МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ

УТВЕРЖДАЮ
Декан факультета
_____ Володин В.М.
«_____»_____2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

С 1.2.22.1 Безопасность информационных систем и персональных данных

Специальность: 38.05.01 – Экономическая безопасность

Специализация: Экономика и организация производства на режимных объектах

Квалификация выпускника - экономист

Форма обучения - очная

Пенза, 2017

1. Цели освоения дисциплины

Целью изучения учебной дисциплины **«Безопасность информационных систем и персональных данных»** является приобретение знаний о системе безопасности информационных ресурсов, о методах борьбы с преступлениями в области информационных ресурсов. Ознакомление с организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области, борьбы с вирусами, изучение методов защиты информации. а также формирование элементов компетенций:

ОК-12 - способность работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации;

ПК-20 - способность соблюдать в профессиональной деятельности требования, установленные нормативными актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности.

В результате изучения дисциплины «Система безопасности информационных ресурсов» студенты должны:

знать: о системе безопасности информационных ресурсов, о методах борьбы с преступлениями в области информационных ресурсов; организационные, технические, алгоритмические и другие методы и средства защиты компьютерной информации, законодательство и стандарты в этой области, основы борьбы с вирусами, методы защиты информации;

уметь: работать с различными информационными ресурсами и технологиями, обеспечивать соблюдение режима секретности;

владеть: навыками применения основных методов, способов и средств получения, хранения, поиска, систематизации, обработки и передачи информации в профессиональной деятельности.

2. Место дисциплины «Безопасность информационных систем и персональных данных» в структуре специалитета

В соответствии с учебным планом по специальности 38.05.01 «Экономическая безопасность» дисциплина «Безопасность информационных систем и персональных данных» относится к дисциплинам по выбору студентов вариантной части.

Изучению данной дисциплины предшествовали такие дисциплины как «Информационные технологии в сфере экономической безопасности», «Информационные системы в экономике». Полученные знания и навыки могут применяться при изучении таких дисциплин, как «Теневая экономика», «Правовые основы экономической безопасности общества, государства и личности», «Экономическая безопасность», «Методы выявления экономических правонарушений» и т.д.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины «Безопасность информационных систем и персональных данных»

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данной специальности:

Коды компетенции	Наименование компетенции	Структурные элементы компетенции (в результате освоения дисциплины обучающийся должен знать, уметь, владеть)
1	2	3
ОК-12	способность работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации.	Знать: различные информационные ресурсы и технологии, основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации.
		Уметь: работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации
		Владеть: навыками применения основных методов, способов и средств получения, хранения, поиска, систематизации, обработки и передачи информации в профессиональной деятельности.
ПК-20	способность соблюдать в профессиональной деятельности требования, установленные нормативными актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности..	Знать: установленные нормативные акты в области защиты государственной тайны и информационной безопасности, обеспечивающие соблюдение режима секретности.
		Уметь: соблюдать в профессиональной деятельности требования, установленные нормативными актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности.
		Владеть: навыками использования нормативных актов в области защиты государственной тайны и информационной безопасности, обеспечивающие соблюдение режима секретности.

1. 4. Структура и содержание дисциплины «Безопасность информационных систем и персональных данных»

4.1. Структура дисциплины

Общая трудоемкость дисциплины составляет __2___ зачетные единицы, __72_____ часа.

№ п/п	Наименование разделов и тем дисциплины	Семестр	Недели семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)									Формы текущего контроля успеваемости *(по неделям семестра)*							
				Аудиторная работа				Самостоятельная работа												
				Всего	Лекция	Практические занятия	Лабораторные занятия	Всего	Подготовка к аудиторным занятиям	Реферат, эссе и др.	Курсовая работа (проект)	Подготовка к экзамену	Собеседование	Коллоквиум	Проверка тестов	Проверка контрольн. работ	Проверка реферата	Проверка эссе и иных творческих работ	курсовая работа (проект)	др.
1.	**Тема I. Информационные системы и персональные данные. Основные понятия и определения.** Информационные системы и документирование информации. Безопасность информационных систем. Государственные информационные системы. Персональные данные о гражданах. Права на доступ к информации. Вычислительные сети и	2	1-3	8	4	4		8	4	4			1		3		2			

	защита информации. Нормативно-правовая база функционирования систем защиты информации. Компьютерные преступления и особенности их расследования.																			
2.	**Тема II. Изучение источников, рисков и форм атак на информационные системы, вредоносные программы и компьютерные вирусы. Проблемы защиты информационных систем.** Изучение источников, рисков и форм атак на информационные системы, вредоносные программы и компьютерные вирусы. Проблемы защиты информационных систем. Классификация угроз и меры по обеспечению сохранности информационных систем. Классификация рисков и основные задачи обеспечения безопасности информационных систем. Защита локальных сетей и операционных систем. Интеграция систем защиты. Internet в структуре информационно-	2	4-6	6	3	3		6	3	3			4		5		6			

	аналитического обеспечения ИС и угрозы исходящие от использования «электронной почты».																			
3.	**Тема III. Правовые основы информационной безопасности и защита интеллектуальной собственности** Нормативно-правовые документы, регламентирующие отношения в сфере информационной безопасности. Предмет и задачи правового обеспечения информационной безопасности. Законодательство о безопасности и защите информации, его структура и содержание. История создания правового института по охране авторского права. Субъекты авторского права. Права обладателей авторских прав. Авторские и патентные права. Ущерб от незаконного использования авторских и смежных прав. Интеллектуальная	2	7-10	8	4	4		8	4	4			7		10	8	9			

	собственность. Произведения, пользующиеся охраной. Правовые нормы и стандарты по лицензированию и сертификации.																			
4.	**Тема 4. Программные средства защиты персональной информации** Классификация вирусов. Каналы проникновения вирусов. Способы заражения. Современные антивирусные средства. Средства антивирусной защиты мобильных телефонов и КПК. Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Разграничение доступа. Межсетевые экраны как средство защиты от несанкционированного доступа. Персональные и корпоративные межсетевые экраны. Криптографические средства защиты. Криптографическое преобразование данных. Симметричные и асимметричные методы шифрования. Общая	2	11-14	8	4	4		8	4	4			11		13	12	14			

	технология шифрования. Технология шифрования речи. Кодирование информации. Электронная цифровая подпись.																				
5	**Тема 5. Технические средства защиты и комплексное обеспечение безопасности.** Организационные требования к системам информационной защиты ИС. Требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению. Требования по применению способов, методов и средств защиты информации. Требования к документированию событий в системе и выявлению несанкционированного доступа. Организация аудита информационной безопасности ИС и предприятия в целом.	2	15-18	6	3	3		6	3	3			15		16	17	18				
	Курсовая работа (проект)																				
	Подготовка к зачету											*12*									
6	Общая трудоемкость, в часах			36	18	18		36	18	18			Промежуточная аттестация								
													Форма				Семестр				
													Зачет				*2*				
													Экзамен								

4.2. Содержание дисциплины

Тема I.
Информационные системы и персональные данные. Основные понятия и определения.
Информационные системы и документирование информации. Безопасность информационных систем. Государственные информационные системы. Персональные данные о гражданах. Права на доступ к информации. Вычислительные сети и защита информации. Нормативно-правовая база функционирования систем защиты информации. Компьютерные преступления и особенности их расследования.

Тема II.
Изучение источников, рисков и форм атак на информационные системы, вредоносные программы и компьютерные вирусы. Проблемы защиты информационных систем.
Изучение источников, рисков и форм атак на информационные системы, вредоносные программы и компьютерные вирусы. Проблемы защиты информационных систем. Классификация угроз и меры по обеспечению сохранности информационных систем. Классификация рисков и основные задачи обеспечения безопасности информационных систем. Защита локальных сетей и операционных систем. Интеграция систем защиты. Internet в структуре информационно-аналитического обеспечения ИС и угрозы исходящие от использования «электронной почты».

Тема III.
Правовые основы информационной безопасности и защита интеллектуальной собственности
Нормативно-правовые документы, регламентирующие отношения в сфере информационной безопасности. Предмет и задачи правового обеспечения информационной безопасности. Законодательство о безопасности и защите информации, его структура и содержание.
История создания правового института по охране авторского права. Субъекты авторского права. Права обладателей авторских прав. Авторские и патентные права. Ущерб от незаконного использования авторских и смежных прав. Интеллектуальная собственность. Произведения, пользующиеся охраной.

Тема 4.
Программные средства защиты персональной информации
Классификация вирусов. Каналы проникновения вирусов. Способы заражения. Современные антивирусные средства. Средства антивирусной защиты мобильных телефонов и КПК.
Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Разграничение доступа. Межсетевые экраны как средство защиты от несанкционированного доступа. Персональные и корпоративные межсетевые экраны.
Криптографические средства защиты. Криптографическое преобразование данных. Симметричные и асимметричные методы шифрования. Общая

технология шифрования. Технология шифрования речи. Кодирование информации. Электронная цифровая подпись.

Тема 5. Технические средства защиты и комплексное обеспечение безопасности.

Организационные требования к системам информационной защиты ИС. Требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению. Требования по применению способов, методов и средств защиты информации. Требования к документированию событий в системе и выявлению несанкционированного доступа. Организация аудита информационной безопасности ИС и предприятия в целом.

5. Образовательные технологии

При проведении занятий по дисциплине «**БИС и ПД**» используются активные и интерактивные методы обучения (деловые и ролевые игры, разбор конкретных ситуаций, мозговые штурмы). Занятия проводятся с использованием ТСО (мультимедийного компьютерного проектора). При проведении самостоятельной работы студентов используется электронный учебник и материалы, размещенные в сети Интернет.

В целях реализации индивидуального подхода к обучению студентов, в том числе с ограниченными возможностями здоровья, осуществляющих учебный процесс по собственной траектории в рамках индивидуального рабочего плана, изучение данной дисциплины базируется на следующих возможностях: обеспечение внеаудиторной работы со студентами в том числе в электронной образовательной среде с использованием соответствующего программного оборудования, дистанционных форм обучения, возможностей Интернет-ресурсов, индивидуальных консультаций и т.д.

По каждому разделу дисциплины на практических занятиях проводятся тесты для определения знаний и формирования профессиональных компетенций.

Перечень активных методов обучения:

1. Пленарная дискуссия «Изучение Российского законодательства по защите информационных технологий. Изучение нормативно-правовой информации».
2. Тесты.
3. Доклады «Влияние человеческого фактора на обеспечение информационной безопасности, методы социальной инженерия»
4. Тесты.
5. Экономический тренинг «Анализ способов защиты информации в компьютерных сетях от разрушающего программного воздействия. Изучение методов борьбы с компьютерными вирусами и средств защиты информации в Internet. Угрозы исходящие от использования " электронной почты».
6. Тесты.
7. Дискуссия «Уточнение задач информационной безопасности организации. Изучение источников, рисков и форм атак на информации».
8. Тесты.

По каждому разделу дисциплины подготавливается реферат до периода начала его изучения.

По каждому разделу дисциплины на практических занятиях проводятся тесты для определения знаний и формирования профессиональных компетенций.

Занятия, проводимые в интерактивных формах, с использованием интерактивных технологий составляют _60__% аудиторных занятий.

6. Учебно-методическое обеспечение самостоятельной работы студентов.
Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.
6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1	**Тема I.** **Информационные системы и персональные данные. Основные понятия и определения.** Информационные системы и документирование информации. Безопасность информационных систем. Государственные информационные системы. Персональные данные о гражданах. Права на доступ к информации. Вычислительные сети и защита информации. Нормативно-правовая база функционирования систем защиты информации. Компьютерные преступления и особенности их расследования.	Собеседование, написание рефератов, тесты	Информационные ресурсы и документирование информации. Безопасность информационных ресурсов. Нормативно-правовая база функционирования систем защиты информации.	Мизюркина Л. А. «Система безопасности информационных ресурсов. Учебно-методическое пособие.(в печати) Пенза: Изд-во ПГУ, 2017 г. – 65 с. (100 шт.). Рабочая программа дисциплины. Криворотов, В. В. Экономическая безопасность государства и регионов [Электронный ресурс] : учеб. пособие для студентов вузов, обучающихся по направлению «Экономика» / В. В. Криворотов, А. В. Калина, Н. Д. Эриашвили. - М.: ЮНИТИ-ДАНА, 2012. - 351 с. - ISBN 978-5-238-01947-5. http://znanium.com/catalog.php. Экономическая безопасность: Учебное пособие / Н.В. Манохина, М.В. Попов, Н.П. Колядин, И.Э. Жадан; Под ред. Н.В. Манохиной - М.: НИЦ ИНФРА-М, 2014. - 320 с.: 60x90 1/16. - (Высшее образование: Бакалавриат). (п) ISBN 978-5-16-009002-3, 500 экз. http://znanium.com/catalog.php.	**16**
2	**Тема II.** **Изучение источников, рисков и форм атак на информационные системы, вредоносные программы и компьютерные вирусы. Проблемы защиты информационных систем.** Изучение источников, рисков и форм атак на информационные	Собеседование, написание рефератов, тесты	Проблемы защиты информационных ресурсов. Классификация угроз и меры по обеспечению сохранности информационных ресурсов. Интеграция систем защиты. Internet в структуре	Мизюркина Л. А. «Система безопасности информационных ресурсов. Учебно-методическое пособие.(в печати) Пенза: Изд-во ПГУ, 2017 г. – 65 с. (100 шт.). Рабочая программа дисциплины. Криворотов, В. В. Экономическая безопасность государства и регионов [Электронный ресурс] : учеб. пособие для студентов вузов, обучающихся по направлению «Экономика» / В. В. Криворотов, А. В.	12

	системы, вредоносные программы и компьютерные вирусы. Проблемы защиты информационных систем. Классификация угроз и меры по обеспечению сохранности информационных систем. Классификация рисков и основные задачи обеспечения безопасности информационных систем. Защита локальных сетей и операционных систем. Интеграция систем защиты. Internet в структуре информационно-аналитического обеспечения ИС и угрозы исходящие от использования «электронной почты».		информационно-аналитического обеспечения.	Калина, Н. Д. Эриашвили. - М.: ЮНИТИ-ДАНА, 2012. - 351 с. - ISBN 978-5-238-01947-5. http://znanium.com/catalog.php. Экономическая безопасность: Учебное пособие / Н.В. Манохина, М.В. Попов, Н.П. Колядин, И.Э. Жадан; Под ред. Н.В. Манохиной - М.: НИЦ ИНФРА-М, 2014. - 320 с.: 60x90 1/16. - (Высшее образование: Бакалавриат). (п) ISBN 978-5-16-009002-3, 500 экз. http://znanium.com/catalog.php.	
3	**Тема III.** **Правовые основы информационной безопасности и защита интеллектуальной собственности** Нормативно-правовые документы, регламентирующие отношения в сфере информационной безопасности. Предмет и задачи правового обеспечения информационной безопасности. Законодательство о безопасности и защите информации, его структура и содержание. История создания правового института по охране авторского права. Субъекты авторского права. Права обладателей авторских прав.	Собеседование, написание рефератов, тесты, контрольная работа	Законодательная, нормативно-методическая и научная база систем защиты информации. Российское законодательство по защите информационных технологий. Политика безопасности.	Мизюркина Л. А. «Система безопасности информационных ресурсов. Учебно-методическое пособие.(в печати) Пенза: Изд-во ПГУ, 2017 г. – 65 с. (100 шт.). Рабочая программа дисциплины. Криворотов, В. В. Экономическая безопасность государства и регионов [Электронный ресурс] : учеб. пособие для студентов вузов, обучающихся по направлению «Экономика» / В. В. Криворотов, А. В. Калина, Н. Д. Эриашвили. - М.: ЮНИТИ-ДАНА, 2012. - 351 с. - ISBN 978-5-238-01947-5. http://znanium.com/catalog.php. Экономическая безопасность: Учебное пособие / Н.В. Манохина, М.В. Попов, Н.П. Колядин, И.Э. Жадан; Под ред. Н.В. Манохиной - М.: НИЦ ИНФРА-М, 2014. - 320 с.: 60x90 1/16. - (Высшее образование: Бакалавриат). (п) ISBN 978-5-16-009002-3, 500 экз. http://znanium.com/catalog.php.	16

	Авторские и патентные права. Ущерб от незаконного использования авторских и смежных прав. Интеллектуальная собственность. Произведения, пользующиеся охраной.				
4	**Тема 4. Программные средства защиты персональной информации** Классификация вирусов. Каналы проникновения вирусов. Способы заражения. Современные антивирусные средства. Средства антивирусной защиты мобильных телефонов и КПК. Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Разграничение доступа. Межсетевые экраны как средство защиты от несанкционированного доступа. Персональные и корпоративные межсетевые экраны. Криптографические средства защиты. Криптографическое преобразование данных. Симметричные и асимметричные методы шифрования. Общая технология шифрования. Технология шифрования речи. Кодирование информации. Электронная цифровая подпись.	Собеседование, написание рефератов, тесты, контрольная работа	Понятие разрушающего программного воздействия. Компьютерные вирусы как особый класс разрушающих программных воздействия.. Рекомендации по защите информации Internet.	Мизюркина Л. А. «Система безопасности информационных ресурсов. Учебно-методическое пособие.(в печати) Пенза: Изд-во ПГУ, 2017 г. – 65 с. (100 шт.). Рабочая программа дисциплины. Криворотов, В. В. Экономическая безопасность государства и регионов [Электронный ресурс] : учеб. пособие для студентов вузов, обучающихся по направлению «Экономика» / В. В. Криворотов, А. В. Калина, Н. Д. Эриашвили. - М.: ЮНИТИ-ДАНА, 2012. - 351 с. - ISBN 978-5-238-01947-5. http://znanium.com/catalog.php. Экономическая безопасность: Учебное пособие / Н.В. Манохина, М.В. Попов, Н.П. Колядин, И.Э. Жадан; Под ред. Н.В. Манохиной - М.: НИЦ ИНФРА-М, 2014. - 320 с.: 60x90 1/16. - (Высшее образование: Бакалавриат). (п) ISBN 978-5-16-009002-3, 500 экз. http://znanium.com/catalog.php.	16
5	**Тема 5. Технические средства защиты и комплексное**	Собеседование,	Организационные требования к системам	Мизюркина Л. А. «Система безопасности информационных ресурсов. Учебно-методическое	12

	обеспечение безопасности. Организационные требования к системам информационной защиты ИС. Требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению. Требования по применению способов, методов и средств защиты информации. Требования к документированию событий в системе и выявлению несанкционированного доступа. Организация аудита информационной безопасности ИС и предприятия в целом.	написание рефератов, тесты, контрольная работа	информационной защиты ИС. Требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению.	пособие.(в печати) Пенза: Изд-во ПГУ, 2017 г. – 65 с. (100 шт.). Рабочая программа дисциплины. Криворотов, В. В. Экономическая безопасность государства и регионов [Электронный ресурс] : учеб. пособие для студентов вузов, обучающихся по направлению «Экономика» / В. В. Криворотов, А. В. Калина, Н. Д. Эриашвили. - М.: ЮНИТИ-ДАНА, 2012. - 351 с. - ISBN 978-5-238-01947-5. http://znanium.com/catalog.php. Экономическая безопасность: Учебное пособие / Н.В. Манохина, М.В. Попов, Н.П. Колядин, И.Э. Жадан; Под ред. Н.В. Манохиной - М.: НИЦ ИНФРА-М, 2014. - 320 с.: 60x90 1/16. - (Высшее образование: Бакалавриат). (п) ISBN 978-5-16-009002-3, 500 экз. http://znanium.com/catalog.php.	

6.2. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа студента по темам дисциплины «Безопасность информационных систем и персональных данных» предусмотрена в объеме, определенном учебным планом в количестве 72 часа. Ее целями являются:

усвоение и закрепление студентами теоретического материала, в том числе в процессе чтения лекций;

приобретение навыков самостоятельного анализа сложных систем, умения выделить и самостоятельно изучить элементы, входящие в состав системы, а также выявить причину возникновения проблемы и способы ее решения;

овладение методикой профессионального изложения и оформления изученного материала в соответствующей письменной научно-теоретической работе;

приобретение опыта аргументации выносимых на защиту самостоятельно полученных результатов (обобщений, выводов).

Самостоятельная работа включает в себя изучение и конспектирование дополнительной литературы в соответствии с программой курса; консультации преподавателя по наиболее сложным темам.

В соответствии с учебным планом студентам надлежит выполнить самостоятельную работу по дисциплине в форме устного ответа с последующей дискуссией, тестов, написания рефератов.

Собеседование. Основной формой самостоятельной работы студента является изучение конспекта лекций, их дополнение рекомендованной литературой, активное участие на практических и семинарских занятиях. После изучения рекомендованной литературы студент докладывает на семинарских занятиях изученную им тему, отвечая на дополнительные вопросы, возникающие в ходе собеседования. При условии получения преподавателем полноценного ответа студент получает максимально предусмотренный балльно-рейтингоовой системой бал. Все отступления от полноценного ответа оцениваются преподавателем в индивидуальном порядке.

Тестирование. Тесты воспринимаются студентами как своеобразная игра. Тем самым снимается целый ряд психологических проблем – страхов, стрессов, которые, к сожалению, характерны для обычных форм контроля знаний студентов. Основное достоинство тестовой формы контроля – это простота и скорость, с которой осуществляется первая оценка уровня обученности по конкретной теме, позволяющая, к тому же, реально оценить готовность к итоговому контролю в иных формах и, в случае необходимости, откорректировать те или иные элементы темы.

Написание рефератов. Реферат – краткое изложение содержания документа или его части, научной работы, включающее основные фактические сведения и выводы, необходимые для первоначального ознакомления с источниками и определения целесообразности обращения к ним. Современные требования к реферату – точность и объективность в передаче сведений, полнота отображения основных элементов как по содержанию, так и по форме. Цель реферата - не только сообщить о содержании реферируемой работы, но и дать представление о вновь возникших проблемах соответствующей отрасли науки.

Рефераты в рамках учебного процесса в вузе оцениваются по следующим основным критериями:

- актуальность содержания, высокий теоретический уровень, глубина и полнота анализа фактов, явлений, проблем, относящихся к теме;

- информационная насыщенность, новизна, оригинальность изложения вопросов;

- простота и доходчивость изложения;

-структурная организованность, логичность, грамматическая правильность и стилистическая выразительность;

- убедительность, аргументированность, практическая значимость и теоретическая обоснованность предложений и выводов.

6.3. Материалы для проведения текущего и промежуточного контроля знаний студентов

Контроль освоения компетенций

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1	Собеседование	1,2,3,4,5.	ОК-12, ПК -20
2	Написание рефератов	1,2,3,4,5.	ОК-12, ПК -20
3	Проведение тестов	1,2,3,4,5.	ОК-12, ПК -20
4	Контрольная работа	3,4,5.	ОК-12, ПК -20
5	Зачет	1,2,3,4,5.	ОК-12, ПК -20

Перечень тем рефератов

1. Криптографические модели.
2. Симметричные и ассиметричные криптосистемы для защиты компьютерной информации в ИС.
3. Международные и Государственные стандарты информационной безопасности и их использование в практической деятельности.
4. Многоуровневая защита корпоративных сетей.
5. Режим функционирования межсетевых экранов и их основные компоненты.
6. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация.
7. Применение межсетевых экранов для организации виртуальных корпоративных сетей.
8. Программные методы защиты информации.
9. Защита компьютерных систем от удаленных атак через сеть Intrnet.
10. Анализ способов защиты информации в компьютерных сетях от разрушающего программного воздействия. Изучение методов борьбы с компьютерными вирусами и средств защиты информации в Internet. Угрозы исходящие от использования " электронной почты

Методические рекомендации по написанию реферата

Структура реферата должна включать следующие разделы:

Раздел 1 – излагаются актуальность и теоретические аспекты рассматриваемой темы.

Раздел 2 – дается характеристика предприятия, по материалам которого выполняется реферат. Название и виды деятельности предприятия характеристика выпускаемой продукции (производимых работ, оказываемых услуг, выполняемых функций); схема производственной структуры; таблица основных технико-экономических показателей и другая информация применительно к теме.

Раздел 3 – приводятся методика и результаты анализа, проведенного студентом в соответствии с выбранной темой.

Раздел 4 самостоятельная оценка полученных в результате анализа данных, выводы и аргументированные предложения по совершенствованию соответствующей сферы деятельности или функций рассматриваемого предприятия.

Объем реферата – 35-40 страниц.

Работу надо проиллюстрировать конкретными расчетами графиками, аналитическими таблицами, отчетными данными. В списке использованной литературы указываются фамилии инициалы авторов, название работы, место издания, издательство и год издания; приводятся название статей, журналов, года и номера их издания.

Изложение отдельных вопросов темы должно быть подчинено раскрытию темы в целом, их следует узнать друг с другом. Для этого необходимо предварительно ознакомиться со специальной литературой по выбранной теме, составить ее список. Предпочтительно пользоваться изданиями последних лет.

Особое внимание следует обратить на то, чтобы содержание работы не носило отвлеченного характера и не сводилось к общим рассуждениям. В связи с этим наряду с четким теоретическим освещением соответствующих вопросов организации промышленного предприятия обязательно нужно раскрыть методику их практического решения в конкретных условиях.

Наиболее важный этап выполнения реферата изучение и систематизация собранных материалов по узловым вопросам избранной темы. Студенту необходимо критически проанализировать имеющиеся в его распоряжении литературные источники и практические материалы, выявить в них наиболее важные моменты и на их основе самостоятельно изложить тему.

Все расчеты выполняются по формам действующей на конкретном предприятии документации планирования и отчетности. Совершенно исключается дословное заимствование текста из учебных пособий и литературы. При цитировании необходимо указать источник (сноска в конце страницы).

Вопросы для собеседования

1. Уточнение задач информационной безопасности организации. Изучение источников, рисков и форм атак на информации.
2. Изучение Российского законодательства по защите информационных технологий. Изучение нормативно-правовой информации.

3. Изучение средств защиты локальных сетей от несанкционированного доступа. Анализ функционирования маршрутизаторов, шлюзов сетевого уровня и межсетевых экранов.
4. Влияние человеческого фактора на обеспечение информационной безопасности, методы социальной инженерия.
5. Методы шифрования трафика. Способы применения SSL-сертификатов. Методы организации атак отказа в обслуживании (DoS, DDoS) и борьбы с ними.

ТЕСТЫ

Тесты 1

1. СВЕДЕНИЯ (СООБЩЕНИЯ, ДАННЫЕ) НЕЗАВИСИМО ОТ ФОРМЫ ИХ ПРЕДСТАВЛЕНИЯ:
1.Информация
2. Информационные технологии
3. Информационная система
4. Информационно-телекоммуникационная сеть
5. Обладатель информации.

2. ПРОЦЕССЫ, МЕТОДЫ ПОИСКА, СБОРА, ХРАНЕНИЯ, ОБРАБОТКИ, ПРЕДОСТАВЛЕНИЯ, РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ И СПОСОБЫ ОСУЩЕСТВЛЕНИЯ ТАКИХ ПРОЦЕССОВ И МЕТОДОВ:
1. Информация
2. Информационные технологии
3. Информационная система
4. Информационно-телекоммуникационная сеть
5. Обладатель информации.

3. ЛИЦО, САМОСТОЯТЕЛЬНО СОЗДАВШЕЕ ИНФОРМАЦИЮ ЛИБО ПОЛУЧИВШЕЕ НА ОСНОВАНИИ ЗАКОНА ИЛИ ДОГОВОРА ПРАВО РАЗРЕШАТЬ ИЛИ ОГРАНИЧИВАТЬ ДОСТУП К ИНФОРМАЦИИ:
1. Источник информации
2. Потребитель информации
3. Уничтожитель информации
4. Носитель информации
5. Обладатель информации.

4. ТЕХНОЛОГИЧЕСКАЯ СИСТЕМА, ПРЕДНАЗНАЧЕННАЯ ДЛЯ ПЕРЕДАЧИ ПО ЛИНИЯМ СВЯЗИ ИНФОРМАЦИИ, ДОСТУП К КОТОРОЙ ОСУЩЕСТВЛЯЕТСЯ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ЭТО:
1. База данных
2. Информационная технология
3. Информационная система
4. Информационно-телекоммуникационная сеть
5. Медицинская информационная система.

5.ОБЯЗАТЕЛЬНОЕ ДЛЯ ВЫПОЛНЕНИЯ ЛИЦОМ, ПОЛУЧИВШИМ ДОСТУП К ОПРЕДЕЛЕННОЙ ИНФОРМАЦИИ, ТРЕБОВАНИЕ НЕ ПЕРЕДАВАТЬ ТАКУЮ ИНФОРМАЦИЮ ТРЕТЬИМ ЛИЦАМ БЕЗ СОГЛАСИЯ ЕЕ ОБЛАДАТЕЛЯ ЭТО:
1. Электронное сообщение
2. Распространение информации
3. Предоставление информации
4. Конфиденциальность информации
5. Доступ к информации.

6. ДЕЙСТВИЯ, НАПРАВЛЕННЫЕ НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ НЕОПРЕДЕЛЕННЫМ КРУГОМ ЛИЦ ИЛИ ПЕРЕДАЧУ ИНФОРМАЦИИ НЕОПРЕДЕЛЕННОМУ КРУГУ ЛИЦ ЭТО:

1. Уничтожение информации
2. Распространение информации
3. Предоставление информации
4. Конфиденциальность информации
5. Доступ к информации

7.ВОЗМОЖНОСТЬ ПОЛУЧЕНИЯ ИНФОРМАЦИИ И ЕЕ ИСПОЛЬЗОВАНИЯ ЭТО:

1. Сохранение информации
2. Распространение информации
3. Предоставление информации
4. Конфиденциальность информации
5. Доступ к информации.

8.ИНФОРМАЦИЯ, ПЕРЕДАННАЯ ИЛИ ПОЛУЧЕННАЯ ПОЛЬЗОВАТЕЛЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ:

1. Электронное сообщение
2. Информационное сообщение
3. Текстовое сообщение
4. Визуальное сообщение
5. SMS-сообщение.

9.ВСЕ КОМПОНЕНТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ, В КОТОРОМ НАКАПЛИВАЮТСЯ И ОБРАБАТЫВАЮТСЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ЭТО:

1. Информационная система персональных данных
2. База данных
3. Централизованное хранилище данных
4. Система Статэкспресс
5. Сервер.

10.К СВЕДЕНИЯМ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА, СОГЛАСНО УКАЗУ ПРЕЗИДЕНТА РФ ОТ 6 МАРТА 1997 Г., ОТНОСЯТСЯ:

1. Информация о распространении программ
2. Информация о лицензировании программного обеспечения
3. Информация, размещаемая в газетах, Интернете
4. Персональные данные
5. Личная тайна

11.ОТНОШЕНИЯ, СВЯЗАННЫЕ С ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ, РЕГУЛИРУЮТСЯ ЗАКОНОМ…

1. «Об информации, информационных технологиях»
2. «О защите информации»
3. Федеральным законом «О персональных данных»
4. Федеральным законом «О конфиденциальной информации»
5. «Об утверждении перечня сведений конфиденциального характера».

12.ДЕЙСТВИЯ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ (СОГЛАСНО ЗАКОНУ), ВКЛЮЧАЯ СБОР, СИСТЕМАТИЗАЦИЮ, НАКОПЛЕНИЕ, ХРАНЕНИЕ, ИСПОЛЬЗОВАНИЕ, РАСПРОСТРАНЕНИЕ И Т. Д ЭТО:

1. «Исправление персональных данных»
2. «Работа с персональными данными»
3. «Преобразование персональных данных»
4. «Обработка персональных данных»
5. «Изменение персональных данных».

13. ДЕЙСТВИЯ, В РЕЗУЛЬТАТЕ КОТОРЫХ НЕВОЗМОЖНО ОПРЕДЕЛИТЬ ПРИНАДЛЕЖНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ КОНКРЕТНОМУ СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ:
1. Выделение персональных данных
2. Обеспечение безопасности персональных данных
3. Деаутентификация
4. Деавторизация
5. Деперсонификация

14. ПО РЕЖИМУ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПОДРАЗДЕЛЯЮТСЯ НА:
1. Многопользовательские
2. Однопользовательские
3. Без разграничения прав доступа
4. С разграничением прав доступа
5. Системы, не имеющие подключений.

15. ПРОЦЕСС СООБЩЕНИЯ СУБЪЕКТОМ СВОЕГО ИМЕНИ ИЛИ НОМЕРА, С ЦЕЛЬЮ ПОЛУЧЕНИЯ ОПРЕДЕЛЁННЫХ ПОЛНОМОЧИЙ (ПРАВ ДОСТУПА) НА ВЫПОЛНЕНИЕ НЕКОТОРЫХ (РАЗРЕШЕННЫХ ЕМУ) ДЕЙСТВИЙ В СИСТЕМАХ С ОГРАНИЧЕННЫМ ДОСТУПОМ:
1. Авторизация
2. Аутентификация
3. Обезличивание
4. Деперсонализация
5. Идентификация.

16. ПРОЦЕДУРА ПРОВЕРКИ СООТВЕТСТВИЯ СУБЪЕКТА И ТОГО, ЗА КОГО ОН ПЫТАЕТСЯ СЕБЯ ВЫДАТЬ, С ПОМОЩЬЮ НЕКОЙ УНИКАЛЬНОЙ ИНФОРМАЦИИ:
1. Авторизация
2. Обезличивание
3. Деперсонализация
4. Аутентифика́ция
5. Идентификация.

17. ПРОЦЕСС, А ТАКЖЕ РЕЗУЛЬТАТ ПРОЦЕССА ПРОВЕРКИ НЕКОТОРЫХ ОБЯЗАТЕЛЬНЫХ ПАРАМЕТРОВ ПОЛЬЗОВАТЕЛЯ И, ПРИ УСПЕШНОСТИ, ПРЕДОСТАВЛЕНИЕ ЕМУ ОПРЕДЕЛЁННЫХ ПОЛНОМОЧИЙ НА ВЫПОЛНЕНИЕ НЕКОТОРЫХ (РАЗРЕШЕННЫХ ЕМУ) ДЕЙСТВИЙ В СИСТЕМАХ С ОГРАНИЧЕННЫМ ДОСТУПОМ
1. Авторизáция
2. Идентификация
3. Аутентификация
4. Обезличивание
5. Деперсонализация.

Тест 2

1. ПРОСТЕЙШИМ СПОСОБОМ ИДЕНТИФИКАЦИИ В КОМПЬЮТЕРНОЙ СИСТЕМЕ ЯВЛЯЕТСЯ ВВОД ИДЕНТИФИКАТОРА ПОЛЬЗОВАТЕЛЯ, КОТОРЫЙ ИМЕЕТ СЛЕДУЮЩЕЕ НАЗВАНИЕ:
1. Токен
2. Password
3. Пароль
4. Login

5. Смарт-карта.

2. ОСНОВНОЕ СРЕДСТВО, ОБЕСПЕЧИВАЮЩЕЕ КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ, ПОСЫЛАЕМОЙ ПО ОТКРЫТЫМ КАНАЛАМ ПЕРЕДАЧИ ДАННЫХ, В ТОМ ЧИСЛЕ – ПО СЕТИ ИНТЕРНЕТ:

1. Идентификация
2. Аутентификация
3. Авторизация
4. Экспертиза
5. Шифрование.

3. ДЛЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ ДАННЫХ ПО КАНАЛАМ ИНТЕРНЕТ ИСПОЛЬЗУЕТСЯ ТЕХНОЛОГИЯ:

1. WWW
2. DICOM
3. VPN
4. FTP
5. XML.

4.КОМПЛЕКС АППАРАТНЫХ И/ИЛИ ПРОГРАММНЫХ СРЕДСТВ, ОСУЩЕСТВЛЯЮЩИЙ КОНТРОЛЬ И ФИЛЬТРАЦИЮ СЕТЕВОГО ТРАФИКА В СООТВЕТСТВИИ С ЗАДАННЫМИ ПРАВИЛАМИ И ЗАЩИЩАЮЩИЙ КОМПЬЮТЕРНЫЕ СЕТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА:

1. Антивирус
2. Замок
3. Брандма́уэр
4. Криптография
5. Экспертная система.

5. ЗА ПРАВОНАРУШЕНИЯ В СФЕРЕ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЗАЩИТЫ ИНФОРМАЦИИ ДАННЫЙ ВИД НАКАЗАНИЯ НА СЕГОДНЯШНИЙ ДЕНЬ НЕ ПРЕДУСМОТРЕН:

1. Дисциплинарные взыскания
2. Административный штраф
3. Уголовная ответственность
4. Лишение свободы
5. Смертная казнь.

6. НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ ЭТО:

1. Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально
2. Работа на чужом компьютере без разрешения его владельца
3. Вход на компьютер с использованием данных другого пользователя
4. Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей
5. Доступ к СУБД под запрещенным именем пользователя.

7. «ПЕРСОНАЛЬНЫЕ ДАННЫЕ» ЭТО:

1. Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу
2. Фамилия, имя, отчество физического лица
3. Год, месяц, дата и место рождения, адрес физического лица
4. Адрес проживания физического лица
5. Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна».

8. В ДАННОМ СЛУЧАЕ СОТРУДНИК УЧРЕЖДЕНИЯ МОЖЕТ БЫТЬ ПРИВЛЕЧЕН К ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:

1. Выход в Интернет без разрешения администратора

2. При установке компьютерных игр
3. В случаях установки нелицензионного ПО
4. В случае не выхода из информационной системы
5. В любом случае неправомочного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности.

9. МОЖЕТ ЛИ СОТРУДНИК БЫТЬ ПРИВЛЕЧЕН К УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ:
1. Нет, только к административной ответственности
2. Нет, если это государственное предприятие
3. Да
4. Да, но только в случае, если действия сотрудника нанесли непоправимый вред
5. Да, но только в случае осознанных неправомочных действий сотрудника

10. ПРОЦЕДУРА, ПРОВЕРЯЮЩАЯ, ИМЕЕТ ЛИ ПОЛЬЗОВАТЕЛЬ С ПРЕДЪЯВЛЕННЫМ ИДЕНТИФИКАТОРОМ ПРАВО НА ДОСТУП К РЕСУРСУ ЭТО:
1. Идентификация
2. Аутентификация
3. Стратификация
4. Регистрация
5. Авторизация.

11.НАИБОЛЕЕ ОПАСНЫМ ИСТОЧНИКОМ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ ЯВЛЯЮТСЯ:
1. Другие предприятия (конкуренты)
2. Сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам
3. Рядовые сотрудники предприятия
4. Возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных
5. Хакеры.

12.ВЫБЕРИТЕ, МОЖНО ЛИ В СЛУЖЕБНЫХ ЦЕЛЯХ ИСПОЛЬЗОВАТЬ ЭЛЕКТРОННЫЙ АДРЕС (ПОЧТОВЫЙ ЯЩИК), ЗАРЕГИСТРИРОВАННЫЙ НА ОБЩЕДОСТУПНОМ ПОЧТОВОМ СЕРВЕРЕ, НАПРИМЕР НА MAIL.RU:
1. Нет, не при каких обстоятельствах
2. Нет, но для отправки срочных и особо важных писем можно
3. Можно, если по нему пользователь будет пересылать информацию, не содержащую сведений конфиденциального характера
4. Можно, если информацию предварительно заархивировать с помощью программы winrar с паролем
5. Можно, если других способов электронной передачи данных на предприятии или у пользователя в настоящий момент нет, а информацию нужно переслать срочно.

13.ДОКУМЕНТИРОВАННАЯ ИНФОРМАЦИЯ, ДОСТУП К КОТОРОЙ ОГРАНИЧИВАЕТ В СООТВЕТСТВИИ С ЗАКОНАДЕЛЬСТВОМ РФ:
1. Информация составляющая государственную тайну
2. Информация составляющая коммерческую тайну
3. Персональная
4. Конфиденциальная информация
5. Документированная информация.

14.ДЛЯ ТОГО ЧТОБЫ СНИЗИТЬ ВЕРОЯТНОСТЬ УТРАТЫ ИНФОРМАЦИИ НЕОБХОДИМО:
1. Регулярно производить антивирусную проверку компьютера
2. Регулярно выполнять проверку жестких дисков компьютера на наличие ошибок
3. Регулярно копировать информацию на внешние носители (сервер, компакт-диски, флэш-карты)

4. Защитить вход на компьютер к данным паролем
5. Проводить периодическое обслуживание ПК.

15.ПАРОЛЬ ПОЛЬЗОВАТЕЛЯ ДОЛЖЕН
1. Содержать цифры и буквы, знаки препинания и быть сложным для угадывания
2. Содержать только цифры
3. Содержать только буквы
4. Иметь явную привязку к владельцу (его имя, дата рождения, номер телефона и т.п.)
5. Быть простым и легко запоминаться, например «123», «111», «qwerty» и т.д.

16.ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЕСПЕЧИВАЕТ…
1. Блокирование информации
2. Искажение информации
3. Сохранность информации
4. Утрату информации
5. Подделку информации.

17.ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ «О ГОСУДАРСТВЕННОЙ ТАЙНЕ» БЫЛ ПРИНЯТ В СЛЕДУЮЩЕМ ГОДУ:
1. 1982
2. 1985
3. 1988
4. 1993
5. 2005.

18.ДОКУМЕНТИРОВАННОЙ ИНФОРМАЦИЕЙ, ДОСТУП К КОТОРОЙ ОГРАНИЧЕН В СООТВЕТСТВИИ С ЗАКОНОДАТЕЛЬСТВОМ РФ, НАЗЫВАЕТСЯ
1. Конфиденциальная
2. Персональная
3. Документированная
4. Информация составляющая государственную тайну
5. Информация составляющая коммерческую тайну.

19. ИНФОРМАЦИЯ ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЕ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ОПИСАНА В:
1. 1 главе Уголовного кодекса
2. 5 главе Уголовного кодекса
3. 28 главе Уголовного кодекса
4. 100 главе Уголовного кодекса
5. 1000 главе Уголовного кодекса.

20. В СТАТЬЕ 272 УГОЛОВНОГО КОДЕКСА ГОВОРИТСЯ…
1. О неправомерном доступе к компьютерной информации
2. О создании, исполнении и распространении вредоносных программ для ЭВМ
3. О нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети
4. О преступлениях в сфере компьютерной информации
5. Об ответственности за преступления в сфере компьютерной информации

Тесты 3

1.ФЕДЕРАЛЬНЫЙ ЗАКОН «ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ» НАПРАВЛЕН НА:
1. Регулирование взаимоотношений в информационной сфере совместно с гражданским кодексом РФ
2. Регулирование взаимоотношений в гражданском обществе РФ
3. Регулирование требований к работникам служб, работающих с информаций
4. Формирование необходимых норм и правил работы с информацией

5. Формирование необходимых норм и правил, связанных с защитой детей от информации

1. ХИЩЕНИЕ ИНФОРМАЦИИ – ЭТО…
1. Несанкционированное копирование информации
2. Утрата информации
3. Блокирование информации
4. Искажение информации
5. Продажа информации

2. ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ПЕРВОЙ КАТЕГОРИИ ЯВЛЯЕТСЯ…
1. Государство
2. Коммерческая организация
3. Муниципальное учреждение
4. Любой гражданин
5. Группа лиц, имеющих общее дело

3. ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ВТОРОЙ КАТЕГОРИИ ЯВЛЯЕТСЯ…
1. Простые люди
2. Государство
3. Коммерческая организация
4. Муниципальное учреждение
5. Некоммерческая организация

5.ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ТРЕТЬЕЙ КАТЕГОРИИ ЯВЛЯЕТСЯ…
1. Люди
2. Государство
3. Муниципальное учреждение
4. Учреждение
5. Некоммерческая организация

6.ИНФОРМАЦИЕЙ, СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, ВЛАДЕЮТ:
1. Государство
2. Только образовательные учреждения
3. Только президиум Верховного Совета РФ
4. Граждане Российской Федерации
5. Только министерство здравоохранения

7.ИНФОРМАЦИЕЙ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ, ВЛАДЕЮТ:
1. Государство
2. Различные учреждения
3. Государственная Дума
4. Граждане Российской Федерации
5. Медико-социальные организации

8.ПЕРСОНАЛЬНЫМИ ДАННЫМИ ВЛАДЕЮТ:
1. Государство
2. Различные учреждения
3. Государственная Дума
4. Жители Российской Федерации
5. Медико-социальные организации

9.ДОСТУП К ИНФОРМАЦИИ – ЭТО:
1. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
2. Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц
3. Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц

4. Информация, переданная или полученная пользователем информационно-телекоммуникационной сети
5. Возможность получения информации и ее использования

10.ДОКУМЕНТИРОВАННАЯ ИНФОРМАЦИЯ, ДОСТУП К КОТОРОЙ ОГРАНИЧИВАЕТСЯ В СООТВЕТСТВИИ С ЗАКОНОДАТЕЛЬСТВОМ РОССИЙСКОЙ ФЕДЕРАЦИИ ЭТО:
1. Конфиденциальная информация
2. Документы офера и договоров
3. Факс
4. Личный дневник
5. Законы РФ

11.ПЛАСТИКОВАЯ КАРТОЧКА, СОДЕРЖАЩАЯ ЧИП ДЛЯ КРИПТОГРАФИЧЕСКИХ ВЫЧИСЛЕНИЙ И ВСТРОЕННУЮ ЗАЩИЩЕННУЮ ПАМЯТЬ ДЛЯ ХРАНЕНИЯ ИНФОРМАЦИИ:
1. Токен
2. Password
3. Пароль
4. Login
5. Смарт-карта

12.УСТРОЙСТВО ДЛЯ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ, ПРЕДСТАВЛЯЮЩЕЕ СОБОЙ МОБИЛЬНОЕ ПЕРСОНАЛЬНОЕ УСТРОЙСТВО, НАПОМИНАЮЩИЕ МАЛЕНЬКИЙ ПЕЙДЖЕР, НЕ ПОДСОЕДИНЯЕМЫЕ К КОМПЬЮТЕРУ И ИМЕЮЩИЕ СОБСТВЕННЫЙ ИСТОЧНИК ПИТАНИЯ:
1. Токен
2. Автономный токен
3. USB-токен
4. Устройство iButton
5. Смарт-карта

13.ДОСТУП ПОЛЬЗОВАТЕЛЯ К ИНФОРМАЦИОННЫМ РЕСУРСАМ КОМПЬЮТЕРА И / ИЛИ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ ДОЛЖЕН РАЗРЕШАТЬСЯ ТОЛЬКО ПОСЛЕ:
1. Включения компьютера
2. Идентификации по логину и паролю
3. Запроса паспортных данных
4. Запроса доменного имени
5. Запроса ФИО

14.АППАРАТНЫЕ МОДУЛИ ДОВЕРЕННОЙ ЗАГРУЗКИ «АККОРД - АМДЗ» ПРЕДСТАВЛЯЮТ СОБОЙ…
1. Аппаратный контролер
2. Электронный замок
3. Система контроля
4. Сетевой адаптер
5. Копировальный аппарат

15.ЭЛЕКТРОННЫЕ ЗАМКИ «СОБОЛЬ» ПРЕДНАЗНАЧЕНЫ ДЛЯ …
1. Обеспечения доверенной загрузки компьютера и контроля целостности файлов в системах
2. Сканирования отпечатков пальцев
3. Проверки скорости и загрузки файлов
4. Общего контроля
5. Идентификации пользователя

16.ФЕДЕРАЛЬНЫЙ ЗАКОН "ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ" ДАЕТ ОПРЕДЕЛЕНИЕ ИНФОРМАЦИИ:
1. Текст книги или письма

2. Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
3. Сведения о явлениях и процессах
4. Факты и идеи в формализованном виде
5. Шифрованный текст, текст на неизвестном языке

17. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЕСТЬ ОБЕСПЕЧЕНИЕ…
1. Независимости информации
2. Изменения информации
3. Копирования информации
4. Сохранности информации
5. Преобразования информации

Тесты 4

1. ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ЭТО ДЕЯТЕЛЬНОСТЬ ПО ПРЕДОТВРАЩЕНИЮ:

1. Получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации
2. Воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации
3. Воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений
4. Неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа
5. Несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

2. ЗАЩИТА ИНФОРМАЦИИ ЭТО:

1. Процесс сбора, накопления, обработки, хранения, распределения и поиска информации
2 Преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа
3. Получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств
4. Совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям
5. Деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

3. ЕСТЕСТВЕННЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ВЫЗВАНЫ:

1. Деятельностью человека
2. Ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения
3. Воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека
4. Корыстными устремлениями злоумышленников
5. Ошибками при действиях персонала.

4. ИКУССТВЕННЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ВЫЗВАНЫ:

1. Деятельностью человека;

2. Ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения
3. Воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека
4. Корыстными устремлениями злоумышленников
5. Ошибками при действиях персонала.

5. К ОСНОВНЫМ НЕПРЕДНАМЕРЕННЫМ ИСКУССТВЕННЫМ УГРОЗАМ АСОИ ОТНОСИТСЯ:
1. Физическое разрушение системы путем взрыва, поджога и т.п.
2. Перехват побочных электромагнитных, акустических и других излучений устройств и линий связи
3. Изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.
4. Чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств
5. Неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

6. К ПОСТОРОННИМ ЛИЦАМ НАРУШИТЕЛЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОТНОСИТСЯ:
1. Представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации
2. Персонал, обслуживающий технические средства
3. Технический персонал, обслуживающий здание
4. Пользователи
5. Сотрудники службы безопасности
6. Представители конкурирующих организаций
7. Лица, нарушившие пропускной режим

7. СПАМ, КОТОРЫЙ ИМЕЕТ ЦЕЛЬ ОПОРОЧИТЬ ТУ ИЛИ ИНУЮ ФИРМУ, КОМПАНИЮ, ПОЛИТИЧЕСКОГО КАНДИДАТА И Т.П:
1. Черный пиар
2. Фишинг
3. Нигерийские письма
4. Источник слухов
5. Пустые письма.

8. СПАМ РАСПРОСТРАНЯЕТ ПОДДЕЛЬНЫЕ СООБЩЕНИЯ ОТ ИМЕНИ БАНКОВ ИЛИ ФИНАНСОВЫХ КОМПАНИЙ, ЦЕЛЬЮ КОТОРЫХ ЯВЛЯЕТСЯ СБОР ЛОГИНОВ, ПАРОЛЕЙ И ПИН-КОДОВ ПОЛЬЗОВАТЕЛЕЙ:
1. Черный пиар
2. Фишинг
3. Нигерийские письма
4. Источник слухов
5. Пустые письма.

9. АНТИВИРУС ОБЕСПЕЧИВАЕТ ПОИСК ВИРУСОВ В ОПЕРАТИВНОЙ ПАМЯТИ, НА ВНЕШНИХ НОСИТЕЛЯХ ПУТЕМ ПОДСЧЕТА И СРАВНЕНИЯ С ЭТАЛОНОМ КОНТРОЛЬНОЙ СУММЫ:
1. Детектор;
2. Доктор
3. Сканер
4. Ревизор
5. Сторож.

10. АНТИВИРУС НЕ ТОЛЬКО НАХОДИТ ЗАРАЖЕННЫЕ ВИРУСАМИ ФАЙЛЫ, НО И "ЛЕЧИТ" ИХ, Т.Е. УДАЛЯЕТ ИЗ ФАЙЛА ТЕЛО ПРОГРАММЫ ВИРУСА, ВОЗВРАЩАЯ ФАЙЛЫ В ИСХОДНОЕ СОСТОЯНИЕ:

1. Детектор
2. Доктор
3. Сканер
4. Ревизор
5. Сторож.

11. АНТИВИРУС ЗАПОМИНАЕТ ИСХОДНОЕ СОСТОЯНИЕ ПРОГРАММ, КАТАЛОГОВ И СИСТЕМНЫХ ОБЛАСТЕЙ ДИСКА КОГДА КОМПЬЮТЕР НЕ ЗАРАЖЕН ВИРУСОМ, А ЗАТЕМ ПЕРИОДИЧЕСКИ ИЛИ ПО КОМАНДЕ ПОЛЬЗОВАТЕЛЯ СРАВНИВАЕТ ТЕКУЩЕЕ СОСТОЯНИЕ С ИСХОДНЫМ:
1. Детектор
2. Доктор
3. Сканер
4. Ревизор
5. Сторож.

12. АНТИВИРУС ПРЕДСТАВЛЯЕТ СОБОЙ НЕБОЛЬШУЮ РЕЗИДЕНТНУЮ ПРОГРАММУ, ПРЕДНАЗНАЧЕННУЮ ДЛЯ ОБНАРУЖЕНИЯ ПОДОЗРИТЕЛЬНЫХ ДЕЙСТВИЙ ПРИ РАБОТЕ КОМПЬЮТЕРА, ХАРАКТЕРНЫХ ДЛЯ ВИРУСОВ:
1. Детектор
2. Доктор
3. Сканер
4. Ревизор
5. Сторож.

13. АКТИВНЫЙ ПЕРЕХВАТ ИНФОРМАЦИИ ЭТО ПЕРЕХВАТ, КОТОРЫЙ:
1. Заключается в установке подслушивающего устройства в аппаратуру средств обработки информации
2. Основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций
3. Неправомерно использует технологические отходы информационного процесса
4. Осуществляется путем использования оптической техники
5. Осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

14. ПЕРЕХВАТ, КОТОРЫЙ ЗАКЛЮЧАЕТСЯ В УСТАНОВКЕ ПОДСЛУШИВАЮЩЕГО УСТРОЙСТВА В АППАРАТУРУ СРЕДСТВ ОБРАБОТКИ ИНФОРМАЦИИ НАЗЫВАЕТСЯ:
1. Активный перехват
2. Пассивный перехват
3. Аудиоперехват
4. Видеоперехват
5. Просмотр мусора.

15. ПЕРЕХВАТ, КОТОРЫЙ ОСНОВАН НА ФИКСАЦИИ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ, ВОЗНИКАЮЩИХ ПРИ ФУНКЦИОНИРОВАНИИ СРЕДСТВ КОМПЬЮТЕРНОЙ ТЕХНИКИ И КОММУНИКАЦИЙ НАЗЫВАЕТСЯ:
1. Активный перехват
2. Пассивный перехват
3. Аудиоперехват
4. Видеоперехват
5. Просмотр мусора.

16. ПЕРЕХВАТ, КОТОРЫЙ ОСУЩЕСТВЛЯЕТСЯ ПУТЕМ ИСПОЛЬЗОВАНИЯ ОПТИЧЕСКОЙ ТЕХНИКИ НАЗЫВАЕТСЯ:
1. Активный перехват
2. Пассивный перехват
3. Аудиоперехват
4. Видеоперехват

5. Просмотр мусора.
17. К ВНУТРЕННИМ НАРУШИТЕЛЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОТНОСИТСЯ:
1. Клиенты;
2. Пользователи системы
3. Посетители
4. Любые лица, находящиеся внутри контролируемой территории
5. Представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации
6. Персонал, обслуживающий технические средства
7. Сотрудники отделов разработки и сопровождения ПО
8. Технический персонал, обслуживающий здание.

Тесты 5

1. КАКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДУСМАТРИВАЮТ РЕГУЛИРОВАНИЕ ДОСТУПА КО ВСЕМ РЕСУРСАМ ИНФОРМАЦИОННЫХ СИСТЕМ УПРАВЛЕНИЯ
1. Программные.
2. Физические.
3. Законодательные.
4. Организационные.
2. К МЕТОДАМ ЗАЩИТЫ ИНФОРМАЦИИ ОТНОСИТСЯ ШИФРОВАНИЕ ИНФОРМАЦИИ:
1. Программных.
2. Физических.
3. Законодательного.
4. Организационных.
3. К МЕТОДАМ ЗАЩИТЫ ИНФОРМАЦИИ ОТНОСИТСЯ УСТАНОВКА СИСТЕМ СИГНАЛИЗАЦИИ
1. Программных.
2. Физических.
3. Законодательного.
4. Организационных.
4. КАКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДУСМАТРИВАЮТ РАЗРАБОТКУ НОРМАТИВНЫХ АКТОВ, КОТОРЫМИ РЕГЛАМЕНТИРУЮТСЯ ПРАВИЛА ИСПОЛЬЗОВАНИЯ И ОБРАБОТКИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА:
1. Программные.
2. Физические.
3. Законодательные.
4. Организационные.
5. КАКОЙ СЕРВИС БЕЗОПАСНОСТИ ОБЕСПЕЧИВАЕТ ПОДТВЕРЖДЕНИЕ ИЛИ ОТРИЦАНИЕ ТОГО, ЧТО ПОЛЬЗОВАТЕЛЬ ИНФОРМАЦИИ ИМЕННО ТОТ, КОТОРЫЙ УКАЗАН:
1. Сервис аутентификации.
2. Сервис обеспечения целостности.
3. Сервис засекречивания данных.
4. Сервис контроля доступа.
6. КАКОВ МЕХАНИЗМ НАРУШЕНИЙ БЕЗОПАСНОСТИ ДАННЫХ ПРИВОДИТ К НАРУШЕНИЮ ЦЕЛОСТНОСТИ ДАННЫХ:
1. Разделение.
2. Перехват.

3. Модификация.
4. Фальсификация.
7. КАКОЙ СПЕЦИАЛИСТ ОТВЕЧАЕТ ЗА ПРИОБРЕТЕНИЕ И ВНЕДРЕНИЕ НОВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РЕСУРСАМИ В ОРГАНИЗАЦИИ:
1. IT-менеджер.
2. Программист.
3. Системный аналитик.
4. Системный администратор.
8. КАКОЙ СПЕЦИАЛИСТ ЗАНИМАЕТСЯ НАПИСАНИЕМ И КОРРЕКТИРОВКОЙ ПРОГРАММ ДЛЯ ЭВМ:
1. Руководитель ИТ-проекта.
2. Программист.
3. Системный аналитик.
4. Системный администратор.
9. КАКОЙ СПЕЦИАЛИСТ ОБЕСПЕЧИВАЕТ ШТАТНУЮ РАБОТУ ПАРКА КОМПЬЮТЕРНОЙ ТЕХНИКИ, СЕТИ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, А ТАКЖЕ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ В ОРГАНИЗАЦИИ:
1. Руководитель ИТ-проекта.
2. Программист.
3. Системный аналитик.
4. Системный администратор.
10. ВЫБЕРИТЕ ОДНУ ИЗ ОСОБЕННОСТЕЙ ПЕРСОНАЛА, КВАЛИФИЦИРОВАННО РАБОТАЮЩЕГО С ИТ:
1. Низкий уровень интеллекта.
2. Высокая востребованность на рынке труда.
3. Низкий уровень притязаний.
4. Низкая социально-професиональная мобильность.
11. ДО КАКОГО УРОВНЯ КВАЛИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ ОТНОСЯТСЯ СОТРУДНИКИ, КОТОРЫЕ СПОСОБНЫ РЕАЛИЗОВАТЬ ВСЕ ВОЗМОЖНОСТИ ИТ НА СВОЕМ УЧАСТКЕ РАБОТЫ:
1. Начинающий пользователь.
2. Пользователь.
3. Опытный пользователь.
4. Пользователь-специальностей.
12. ДО КАКОГО УРОВНЯ КВАЛИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ ОТНОСЯТСЯ СОТРУДНИКИ, КОТОРЫЕ УВЕРЕННО ВЛАДЕЮТ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ ОБЩЕГО НАЗНАЧЕНИЯ:
1. Начинающий пользователь.
2. Пользователь.
3. Опытный пользователь.
4. Пользователь-специальностей.
13. ВЫБЕРИТЕ ОДНУ ИЗ ХАРАКТЕРНЫХ ЧЕРТ ПОЛЬЗОВАТЕЛЕЙ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ, КОТОРЫЕ ДЕМОНСТРИРУЮТ ИННОВАЦИОННЫЙ СТИЛЬ ТРУДОВОГО ПОВЕДЕНИЯ:
1. Неосознанное воспроизведения последовательности действий.
2. Создание собственных алгоритмов решения управленческих задач.
3. Трудности с комбинированием отдельных операций.
4. Несистемные базовые знания.
14. ТРЕБОВАНИЯ К КВАЛИФИКАЦИИ КАКОМУ СПЕЦИАЛИСТУ ВКЛЮЧАЮТ НАЛИЧИЕ НАВЫКОВ И ОПЫТА РАБОТЫ ОРГАНИЗАТОРА, УМЕНИЕ УПРАВЛЯТЬ КОЛЛЕКТИВОМ РАЗРАБОТЧИКОВ:
1. IT-менеджер.

2. Программист.
3. Системный аналитик.
4. Системный администратор.

15. ТРЕБОВАНИЯ К КВАЛИФИКАЦИИ КАКОМУ СПЕЦИАЛИСТУ ВКЛЮЧАЮТ НАЛИЧИЕ СОВЕРШЕННЫХ ЗНАНИЙ РАЗЛИЧНЫХ ОПЕРАЦИОННЫХ СИСТЕМ, СЕТЕВОГО ОБОРУДОВАНИЯ, ПРИКЛАДНЫХ ПРОГРАММ:

1. IT-менеджер.
2. Программист.
3. Системный аналитик.
4. Системный администратор.

16. МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ КОНТРОЛЬ ДОСТУПА К АППАРАТУРЕ ЗАКЛЮЧАЕТСЯ В:

1. Контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления.
2. Создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями
3. Разделении информации, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями
4. Том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.
5. Проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

17. МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ РАЗГРАНИЧЕНИЕ И КОНТРОЛЬ ДОСТУПА К ИНФОРМАЦИИ ЗАКЛЮЧАЕТСЯ В:

1. Контроле доступа к внутреннему монтаж, линиям связи и технологическим органам управления
2. Создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями
3. Разделении информации, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями
4. Том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы
5. Проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

18. МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДОСТАВЛЕНИЕ ПРИВИЛЕГИЙ НА ДОСТУП ЗАКЛЮЧАЕТСЯ В:

1. Контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления
2. Создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями
3. Разделении информации, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями
4. Том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы
5. Проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

19. МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ ИДЕНТИФИКАЦИЯ И УСТАНОВЛЕНИЕ ПОДЛИННОСТИ ЗАКЛЮЧАЕТСЯ В:

1.Контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления
2. Создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями

3. Разделении информации, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями
4. том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы
5. Проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.
20. ШИФРОВАНИЕ МЕТОДОМ ПОДСТАНОВКИ:
1. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста
2. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности
3. Шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор
4. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов
5. Замена слов и предложений исходной информации шифрованными.

Примерный перечень вопросов к зачету

1 Информационные системы и документирование информации.
2. Безопасность информационных систем.
3. Государственные информационные системы.
4. Персональные данные о гражданах.
5. Права на доступ к информации. Вычислительные сети и защита информации. Нормативно-правовая база функционирования систем защиты информации. Компьютерные преступления и особенности их расследования.
6. Проблемы защиты информационных систем.
7. Классификация угроз и меры по обеспечению сохранности информационных систем.
8. Классификация рисков и основные задачи обеспечения безопасности информационных систем.
9. Защита локальных сетей и операционных систем.
10. Интеграция систем защиты. Internet в структуре информационно-аналитического обеспечения ИС и угрозы исходящие от использования «электронной почты».
11. Нормативно-правовые документы, регламентирующие отношения в сфере информационной безопасности.
12. Предмет и задачи правового обеспечения информационной безопасности. Законодательство о безопасности и защите информации, его структура и содержание.
13. История создания правового института по охране авторского права.
14. Субъекты авторского права.
15. Права обладателей авторских прав. Авторские и патентные права.
16. Ущерб от незаконного использования авторских и смежных прав. Интеллектуальная собственность.
17. Произведения, пользующиеся охраной.

18. Классификация вирусов. Каналы проникновения вирусов. Способы заражения. Современные антивирусные средства. Средства антивирусной защиты мобильных телефонов и КПК.

19. Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Разграничение доступа.

20. Межсетевые экраны как средство защиты от несанкционированного доступа. Персональные и корпоративные межсетевые экраны.

21. Криптографические средства защиты.

22. Криптографическое преобразование данных.

23. Симметричные и асимметричные методы шифрования.

24. Общая технология шифрования.

25. Технология шифрования речи.

26. Кодирование информации.

27. Электронная цифровая подпись.

28. Организационные требования к системам информационной защиты ИС. Требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению.

29. Требования по применению способов, методов и средств защиты информации. Требования к документированию событий в системе и выявлению несанкционированного доступа.

30. Организация аудита информационной безопасности ИС и предприятия в целом.

7. Учебно-методическое и информационное обеспечение дисциплины

а) Основная литература:

1. Мизюркина Л. А. «Система безопасности информационных ресурсов. Учебно-методическое пособие.(в печати) Пенза: Изд-во ПГУ, 2017 г. – 65 с. (100 шт.).
2. Рабочая программа дисциплины. (50 экз.)
3. Кузнецова, Е. И. Экономическая безопасность и конкурентоспособность. Формирование экономической стратегии государства [Электронный ресурс] : монография / Е. И. Кузнецова. - ЮНИТИ-ДАНА, 2012. - 239 с. - ISBN 978-5-238-02242-0. http://znanium.com/catalog.php.
4. Криворотов, В. В. Экономическая безопасность государства и регионов [Электронный ресурс] : учеб. пособие для студентов вузов, обучающихся по направлению «Экономика» / В. В. Криворотов, А. В. Калина, Н. Д. Эриашвили. - М.: ЮНИТИ-ДАНА, 2012. - 351 с. - ISBN 978-5-238-01947-5. http://znanium.com/catalog.php.
5. Экономическая безопасность: Учебное пособие / Н.В. Манохина, М.В. Попов, Н.П. Колядин, И.Э. Жадан; Под ред. Н.В. Манохиной - М.: НИЦ ИНФРА-М, 2014. - 320 с.: 60x90 1/16. - (Высшее образование: Бакалавриат). (п) ISBN 978-5-16-009002-3, 500 экз. http://znanium.com/catalog.php.

б) Дополнительная литература:

1. Экономическая безопасность современной России в условиях кризиса: Монография / Т.Р. Орехова и др.; Под науч. ред. Т.Р. Ореховой. - М.: НИЦ ИНФРА-М, 2013. - 105 с.: 60x88 1/16. - (Научная мысль). (о) ISBN 978-5-16-009568-4, 500 экз.. http://znanium.com/catalog.php.
2. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования. http://otherreferats.allbest.ru/programming/00068463_0.html.
3. Доктрина информационной безопасности Российской федерации от 09.09.2000г. http://dehack.ru/zak_akt/npa_prezidentarf/doktrina_ib/?p=18.
4. Федеральный закон РФ от 10.01.2002г. N 1-ФЗ «Об электронной цифровой подписи». https://rg.ru/2011/04/08/podpis-dok.html
5. Федеральный Закон РФ от 20.02.1995г. № 24-ФЗ «Об информации, информатизации и защите информации». http://base.garant.ru/10103678/.

в) Профессиональные базы данных и информационные справочные системы

1. Справочно-правовая система «КонсультантПлюс». http://www.consultant.ru/law/ (договор о сотрудничестве от 03.01.2002 г. бессрочный).
2. Справочно-правовая система «Гарант». http://www.aero.garant.ru/newver/ (договор 2012-УЗ02 от 10.01.2012 г. бессрочный)
3. Официальный сайт Евразийской экономической комиссии ЕАЭС. http://www.eurasiancommission.org
2. Официальный сайт Федеральной службы государственной статистики. http://www.gks.ru
3. ЭБС «Консультант студента». http://www.studmedlib.ru
4. ЭБС «Библиокомплектатор». Сформированная вузом покнижная сборка. http://www.bibliocomplectator.ru
5. ЭБС «Библиокомплектатор». Полная коллекция издательства «ИНТУИТ», сформированные вузом покнижная сборка. http://www.bibliocomplectator.ru
6. ЭБС «ZNANIUM.COM». Основная коллекция. http://znanium.com
7. Официальный сайт http://asu.gubkin.ru/ (Методы и средства защиты информации)
8. Официальный сайт http://www.osp.ru/ (Открытие Системы)
9. Официальный сайт http://www.compulog.ru/ (HackZone)
10. Официальный сайт http://www.iso.org/ (Международные стандарты безопасности ISO)
11. Официальный сайт http://www.groteck.ru/security_ru (Информационная безопасность)

8. Материально-техническое обеспечение дисциплины

Для проведения занятий лекционного типа, занятий семинарского типа, лабораторных занятий, выполнения курсовых работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы обучающихся используются помещения, укомплектованные:

- учебной мебелью и мультимедийными системами;
- техническими средствами обучения (компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации (ЭИОС) по индивидуальному логину и паролю обучающегося, к электронному каталогу ПГУ: http://kleopatra.pnzgu.ru., к электронно-библиотечной системе (ЭБС) по подписке ПГУ; сетевым оборудованием, специализированным лицензионным и свободно распространяемым программным обеспечением).

Электронный читальный зал библиотеки ПГУ обеспечивает доступ обучающихся к:

- ЭБС издательства «Лань». Пакет «Математика» (книги издательства «Лань»). Соглашение о сотрудничестве № 12/46 от 19.10.2017;
- ЭБС «Консультант студента». Договор № 471КС/08-2017 от 07.11.2017;
- ЭБС «Библиокомплектатор». Сформированная вузом покнижная сборка. Договор № 3434/17 от 07.12.2017;
- ЭБС «Библиокомплектатор». Полная коллекция издательства «ИНТУИТ», сформированные вузом покнижная сборка. Договор № 3308/17 от 14.12. 2017;
- ЭБС «ZNANIUM.COM». Основная коллекция. Договор № 2450 эбс от 07.12.2017;
- ЭБС «Троицкий мост» (пакет «Таможенное дело + туризм»). Договор № ХП-89/18 от 01.03.2018;
- ЭБС «Библиокомплектатор». Сформированная вузом покнижная сборка. Договор № 3821/18 от 12.03.2018.

Обеспечен удаленный доступ к ЭБС посредством использования обучающимися персональных логинов и паролей.

Лицензионное программное обеспечение представлено: «Microsoft Windows» (Microsoft Imagine Standard) регистрационный номер 00037FFEBACF8FD7, договор № СД-130712001 от 12.07.2013; ПО «Антивирус Касперского», регистрационный номер KL4863RAUFQ договор № СД-130712001 от 12.07.2013; «Антивирус Касперского» 2017-2018 гг. Договор № 030-17-223 от 22 ноября 2017.

Свободно распространяемое ПО: «Mozilla Firefox», «Open Office», «Google Chrome», «Adobe Acrobat Reader», «Яндекс».

Рабочая программа дисциплины «Безопасность информационны персональных данных» составлена в соответствии с требованиями специальности **38.05.01 «Экономическая безопасность», специа «Экономика и организация производства на режимных объектах»**

Программу составила:

1. _____доцент Мизюркина Л. А._____

(Ф.И.О., должность, подпись)

Настоящая программа не может быть воспроизведена ни в какой предварительного письменного разрешения кафедры-ра программы.

Программа одобрена на заседании кафедры «Менеджмент и эко безопасность».

Протокол № 7а от «09» марта 2017 года

Зав. кафедрой

«Менеджмент и экономическая безопасность» Тактарова С. В

Программа одобрена методической комиссией ФЭиУ

Протокол №4 от «16» марта 2017 года

Председатель методической

комиссии ФЭиУ _____Еремина Е. В

Сведения о переутверждении программы на очередной учебный год и регистрации изменений

Учебный год	Решение кафедры (№ протокола, дата, подпись зав. кафедрой)	Внесенные изменения	Номера листов (страниц)		
			заменен-ных	новых	аннулиро-ванных
17-18					
18-19					