы во всем многообразии их правильных вариантов.

5.2. Пример задачи(в виде программы)

Написать программу преобразования исходных данных по методу гаммирования.

```
#include<iostream.h>
#include<conio.h>
#include<stdlib.h>
#include<math.h>

const int Max=12;
void main()
{
    bool M[Max]={true, true, false, true, false};
    bool A[Max]={false, true, false, true, true};
    randomize();
    for( short i=0;i<Max;i++){M[i]=floor(random(2));}
    for( short i=0;i<Max;i++){A[i]=floor(random(2));}
    //cout<<M[0];
    cout<<" ";
    for( short i=0;i<Max;i++){cout<<A[i];}
    cout<<"\n-----";
    for(int k=0;k<100;k++){
        cout<<"\n";

        float N = 0;
            for( short i=0;i<Max;i++){N+=M[i]*A[i];}

        cout<<"["<<M[0]<<"]<-";
        for( short i=0;i<Max;i++){cout<<M[i];}

        for( short i=1;i<Max;i++){M[i-1]=M[i];}

        M[Max-1]= fmod(N,2);
        cout<<"<-["<<M[Max-1]<<"]";
        getch();
    }
    getch();
}
```

5.3. Вопросы к промежуточной аттестации

1. Понятие информационной безопасности. Основные составляющие информационной безопасности.
2. Важность и сложность проблемы информационной безопасности
3. Программно-технические меры безопасности. Понятие сервиса информационной безопасности. Архитектурная безопасность.
4. Понятие сервиса информационной безопасности. Идентификация и аутентификация.
5. Понятие сервиса информационной безопасности. Управление доступом.
6. Понятие сервиса информационной безопасности. протоколирование и аудит.
7. Понятие сервиса информационной безопасности. управление и анализ защищенности.

8. Понятие сервиса информационной безопасности. обеспечение высокой доступности и отказоустойчивости.
9. Понятие сервиса информационной безопасности. экранирование и туннелирование.
10. Понятие сервиса информационной безопасности. криптография: шифрование.
11. Понятие сервиса информационной безопасности. криптография: контроль целостности.
12. Криптология : базовые понятия и терминология.
13. Криптографические примитивы и их свойства.
14. Модели основных криптоаналитических атак.
15. Антивирусная защита. История развития вирусов и их классификация. Методы защиты от вредоносных программ

ТЕХНОЛОГИЧЕСКАЯ КАРТА ДИСЦИПЛИНЫ
ОСНОВНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
09.03.02 Информационные системы и технологии
Направленность (профиль) «Программно-аппаратные комплексы»

(код, направление, профиль)

ТЕХНОЛОГИЧЕСКАЯ КАРТА

Шифр дисциплины по РУП		Б1.В.08					
Дисциплина		Защита информации					
Курс	4	семестр	7				
Кафедра		Информатики и вычислительной техники					
Ф.И.О. преподавателя, звание, должность			Федоров Андрей Михайлович, канд. техн. наук, доцент кафедры информатики и вычислительной техники				
Общ. трудоемкость ^{час/ЗЕТ}		144/4	Кол-во семестров	1	Форма контроля	Экзамен	
ЛК _{общ./тек. сем.}	32/32	ПР/СМ _{общ./тек. сем.}	-/-	ЛБ _{общ./тек. сем.}	32/32	СРС _{общ./тек. сем.}	44/44

Компетенции обучающегося, формируемые в результате освоения дисциплины:

- способность применять системный подход и математические методы в формализации решения прикладных задач, моделировать прикладные (бизнес) процессы и предметную область автоматизации организации (ПК-2);
- способность эксплуатировать и сопровождать информационные системы и сервисы, осуществлять ведение информационных хранилищ для решения прикладных задач профессиональной деятельности (ПК-3).

Код формируемой компетенции	Содержание задания	Количество мероприятий	Максимальное количество баллов	Срок предоставления
Вводный блок				
Не предусмотрен				
Основной блок				
ПК-2 ПК-3	Тестовый экспресс-опрос	10	20	В начале каждой лекции (проверка знаний предыдущей темы)
ПК-2 ПК-3	Решение задач (в виде программы)	4	40	По согласованию с преподавателем
Всего:			60	
ПК-2 ПК-3	Экзамен	Вопрос 1 Вопрос 2	20 20	В сроки сессии
Всего:			40	
Итого:			100	
Дополнительный блок				
ПК-2 ПК-3	Выполнение дополнительной лабораторной работы		10	по согласованию с преподавателем
Всего:			10	

Шкала оценивания в рамках балльно-рейтинговой системы МАГУ: «2» - 60 баллов и менее, «3» - 61-80 баллов, «4» - 81-90 баллов, «5» - 91-100 баллов.