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

2. Перечень компетенций

- 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 ПК-3	базовые понятия и определения, используемые в сфере информационной безопасности	готовить справочно-аналитические материалы для принятия управленческих решений	иметь представление о моделях безопасности ИС	Лабораторная работа (в виде программы)
Наиболее распространенные угрозы информационной безопасности	ПК-2 ПК-3	основы безопасности жизнедеятельности в области профессиональной деятельности	проектировать, внедрять в организации эксплуатацию ИС и ИКТ;	методами проектирования, разработки и реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятия	Лабораторная работа (в виде программы)
Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом	ПК-2 ПК-3	основные угрозы безопасности информации и возможные способы их реализации, а также методы и средства противодействия этим угрозам	применять на практике собственные и классические алгоритмы криптографической защиты данных	методами проектирования, разработки и реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятия	Лабораторная работа (в виде программы)
Криптография: шифрование и обеспечение целостности	ПК-2 ПК-3	основные угрозы безопасности информации и возможные способы их реализации, а также методы и средства противодействия этим угрозам	применять на практике собственные и классические алгоритмы криптографической защиты данных	методами проектирования, разработки и реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятия	Лабораторная работа (в виде программы)

4. Критерии и шкалы оценивания

4.1. Лабораторная работа (в виде программы)

15 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.

10 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. Пример лабораторной задачи

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();
}
```

5.2. Вопросы к экзамену

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	**7-8**				
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	**2**	Форма контроля	**Экзамен**		
ЛК $_{общ./тек.\ сем.}$	**6/6**	ПР/СМ$_{общ./тек.\ сем.}$	**-/-**	ЛБ$_{общ./тек.\ сем.}$	**12/12**	СРС $_{общ./тек.\ сем.}$	**117/117**

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	Лабораторные работы	4	60	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.