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 1.2.22.2 Система безопасности информационных ресурсов

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 **Система безопасности информационных ресурсов** 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 «Система безопасности информационных ресурсов» в структуре специалитета

В соответствии с учебным планом по специальности 38.05.01 «Экономическая безопасность» дисциплина «Система безопасности информационных ресурсов» 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 «Система безопасности информационных ресурсов»

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.

4. Структура и содержание дисциплины ___«Система безопасности информационных ресурсов»_____

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 ресурсы. Защита информации. Основные понятия и определения.** Информационные ресурсы и документирование информации. Безопасность информационных ресурсов. Государственные информационные ресурсы. 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 ресурсы, вредоносных программ и компьютерных вирусов. Проблемы защиты информационных ресурсов.** Изучение источников, рисков и форм атак на информационные ресурсы, вредоносных программ и компьютерных вирусов. Проблемы защиты информационных ресурсов. Классификация угроз и меры по обеспечению сохранности информационных ресурсов. Классификация рисков и основные задачи обеспечения безопасности информационных ресурсов. 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. Законодательные и правовые основы защиты компьютерных информационных ресурсов. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной информации.** Законодательная, нормативно-методическая и научная база систем защиты информации. Требования к содержанию нормативно-методических документов по защите информации. Российское законодательство по защите информационных технологий. Политика безопасности. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в ИС.	2	7-10	8	4	4		8	4	4			7		10	8	9			

4.	**Тема 4.** **Защита информационных ресурсов в компьютерных сетях, антивирусная защита.** Классификация способов защиты информации в компьютерных сетях. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Методы внедрения программных закладок. Компьютерные вирусы как особый класс разрушающих программных воздействия. Защита от разрушающих программных воздействий. Антивирусная защита в сетях. Понятие изолированной программной среды. Рекомендации по защите информации Internet.	2	11-14	8	4	4		8	4	4			11		13	12	14			
5	**Тема 5.** **Требования к системам информационной защиты.** Организационные требования к системам информационной защиты ИС. Требования по обеспечению	2	15-18	6	3	3		6	3	3			15		16	17	18			

	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.																			
	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 ресурсы. Защита информации. Основные понятия и определения.
Информационные ресурсы и документирование информации. Безопасность информационных ресурсов. Государственные информационные ресурсы. 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 ресурсы, вредоносных программ и компьютерных вирусов. Проблемы защиты информационных ресурсов.
Изучение источников, рисков и форм атак на информационные ресурсы, вредоносных программ и компьютерных вирусов. Проблемы защиты информационных ресурсов. Классификация угроз и меры по обеспечению сохранности информационных ресурсов. Классификация рисков и основные задачи обеспечения безопасности информационных ресурсов. 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.
Законодательные и правовые основы защиты компьютерных информационных ресурсов. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной информации.
Законодательная, нормативно-методическая и научная база систем защиты информации. Требования к содержанию нормативно-методических документов по защите информации. Российское законодательство по защите информационных технологий. Политика безопасности. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в ИС.

Тема IV.
Защита информационных ресурсов в компьютерных сетях, антивирусная защита.
Классификация способов защиты информации в компьютерных сетях. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Методы внедрения программных закладок. Компьютерные вирусы как особый класс разрушающих программных воздействия. Защита от разрушающих программных воздействий. Антивирусная защита в сетях. Понятие изолированной программной среды. Рекомендации по защите информации Internet.

Тема V.
Требования к системам информационной защиты. 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 «СБИР» 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 1. Информационные ресурсы. Защита информации. Основные понятия и определения.** Информационные ресурсы и документирование информации. Безопасность информационных ресурсов. 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 ресурсы. Проблемы защиты информационных ресурсов.** Изучение источников, рисков и форм атак на информационные ресурсы, вредоносных	Собеседование, написание рефератов, тесты	Проблемы защиты информационных ресурсов. Классификация угроз и меры по обеспечению сохранности информационных ресурсов. Интеграция	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.	12

	программ и компьютерных вирусов. Проблемы защиты информационных ресурсов. Классификация угроз и меры по обеспечению сохранности информационных ресурсов. Интеграция систем защиты. Internet в структуре информационно-аналитического обеспечения.		систем защиты. Internet в структуре информационно-аналитического обеспечения.	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. Законодательные и правовые основы защиты компьютерных информационных ресурсов. Политика информационной безопасности.** Законодательная, нормативно-методическая и научная база систем защиты информации. Российское законодательство по защите информационных технологий. Политика безопасности.	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
4	**Тема IV. Защита информационных ресурсов в компьютерных сетях, антивирусная защита.** Классификация способов защиты информации в	Собеседование, написание рефератов, тесты, контрольная работа	Понятие разрушающего программного воздействия. Компьютерные вирусы как особый	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.	16

	компьютерных сетях. Понятие разрушающего программного воздействия. Компьютерные вирусы как особый класс разрушающих программных воздействия.. Рекомендации по защите информации Internet.		класс разрушающих программных воздействия.. Рекомендации по защите информации Internet.	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.	
5	**Тема V. Требования к системам информационной защиты.** Организационные требования к системам информационной защиты ИС. Требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению.	Собеседование, написание рефератов, тесты, контрольная работа	Организационные требования к системам информационной защиты ИС. Требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению.	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.	12

6.2. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа студента по темам дисциплины «Система безопасности информационных ресурсов» 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

Примерный 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).

Примерные 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.

Примерный перечень вопросов к зачету

1. Информационные ресурсы и документирование информации.
2. Безопасность информационных ресурсов.
3. Государственные информационные ресурсы.
4. Персональные данные о гражданах. Права на доступ к информации.
5. Вычислительные сети и защита информации.
6. Нормативно-правовая база функционирования систем защиты информации. Компьютерные преступления и особенности их расследования.
7. Изучение источников, рисков и форм атак на информационные ресурсы, вредоносных программ и компьютерных вирусов.
8. Проблемы защиты информационных ресурсов.
9. Классификация угроз и меры по обеспечению сохранности информационных ресурсов.
10. Классификация рисков и основные задачи обеспечения безопасности информационных ресурсов.
11. Защита локальных сетей и операционных систем.
12. Интеграция систем защиты. Internet в структуре информационно-аналитического обеспечения ИС и угрозы исходящие от использования «электронной почты».
13. Законодательная, нормативно-методическая и научная база систем защиты информации.
14. Требования к содержанию нормативно-методических документов по защите информации.
15. Российское законодательство по защите информационных технологий.
16. Политика безопасности. Политика информационной безопасности.
17. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в ИС.
18. Классификация способов защиты информации в компьютерных сетях.
19. Понятие разрушающего программного воздействия.
20. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации.
21. Методы внедрения программных закладок.
22. Компьютерные вирусы как особый класс разрушающих программных воздействия.
23. Защита от разрушающих программных воздействий.
24. Антивирусная защита в сетях.

25. Понятие изолированной программной среды.
26. Рекомендации по защите информации Internet.
27. Организационные требования к системам информационной защиты ИС.
28. Требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению.
29. Требования по применению способов, методов и средств защиты информации.
30. Требования к документированию событий в системе и выявлению несанкционированного доступа.

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 «**Система безопасности информационных ресурсов»** составлена в соответствии с требованиями ФГОС по специальности **38.05.01 «Экономическая безопасность», с**пециализация – **«Экономика и организация производства на режимных объектах»**

Программу составила:

доцент Мизюркина Л. А. _____

(Ф.И.О., должность, подпись)

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

Программа одобрена на заседании кафедры «Менеджмент и экономическая 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					