МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ

УТВЕРЖДАЮ
Декан факультета

_____ Володин В.М.
«___» _____ 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

С1.2.15.2 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 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:

Задачи изучения дисциплины «Система безопасности информационных ресурсов»: 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 стан уметь работать с различными информационными ресурсами и технологиями, обеспечивать соблюдение режима секретности; владеет: 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 ОПОП специалитета

В соответствии с учебным планом по специальности 38.05.01 «Экономическая безопасность» дисциплина «Система безопасности информационных ресурсов» относится к дисциплинам по выбору студентов вариативной части.

Изучению данной дисциплины предшествовали такие дисциплины, как «Информационные технологии в сфере экономической безопасности» (ОК-12, ПК-20), «Информационные системы в экономике» (ОК-12).

Полученные знания и навыки могут применяться при изучении таких дисциплин, как «Статистика» (ОК-12), «Административное право» (ПК-20), «Автоматизированные системы бухгалтерского учета (1С-Бухгалтерия)» (ОК-12) «Режим секретности» (ПК-20), а также при прохождении Практики по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности (ОК-12), Практике по получению профессиональных умений и опыта профессиональной деятельности (ПК-20), Научно-исследовательской работе (ОК-12, ПК-20), Подготовке к сдаче и сдача государственного экзамена (ОК-12, ПК-20), Защите выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (ПК-20).

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,	Знать: различные информационные ресурсы и технологии, основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации.
		Уметь: работать с различными

	систематизации, обработки и передачи информации.	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	Лабораторные занятия	Всего	Подготовка к аудиторным занятиям	Реферат, тесты, контр. работа	Собеседование	Проверка тестов	Проверка контрольн. работ	Проверка реферата
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 защита информации. Нормативно-правовая база функционирования систем защиты информации. Компьютерные преступления и особенности их расследования.	4	1-3	8	4	4	8	4	4	1			2-3
2.	**Тема II.** **Изучение источников, рисков и форм атак на информационные ресурсы, вредоносных программ и компьютерных вирусов. Проблемы защиты информационных ресурсов.**	4	4-6	6	3	3	6	3	3	4	5		6

	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».												
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.	4	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.	4	11-14	8	4	4	8	5	3	11	13		12, 14

5	**Тема 5.** **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.	4	15-17	4	2	2	8	3	5	15	16		17
6	Общая трудоемкость, в часах			34	17	17	38	19	19	Промежуточная аттестация			
										Форма		Семестр	
										Зачет		*4*	

4.2. Содержание дисциплины

Тема I.

Информационные ресурсы. Защита информации. Основные понятия и определения. (ОК-12, ПК -20)

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. (ОК-12, ПК -20)

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. (ОК-12, ПК -20)

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. (ОК-12, ПК -20)

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. (ОК-12, ПК -20)

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

В целях реализации индивидуального подхода к обучению студентов, в т.ч. лиц с ограниченными возможностями здоровья, осуществляющих учебный процесс по собственной траектории в рамках индивидуального рабочего плана, изучение данной дисциплины базируется на предоставлении студентам следующих возможностей: обеспечение внеаудиторной работы со студентами, в том числе, в электронной образовательной среде с использованием соответствующего программного обеспечения, оборудования, дистанционных форм обучения, возможностей использования учебной литературы посредством доступа к электронным библиотечным системам (электронным библиотекам), профессиональным базам данных и информационно-справочным системам, индивидуальных консультаций, в т.ч. на форуме в электронной информационно-образовательной среде, что обеспечено возможностью доступа обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории университета, так и вне ее.

Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

В процессе изучения дисциплины используются современные образовательные технологии, такие как технология обучения, использующая реальную информационную ситуацию, содержащую в себе какую-либо проблему; технологии электронного обучения в сочетании с аудиторной формой, способствующие организации самостоятельной работы студентов, реализуемые посредством:

- лекций: вводных, текущих, обзорных, проблемных, заключительно-обобщающих;
- практических занятий с использованием методов активного обучения, научного познания, проблемно-поисковых методов обучения, реализация которых осуществляется через выполнение аналитических задач, подготовку докладов, презентаций;
- организации самостоятельной работы обучающихся на основе личностно-дифференцированного подхода к выполнению заданий, а также самостоятельной работы в процессе проведения практического занятия, подготовке докладов по выбранной теме.

Лекции – основная форма проведения занятий, как аудиторных, так и занятий в онлайн-режиме.

Практические занятия – важная форма аудиторного обучения, проводимого по определенному кругу вопросов и практических заданий, на основе проведения семинаров, деловых игр и пр.

На лекционных и семинарских занятиях по дисциплине в целях

достижения учебных, воспитательных и научно-исследовательских задач, используются такие интерактивные формы как тренинг, вопросы на сообразительность, доклады по актуальным проблемам СБИР.

На практических занятиях широкое применение находят такие эффективные методы, как тестирование, ответы на вопросы аудитории.

Семинары являются неотъемлемой частью практических занятий учебной дисциплины, так как позволяют закрепить полученные на лекциях и в ходе проведения самостоятельной работы знания, а также способствуют активному участию всех студентов группы в обсуждениях на заданную тему. В целях повышения эффективности проведения семинаров необходимо, прежде всего, провести самостоятельную внеаудиторную работу:

внимательно ознакомиться с вопросами, которые должны быть рассмотрены на занятии;

- определиться с источниками информации;

- изучить различные точки зрения по рассматриваемому вопросу, выявить основные проблемы, динамику и перспективы развития явления или процесса;

- сформировать собственное мнение.

Самостоятельная работа студентов подразумевает работу под руководством преподавателя (проведение консультаций посредством контактной формы или онлайн-формы на форуме, оказание помощи в написании рефератов, докладов, аннотаций, а также научных статей) и индивидуальную работу студента, выполняемую, в том числе, в читальных залах университета, а также посредством ЭБС университета.

Форма проведения текущей и промежуточной аттестации для студентов-лиц с ограниченными возможностями здоровья устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.), что позволяет оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех заявленных компетенций.

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,	Информационные ресурсы и документирование информации. Безопасность информационных ресурсов. Нормативно-правовая база функционирования систем защиты информации.	Основная и дополнительная литература рабочей программы (пункт 7)	**8**
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 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.	Собеседование, написание рефератов, тестирование	Проблемы защиты информационных ресурсов. Классификация угроз и меры по обеспечению сохранности информационных ресурсов. Интеграция систем защиты. Internet в структуре информационно-аналитического обеспечения.	Основная и дополнительная литература рабочей программы (пункт 7)	6

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, тестирование, контрольная работа	Законодательная, нормативно-методическая и научная база систем защиты информации. Российское законодательство по защите информационных технологий. Политика безопасности.	Основная и дополнительная литература рабочей программы (пункт 7)	8
4	**Тема IV.** **Защита информационных ресурсов в компьютерных сетях, антивирусная защита.** Классификация способов защиты информации в компьютерных сетях. Понятие разрушающего программного воздействия. Компьютерные вирусы как особый класс разрушающих программных воздействия.. Рекомендации по защите информации Internet.	Собеседование, написание рефератов, тестирование	Понятие разрушающего программного воздействия. Компьютерные вирусы как особый класс разрушающих программных воздействия.. Рекомендации по защите информации Internet.	Основная и дополнительная литература рабочей программы (пункт 7)	8
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, тестирование	Организационные требования к системам информационной защиты ИС. Требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению.	Основная и дополнительная литература рабочей программы (пункт 7)	8

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 38 часов. 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.

Объем реферата – 20-25 страниц.

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.

6.3. Материалы для проведения текущего контроля знаний и промежуточной аттестации студентов

Контроль освоения компетенций

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1	Текущий контроль (собеседование)	Все темы	ОК-12, ПК -20
2	Текущий контроль (проведение тестирования)	Темы 2,3,4,5.	ОК-12, ПК -20
3	Текущий контроль (проверка рефератов)	1,2,3,4,5.	ОК-12, ПК -20
4	Текущий контроль (проведение контрольной работы)	Тема 3	ОК-12, ПК -20
5	Промежуточная аттестация (проведение зачета)	Все темы	ОК-12, ПК -20

Примерные вопросы для собеседования

Тема 1. Информационные ресурсы. Защита информации. Основные понятия и определения.
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.
Проблемы защиты информационных ресурсов.
Классификация угроз и меры по обеспечению сохранности информационных ресурсов.
Классификация рисков и основные задачи обеспечения безопасности информационных ресурсов.
Тема III. Законодательные и правовые основы защиты компьютерных информационных ресурсов. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной 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.
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.
Рекомендации по защите информации Internet.
Тема V. Требования к системам информационной защиты.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.

Примерные темы рефератов

Тема 1.
Криптографические модели.
Симметричные и ассиметричные криптосистемы для защиты компьютерной информации в ИС.
Вычислительные сети и защита информации.
Компьютерные преступления и особенности их расследования.
Тема II. Проблемы защиты информационных ресурсов.

Международные и Государственные стандарты информационной безопасности и их использование в практической деятельности.
Многоуровневая защита корпоративных сетей.
Режим функционирования межсетевых экранов и их основные компоненты.

Тема III.

Маршрутизаторы.
Шлюзы сетевого уровня.
Усиленная аутентификация.
Применение межсетевых экранов для организации виртуальных корпоративных сетей.
Программные методы защиты информации.
Российское законодательство по защите информационных технологий.

Тема IV.

Защита компьютерных систем от удаленных атак через сеть Intrnet.
Анализ способов защиты информации в компьютерных сетях от разрушающего программного воздействия.
Методы борьбы с компьютерными вирусами и средств защиты информации в Internet.
Угрозы исходящие от использования " электронной почты.
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.

Тема V.

Организация аудита информационной безопасности ИС и предприятия в целом.
Способы, методы и средства защиты информации.
Документирование событий в системе и выявление несанкционированного доступа.

Примерные вопросы для контрольной работы

Вариант 1

Государственные информационные ресурсы.
Классификация рисков и основные задачи обеспечения безопасности информационных ресурсов.
Тесты.

Вариант 2

Российское законодательство по защите информационных технологий.
Классификация способов защиты информации в компьютерных сетях.
Тесты.

Вариант 3

Организационные требования к системам информационной защиты ИС.
Требования по применению способов, методов и средств защиты информации.
Тесты.

Демонстрационный вариант теста

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

2 ДЕЙСТВИЯ, НАПРАВЛЕННЫЕ НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ НЕОПРЕДЕЛЕННЫМ КРУГОМ ЛИЦ ИЛИ ПЕРЕДАЧУ ИНФОРМАЦИИ НЕОПРЕДЕЛЕННОМУ КРУГУ ЛИЦ ЭТО:
Уничтожение информации
Распространение информации
Предоставление информации
Конфиденциальность информации
Доступ к информации
Сервер

3 К СВЕДЕНИЯМ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА, СОГЛАСНО УКАЗУ ПРЕЗИДЕНТА РФ ОТ 6 МАРТА 1997 Г., ОТНОСЯТСЯ:
Информация о распространении программ
Информация о лицензировании программного обеспечения
Информация, размещаемая в газетах, Интернете
Персональные данные
Личная тайна

4 ОТНОШЕНИЯ, СВЯЗАННЫЕ С ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ, РЕГУЛИРУЮТСЯ ЗАКОНОМ…
«Об информации, информационных технологиях»
«О защите информации»
Федеральным законом «О персональных данных»
Федеральным законом «О конфиденциальной информации»
«Об утверждении перечня сведений конфиденциального характера»

5 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:
Авторизация
Аутентификация
Обезличивание
Деперсонализация
Идентификация

Примерные вопросы 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.

7. Учебно-методическое и информационное обеспечение дисциплины

а) Основная литература:

Мизюркина Л. А. «Система безопасности информационных ресурсов. Учебно-методическое пособие.(в печати) Пенза: Изд-во ПГУ, 2017 г. – 65 с. (100 шт.).

Экономическая безопасность: учебник для вузов / Под общ. ред. Л. П. Гончаренко, Ф. В. Акулинина. - М.: Издательство Юрайт, 2018. - 340 с. - URL: https://biblio-online.ru/book/67C9DADE-09C6-41E8-8CB6-AA6D1846E447

б) Дополнительная литература:

Информационные технологии и управление предприятием: Пособие / Баронов В.В., Калянов Г.Н., Попов Ю.И., - 2-е изд., (эл.) - М.:ДМК Пресс, 2018. - 329 с.: - Режим доступа: http://znanium.com/catalog/product/982276

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.

.

в) Профессиональные базы данных и информационные справочные системы

Справочно-правовая система «КонсультантПлюс». http://www.consultant.ru/law/ (договор о сотрудничестве от 03.01.2002 г. бессрочный).

Справочно-правовая система «Гарант». http://www.aero.garant.ru/newver/ (договор 2012-УЗ02 от 10.01.2012 г. бессрочный)

Официальный сайт Федеральной службы государственной статистики. http://www.gks.ru

ЭБС «Консультант студента». http://www.studmedlib.ru

ЭБС «Библиокомплектатор». Сформированная вузом покнижная сборка. http://www.bibliocomplectator.ru

ЭБС «Библиокомплектатор». Полная коллекция издательства «ИНТУИТ», сформированные вузом покнижная сборка. http://www.bibliocomplectator.ru

ЭБС «ZNANIUM.COM». Основная коллекция. http://znanium.com

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 «Консультант студента». Договор № 552КС/09-2018 от 31.10.2018;
- ЭБС «Библиокомплектатор». Полная издательская коллекция издательства «ИНТУИТ»; Две покнижные коллекции. Договор № 4658/18 от 13.12.2018;
- ЭБС издательства «Лань». Пакет «Социально-гуманитарные науки» (книги издательства МГИМО). Договор № ХП-97/19 от 10.04.2019;

- Электронная библиотека диссертаций Российской государственной библиотеки. Договор № 095/04/0107 от 21.06.2019;

- ЭБС «ZNANIUM.COM». Основная коллекция. Договор № 4082 эбс от 11.12.2019;

- ЭБС «Юрайт». Договор № ХП-364/19 от 22.10.2019.

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

Лицензионное ПО:

ПО «Microsoft Windows» (подписка DreamSpark/Microsoft Imagine Standard); регистрационный номер 00037FFEBACF8FD7 договор № СД-130712001 от 12.07.2013 (подписка с 1 сентября 2013 г. до 31 августа 2017 г.), продление Microsoft Imagine Standard KDF-00031 (подписка с 1 сентября 2017 г. до 31 августа 2020 г.)

ПО «Антивирус Касперского» 2016-2017, договор № ХП-567116 от 29.08.2016,
ПО «Антивирус Касперского» 2017-2018, договор № 030-17-223 от 22.11.2017,
ПО «Антивирус Касперского» 2018-2019, договор № 096-18-223 от 17.12.2018,
ПО «Антивирус Касперского» 2019-2020, договор № 075-19-223 от 18 ноября 2019.

Свободно распространяемое ПО: Mozilla Firefox, 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», специализация – «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 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
2018-2019	№1 от 31.08.18	обновлены профессиональные БД и ИСС, договора на ЭБС и лицензионное ПО (п.7, 8)			
2019-2020	№14 от 04.07.19	обновлены список тем рефератов, профессиональные БД и ИСС, договора на ЭБС и лицензионное ПО (п.7, 8)			