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 дисциплины «Безопасность информационных систем и персональных данных» является приобретение знаний о безопасности информационных систем и персональных данных, о методах их защиты. Ознакомление с основными методами и средствами защиты информационных систем и персональных данных, с законодательством и стандартами в данной области, с различными информационными ресурсами и технологиями, применением основных методов, способов и средств получения, хранения, поиска, систематизации, обработки и передачи информации.

Задачи изучения дисциплины «Безопасность информационных систем и персональных данных» - знать методы и средства защиты информационных систем и персональных данных, законодательство и стандарты в данной области, различные информационные ресурсы и технологии; уметь 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.

2. Место дисциплины «Безопасность информационных систем и персональных данных» в структуре ОПОП 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 вариативной части.

Изучению данной дисциплины предшествовали такие дисциплины, как «Информационные системы в экономике» (ОК-12), «Основы права» (ПК-20).

Полученные знания и навыки могут применяться при изучении таких дисциплин, как «Социально-экономическая 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), Преддипломной практике (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 «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,	Знать: виды информационных ресурсов и систем, методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации и персональных данных.

	хранения, поиска, систематизации, обработки и передачи информации.	Уметь: работать с различными информационными ресурсами и системами, использовать методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации и персональных данных.
		Владеть: навыками применения основных методов, способов и средств получения, хранения, поиска, систематизации, обработки, передачи информации и персональных данных.
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 информационных систем и персональных данных, государственной тайны, обеспечивающие соблюдение режима секретности.
		Уметь: соблюдать в профессиональной деятельности требования, установленные нормативными актами в области защиты информационных систем и персональных данных, государственной тайны, обеспечивающие соблюдение режима секретности.
		Владеть: навыками использования нормативных актов в области защиты информационных систем и персональных данных, государственной тайны, обеспечивающие соблюдение режима секретности.

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	Лабораторные занятия	Всего	Подготовка к аудиторным занятиям	Реферат, тесты, контр. работа	Собеседование	Проверка тестов	Проверка контрольн. работ	Проверка реферата
1.	**Тема I. Основные понятия информационных систем и персональных данных.** Информационные системы. Персональные данные о гражданах. Права на доступ к информации. Перечень сведений, доступ к которым не может быть и должен быть ограничен.	2	1-3	8	4	4	8	4	4	1	3		2
2.	**Тема II. Виды рисков информационных систем и персональных данных Проблемы защиты информационных систем и персональных данных.** Изучение источников и рисков информационных систем. Проблемы безопасности информационных систем и персональных данных. Классификация угроз и меры по обеспечению сохранности информационных систем и персональных данных.. Интеграция систем защиты.	2	4-6	6	3	3	6	3	3	4	5		6
3.	**Тема III.**	2	7-	8	4	4	8	4	4	7	10	8	9

	Правовые основы безопасности информационных систем и персональных данных. Нормативно-правовые документы, регламентирующие отношения в сфере безопасности информационных систем и персональных данных. Субъекты авторского права. Авторские и патентные права. Ущерб от незаконного использования авторских и смежных прав. Правовые нормы и стандарты по лицензированию и сертификации.		10										
4.	**Тема 4.** **Программные средства защиты персональной информации.** Классификация вирусов. Каналы проникновения вирусов. Способы заражения. Современные антивирусные средства. Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Персональные и корпоративные межсетевые экраны. Криптографические средства защиты. Общая технология шифрования. Кодирование информации. Электронная цифровая подпись.	2	11-14	8	4	4	8	3	5	11	13		12, 14
5	**Тема 5. Комплексное обеспечение безопасности информационных систем и персональных данных.** Средства контроля доступа. Технические средства защиты. Механические системы защиты информационных систем и персональных данных. Биометрические системы идентификации. Требования по применению способов, методов и средств защиты информационных систем и персональных данных**.**	2	15-18	6	3	3	6	2	4	15	16		17, 18
6	Общая трудоемкость, в часах			36	18	18	36	16	20	Промежуточная аттестация			
										Форма	Семестр		
										Зачет	*2*		

4.2. Содержание дисциплины

4.2.1 Темы лекций

Тема 1. Основные понятия информационных систем и персональных данных. (ОК-12, ПК -20)

Информационные системы. Персональные данные о гражданах. Права на доступ к информации. Перечень сведений, доступ к которым не может быть и должен быть ограничен.

Тема 2. Виды рисков информационных систем и персональных данных Проблемы защиты информационных систем и персональных данных. (ОК-12, ПК -20)

Изучение источников и рисков информационных систем. Проблемы безопасности информационных систем и персональных данных. Классификация угроз и меры по обеспечению сохранности информационных систем и персональных данных.. Интеграция систем защиты.

Тема 3. Правовые основы безопасности информационных систем и персональных данных. (ОК-12, ПК -20)

Нормативно-правовые документы, регламентирующие отношения в сфере безопасности информационных систем и персональных данных. Субъекты авторского права. Авторские и патентные права. Ущерб от незаконного использования авторских и смежных прав.

Правовые нормы и стандарты по лицензированию и сертификации.

Тема 4. Программные средства защиты персональной информации. (ОК-12, ПК -20)

Классификация вирусов. Каналы проникновения вирусов. Способы заражения. Современные антивирусные средства.

Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Персональные и корпоративные межсетевые экраны.

Криптографические средства защиты. Общая технология шифрования. Кодирование информации. Электронная цифровая подпись.

Тема 5. Комплексное обеспечение безопасности информационных систем и персональных данных. (ОК-12, ПК -20)

Средства контроля доступа. Технические средства защиты. Механические системы защиты информационных систем и персональных данных.

Биометрические системы идентификации. Требования по применению способов, методов и средств защиты информационных систем и персональных данных**.**

4.2.2 Темы лабораторных работ

Тема 1. Нормативно-правовая база функционирования защиты информационных систем и персональных данных. (ОК-12, ПК -20)

Требования к содержанию нормативно-правовой базы функционирования защиты информационных систем и персональных данных. Российское законодательство по защите информационных систем и персональных данных. Политика безопасности. Информационные системы и персональные данные, как объект правовых отношений. Использование информационно-телекоммуникационных сетей. Система защиты персональных данных.

Тема 2. Практика обеспечения безопасности информационных систем и персональных данных. (ОК-12, ПК -20)

Изучение источников, рисков и форм атак на информационные системы и персональные данные. Проблемы защиты информационных систем и персональных данных. Классификация угроз и меры по обеспечению сохранности информационных систем и персональных данных. Классификация рисков и основные задачи обеспечения безопасности информационных систем и персональных данных. Защита локальных сетей и операционных систем. Интеграция систем защиты. Internet в структуре информационно-аналитического обеспечения ИС и угрозы исходящие от использования «электронной почты». Рекомендации по предотвращению краж идентификационных данных.

Тема 3. Комплексное решение для защиты информационных систем и персональных данных от внутренних и внешних угроз. (ОК-12, ПК -20)

Персональные данные о гражданах. Права на доступ к информации. Вычислительные сети и защита информации. Антивирусное программное обеспечение. Рекомендации по реализации принципа минимальных привилегий. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Методы внедрения программных закладок. Компьютерные вирусы как особый класс разрушающих программных воздействий.

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 безопасности информационных систем и персональных данных.

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. Основные понятия информационных систем и персональных данных.** Информационные системы. Персональные данные о гражданах. Права на доступ к информации. Перечень сведений, доступ к которым не может быть и должен быть ограничен.	Собеседование, написание рефератов, тестирование	Информационные ресурсы и документирование информации. Безопасность информационных ресурсов. Нормативно-правовая база функционирования систем защиты информации.	Основная лит-ра - (2,3,4,5), Дополнительная –(1-15), в) – (11-26).	**8**
2	**Тема 2. Виды рисков информационных систем и персональных данных Проблемы защиты информационных систем и персональных данных.** Изучение источников и рисков информационных систем. Проблемы безопасности информационных систем и персональных данных. Классификация угроз и меры по обеспечению сохранности информационных систем и персональных данных.. Интеграция систем защиты.	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 лит-ра - (1,2,3,5), Дополнительная –(1-15), в) – (11-26).	6
3	**Тема 3. Правовые основы безопасности информационных систем и персональных данных.** Нормативно-правовые документы, регламентирующие отношения в сфере безопасности информационных систем и персональных данных. Субъекты авторского права. Авторские и патентные права. Ущерб от незаконного использования авторских и смежных прав. Правовые нормы и стандарты по лицензированию и сертификации.	Собеседование, написание рефератов, тестирование, контрольная работа	Законодательная, нормативно-методическая и научная база систем защиты информации. Российское законодательство по защите информационных технологий. Политика безопасности.	Основная лит-ра - (1,2,3,4), Дополнительная –(1-15), в) – (11-26).	8
4	**Тема 4. Программные средства защиты персональной информации.** Классификация вирусов. Каналы проникновения вирусов. Способы заражения. Современные антивирусные средства.	Собеседование, написание рефератов, тестирование	Понятие разрушающего программного воздействия. Компьютерные вирусы как особый класс разрушающих программных воздействия.. Рекомендации по	Основная лит-ра - (1-5), Дополнительная –(1-15), в) – (11-26).	8

	Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Персональные и корпоративные межсетевые экраны. Криптографические средства защиты. Общая технология шифрования. Кодирование информации. Электронная цифровая подпись.		защите информации Internet.		
5	**Тема 5. Комплексное обеспечение безопасности информационных систем и персональных данных.** Средства контроля доступа. Технические средства защиты. Механические системы защиты информационных систем и персональных данных. Биометрические системы идентификации. Требования по применению способов, методов и средств защиты информационных систем и персональных данных**.**	Собеседование, написание рефератов, тестирование	Организационные требования к системам информационной защиты ИС. Требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению.	Основная лит-ра - (1,2,3,4), Дополнительная –(1-15), в) – (11-26).	6

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 36 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.

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 (проверка рефератов)	Все темы	ОК-12, ПК -20
3	Текущий контроль (проверка тестов)	Все темы	ОК-12, ПК -20
4	Текущий контроль (проверка контрольной работы)	Тема 3	ОК-12, ПК -20
5	Промежуточная аттестация (проведение зачета)	Все темы	ОК-12, ПК -20

1 Примерный перечень вопросов для самостоятельного изучения к собеседованию

Тема 1. Основные понятия информационных систем и персональных данных.

Задачи безопасности информационных ресурсов и персональных данных.

Источники, риски и форм атак на информационные ресурсы и персональные данные.

Перечень сведений, доступ к которым не может быть и должен быть ограничен.

Тема 2. Виды рисков информационных систем и персональных данных Проблемы защиты информационных систем и персональных данных.

Классификация угроз и меры по обеспечению сохранности информационных систем и персональных данных.

Изучение средств защиты информационных ресурсов и персональных данных

Влияние человеческого фактора на обеспечение безопасности, информационных ресурсов и персональных данных

Тема 3. Правовые основы безопасности информационных систем и персональных данных.

Идентификация и аутентификация.

Персональные и корпоративные межсетевые экраны.
Субъекты авторского права.
Ущерб от незаконного использования авторских и смежных прав.
Правовые нормы и стандарты по лицензированию и сертификации.

Тема 4. Программные средства защиты персональной информации.

Российское законодательство по защите информационных ресурсов и персональных данных.
Криптографические средства защиты.
Общая технология шифрования.
Кодирование информации.
Электронная цифровая подпись.

Тема 5. Комплексное обеспечение безопасности информационных систем и персональных данных.

Механические системы защиты информационных систем и персональных данных.
Биометрические системы идентификации.
Парольная защита с помощью стандартных системных средств.

2 Примерный перечень тем рефератов

Тема 1.

Перечень сведений, доступ к которым не может быть и должен быть ограничен.
Методы борьбы с компьютерными вирусами и средств защиты информационных ресурсов и персональных данных в Internet.
Угрозы исходящие от использования " электронной почты».

Тема 2.

Проблемы защиты информационных систем и персональных данных.
Влияние человеческого фактора на обеспечение безопасности, информационных ресурсов и персональных данных.
Способы защиты информационных ресурсов и персональных данных в компьютерных сетях от разрушающего программного воздействия.

Тема 3.

Маршрутизаторы.
Шлюзы сетевого уровня.
Усиленная аутентификация.
Правовые нормы и стандарты по лицензированию и сертификации.

Тема 4.

Применение межсетевых экранов для организации защиты информационных ресурсов и персональных данных.
Персональные и корпоративные межсетевые экраны.
Российское законодательство по защите информационных ресурсов и персональных данных.
Общая технология шифрования.

Тема 5.

Кодирование информации.
Электронная цифровая подпись.
Механические системы защиты информационных систем и персональных данных.
Биометрические системы идентификации.
Парольная защита с помощью стандартных системных средств.

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 – 20 - 25 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).

3 Примерный перечень вопросов для контрольной работы

Вариант 1

История создания правового института по охране авторского права.
Интеллектуальная собственность.
Парольная защита с помощью стандартных системных средств.

Идентификация и аутентификация.
Классификация угроз и меры по обеспечению сохранности информационных систем.

Вариант 2

Классификация рисков и основные задачи обеспечения безопасности информационных ресурсов и персональных данных.
Задачи правового обеспечения безопасности информационных ресурсов и персональных данных.
Законодательство о безопасности и защите информации, его структура и содержание.
Парольная защита с помощью стандартных системных средств.
Идентификация и аутентификация.

Вариант 3

Персональные и корпоративные межсетевые экраны.
Криптографические средства защиты.
Общая технология шифрования.
Электронная цифровая подпись.
Комплексное обеспечение безопасности информационных систем и персональных данных.

Вариант 4

Биометрические системы идентификации.
Требования по применению способов, методов и средств защиты информационных систем и персональных данных.
Информационные системы и документирование информации.
Персональные данные о гражданах.
Авторизация.

4 Демонстрационный вариант теста

1 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

2 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»

3 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

4ПРОЦЕССЫ, 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.

5ДЕЙСТВИЯ, 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

6ПО 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.

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. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЕСТЬ ОБЕСПЕЧЕНИЕ…

1. Независимости информации
2. Изменения информации
3. Копирования информации
4. Сохранности информации
5. Преобразования информации

5 Примерный перечень вопросов к зачету

1 Основные понятия информационных систем и персональных данных.
2 Информационные системы.
3 Персональные данные о гражданах.
4 Права на доступ к информации.
5 Перечень сведений, доступ к которым не может быть и должен быть ограничен.
6 Виды рисков информационных систем и персональных данных
7 Проблемы защиты информационных систем и персональных данных.
8 Изучение источников и рисков информационных систем.
9 Проблемы безопасности информационных систем и персональных данных.
10 Классификация угроз и меры по обеспечению сохранности информационных систем и персональных данных.
11 Интеграция систем защиты.
12 Правовые основы безопасности информационных систем и персональных данных.
13 Нормативно-правовые документы, регламентирующие отношения в сфере безопасности информационных систем и персональных данных.
14 Субъекты авторского права.
15 Авторские и патентные права.
16 Ущерб от незаконного использования авторских и смежных прав.
17 Правовые нормы и стандарты по лицензированию и сертификации.
18 Программные средства защиты персональной информации.
19 Классификация вирусов.
20 Каналы проникновения вирусов.
21 Способы заражения.
22 Современные антивирусные средства.
23 Парольная защита с помощью стандартных системных средств.
24 Идентификация и аутентификация.
25 Персональные и корпоративные межсетевые экраны.
26 Криптографические средства защиты.
27 Общая технология шифрования.
28 Кодирование информации.
29 Электронная цифровая подпись.
30 Комплексное обеспечение безопасности информационных систем и персональных данных.
31 Средства контроля доступа.
32 Технические средства защиты.
33 Механические системы защиты информационных систем и персональных данных.
34 Биометрические системы идентификации.
35 Требования по применению способов, методов и средств защиты информационных систем и персональных данных.
36 Информационные системы и документирование информации.
37 Персональные данные о гражданах.
38 Проблемы защиты информационных систем.
39 Межсетевые экраны как средство защиты от несанкционированного доступа.
40 Организация аудита информационной безопасности.

7. Учебно-методическое и информационное обеспечение дисциплины

а) Основная литература:

1. Мизюркина Л. А. «Система безопасности информационных ресурсов. Учебно-методическое пособие. Пенза: Изд-во ПГУ, 2017 г. – 65 с. (100 шт.). http://www.book.lib-i.ru/25ekonomika/296619-1-l-mizyurkina-agamagomedova-tenevaya-ekonomika-metodicheskie-ukazaniya-penza-2015-metodicheskie-ukazaniya-sem.php.
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. https://rusneb.ru/catalog/000199_000009_005028249/.
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://new-books.bid/ekonomicheskaya_bezopasnostj_gosudarstva_i_regionov_uchebnoe_posobie_dlya_studentov_vuzov_obuchayuschihsya_po_napravleniyu_ekonomika_vv_krivorotov_av_kalina_nd_eriashvili/.
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://new-books.bid/ekonomicheskaya_bezopasnostj_uchebnoe_posobie_nv_manohina_mv_popov_np_kolyadin_ie_jadan_pod_red_nv_manohina_visshee_obrazovanie_bakalavriat_grif/
6. Политика безопасности информационных систем и персональных данных. https://sakuramed.ru/politika-informatsionnoy-bezopasnosti-informatsionnykh-sistem-personalnykh-dannykh.

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/.
6. Федеральный Закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» http://www.consultant.ru/document/cons_doc_LAW_61801/.

7. Постановление Правительства РФ от 24 октября 2011 г. № 861 «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)» http://www.consultant.ru/document/cons_doc_LAW_120963/.
8. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» http://www.consultant.ru/document/cons_doc_LAW_137356/
9. Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» http://base.garant.ru/70152982/.
10. Постановление Правительства РФ от 27 сентября 2011 г. № 797 «О взаимодействии между многофункциональными центрами предоставления государственных и муниципальных услуг и федеральными органами исполнительной власти, органами государственных внебюджетных фондов, органами государственной власти субъектов Российской Федерации, органами местного самоуправления» http://base.garant.ru/55172242/
11. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» http://www.consultant.ru/document/cons_doc_LAW_147084/.
12. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» http://www.consultant.ru/document/cons_doc_LAW_146520/.
13. Приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» http://base.garant.ru/187947/.
14. Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» http://base.garant.ru/183628/.
15. Методический документ «Меры защиты информации в государственных информационных системах» утвержденный ФСТЭК России 11 февраля 2014 г. https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodiche.
16. «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных»,

утвержденные ФСБ России 21 февраля 2008 г. № 149/6/6-622 http://www.consultant.ru/document/cons_doc_LAW_126991/.

17. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённая Заместителем директора ФСТЭК России 15 февраля 2008 г. http://www.consultant.ru/document/cons_doc_LAW_99662/.

18. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённая Заместителем директора ФСТЭК России 15 февраля 2008 г. http://saratov.gov.ru/gov/docs/metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh.

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

4. Официальный сайт ФТС России www.customs.ru.

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

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

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

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

9. 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 «Безопасность информационных систем и персональных данных» составлена в соответствии с требованиями ФГОС по специальности **38.05.01 «Экономическая безопасность», с**пециализация – **«Экономика и организация производства на режимных объектах»**

Программу составила:

1. _____доцент Мизюркина Л. А._____

(Ф.И.О., должность, подпись)

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 профессиональные БД и ИСС, договора на ЭБС и лицензионное ПО (п.7, 8)			