МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СЕРВИСА»
(ФГБОУ ВО «ПВГУС»)

Кафедра «Прикладная информатика в экономике»

РАБОЧАЯ УЧЕБНАЯ ПРОГРАММА

по дисциплине «Организация и управление службой ЗИ»
для студентов направления подготовки 10.03.01 «Информационная безопасность»
направленности (профиля) «Организация и технология защиты информации»

Тольятти 2018 г.

Рабочая учебная программа по дисциплине «Организация и управление службой ЗИ» включена в основную профессиональную образовательную программу направленности (профиля) «Организация и технология защиты информации» направления подготовки 10.03.01 «Информационная безопасность» решением Президиума Ученого совета (Протокол № 4 от 28.06.2018 г.).

Начальник учебно-методического отдела _____ Н.М. Шемендюк

28.06.2018 г.

Рабочая учебная программа по дисциплине «Организация и управление службой ЗИ» разработана в соответствии с Федеральным государственным образовательным стандартом направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Минобрнауки РФ от 1 декабря 2016 г. N 1515.

Составили Малышева Е.Ю., Бобровский С.М.

Согласовано Директор научной библиотеки _____ В.Н.Еремина

Согласовано Начальник управления информатизации _____ В.В.Обухов

Рабочая программа утверждена на заседании кафедры
«Прикладная информатика в экономике»
Протокол № 12 от «22» июня 2018г.

И.о. заведующего кафедрой _____ д.э.н., профессор Бердников В.А.
(подпись) (ученая степень, звание, Ф.И.О.)

Согласовано начальник учебно-методического отдела _____ Н.М.Шемендюк

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

1.1. Цели освоения дисциплины

изучение организационной деятельности служб защиты информации предприятий и организаций, рассмотрение различных правовых аспектов деятельности службы защиты информации, принципов, методов и технологии управления службой защиты информации.

1.2. В соответствии с видами профессиональной деятельности, на которые ориентирована образовательная программа указанного направления подготовки, содержание дисциплины позволит обучающимся решать следующие профессиональные задачи:

эксплуатационная деятельность:

участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;

проектно-технологическая деятельность:

сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

проведение предварительного технико-экономического обоснования проектных расчетов;

организационно-управленческая деятельность:

осуществление организационно-правового обеспечения информационной безопасности объекта защиты;

организация работы малых коллективов исполнителей;

участие в совершенствовании системы управления информационной безопасностью;

изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;

контроль эффективности реализации политики информационной безопасности объекта защиты.

1.3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины у обучающихся формируются следующие компетенции:

Код компетенции	Наименование компетенции
ПК-5	Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации.
ПК-7	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.
ПК-13	Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.
ПК-14	Способность организовывать работу малого коллектива исполнителей в профессиональной деятельности.
ПК-15	Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

1.4. Перечень планируемых результатов обучения по дисциплине

Результаты освоения дисциплины	Технологии формирования компетенции по указанным результатам	Средства и технологии оценки по указанным результатам
***Знает*:** методы организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5); методы проведения технико-экономического обоснования проектных решений; подсистем и средств обеспечения информационной безопасности (ПК-7); методы, организации комплекса мер по обеспечению информационной безопасности (ПК-13); методики организации работы малого коллектива исполнителей в профессиональной деятельности (ПК-14); методы организации технологического процесса защиты информации ограниченного доступа (ПК-15).	Лекции	Собеседование
***Умеет*:** применять методы организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5); проводить технико-экономическое обоснование проектных решений;	Практические работы	Защита практических работ

подсистем и средств обеспечения информационной безопасности (ПК-7); использовать методы организации комплекса мер по обеспечению информационной безопасности (ПК-13); применять методики организации работы малого коллектива исполнителей в профессиональной деятельности (ПК-14); использовать методы организации технологического процесса защиты информации ограниченного доступа (ПК-15).		
***Имеет практический опыт*:** организации и сопровождения аттестации объекта информатизации по требованиям безопасности информации (ПК-5); проведения технико-экономического обоснования проектных решений; подсистем и средств обеспечения информационной безопасности (ПК-7); организации комплекса мер по обеспечению информационной безопасности (ПК-13); организации работы малого коллектива исполнителей в профессиональной деятельности (ПК-14); использования методов организации технологического процесса защиты	Решение разноуровневых и проблемных задач	Защита практических работ

информации ограниченного доступа (ПК-15).		

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к вариативной части.
Её освоение осуществляется: в 8 семестре.

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Код компетенции(й)
	Предшествующие дисциплины	
1.	Основы информационной безопасности	ОК-5, ОПК-7
2.	Экономика защиты информации	ПК-9
3.	Организационное и правовое обеспечение информационной безопасности	ОК-4, ОПК-5

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу

Распределение фонда времени по семестрам и видам занятий

Виды занятий	очная форма обучения	очно-заочная форма обучения	заочная форма обучения
Итого часов Зачетных единиц	180 ч. 5 з.е.	180 ч. 5 з.е.	- -
Лекции (час)	32 ч.	8 ч.	-
Практические (семинарские) занятия (час)	42 ч.	10 ч.	-
Лабораторные работы (час)	-	-	-
Самостоятельная работа (час)	79 ч.	153 ч.	-
Курсовая работа (+,-)	+	+	-
Контрольная работа (+,-)	-	-	-
Экзамен, семестр/час.	8 семестр/ 27 ч.	8 семестр/ 9 ч.	-
Дифференцированный зачет, семестр	-	-	-
Контрольная работа, семестр	-	-	-

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Содержание дисциплины

№ п/п	Раздел дисциплины	Виды учебных занятий, включая самостоятельную работу студентов и трудоемкость (в академических часах)				Средства и технологии оценки
		Лекции, час	Практические занятия, час	Лабораторные работы, час	Самостоятельная работа, час	
1.	Тема 1. Введение. Основные понятия. Вопросы для изучения Введение. Структура и содержание дисциплины, задачи, цели изучения. Основные понятия, связанные с защитой информации. Проблемы организации процессов управления в службе защиты информации/	2/1/-	0/0/-	-/-/-	9/15/-	Устный опрос
2.	Тема 2. Место и роль службы защиты информации в системе защиты информации. Вопросы для изучения Понятие о системном подходе к формированию СЗИ. Определение места, роли СЗИ в общей системе и системе безопасности; задачи и функции службы защиты информации/	4/1/-	0/0/-	-/-/-	14/26/-	Устный опрос
3.	Тема 3. Структура и штаты службы защиты информации. Вопросы для изучения Структура и штаты службы защиты информации; Особенности формирования штатов СЗИ, как одного из видов ресурсов; подбор, расстановка и особенности обучения сотрудников службы защиты информации	6/2/-	10/2/-	-/-/-	14/28/-	Устный опрос, защита практических работ
4.	Тема 4. Организационные основы и принципы деятельности службы защиты информации. Вопросы для изучения	8/2/-	10/2/-	-/-/-	14/28/-	Устный опрос, защита практических работ

	Основные подходы к организации и управлению СЗИ: управление сотрудниками, реализация направлений деятельности.					
5.	Тема 5. Организация труда сотрудников службы защиты информации. Вопросы для изучения Особенности организации труда сотрудников, приобретение навыков разработки функциональных обязанностей.	6/1/-	10/2/-	-/-/-	14/28/-	Устный опрос, защита практических работ
6.	Тема 6. Принципы, методы и технология управления службой защиты информации. Вопросы для изучения Особенности, принципы, методы и технология управления СЗИ в системах защиты информации, Модели управления СЗИ.	6/1/-	12/4/-	-/-/-	14/28/-	Устный опрос, защита практических работ
	Промежуточная аттестация по дисциплине	32/8/-	42/10/-	-/-/-	79/153/-	Экзамен

Примечание:
-/-/-, объем часов соответственно для очной, очно-заочной

4.2. Содержание практических работ

№	Наименование практических работ	Обьем часов	Наименование темы дисциплины
1.	*Практическая работа 1:* Разработка организационно-правовых аспектов деятельности службы защиты информации.	10/2/-	Тема 3. Структура и штаты службы защиты информации.
2.	*Практическая работа 2:* Разработка организационно-правовых аспектов деятельности службы защиты информации.	4/2/-	Тема 4. Организационные основы и принципы деятельности службы защиты информации.
3.	*Практическая работа 3:* Разработка организационной структуры службы защиты информации.	6/-/-	Тема 4. Организационные основы и принципы деятельности службы защиты информации.
4.	*Практическая работа 4:* Разработка модели системы защиты информации для службы защиты информации.	4/2/-	Тема 5. Организация труда сотрудников службы защиты информации.
5.	*Практическая работа 5:* Оценка производительности труда по результатам оптимизации процессов в службе защиты информации.	6/-/-	Тема 5. Организация труда сотрудников службы защиты информации.
6.	*Практическая работа 6:* Экспертная оценка мероприятий по защите информации в службе защиты	6/2/-	Тема 6. Принципы, методы и технология управления службой защиты информации.

	информации.		
7.	*Практическая работа 7:* Мониторинг и корректировка внутренних мер по защите информации в службе защиты информации.	6/2/-	Тема 6. Принципы, методы и технология управления службой защиты информации.
	Итого	42/10/-	

Примечание:
-/-/-, объем часов соответственно для очной, очно-заочной

5. Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине

Технологическая карта самостоятельной работы студента

Код реализуемой компетенции	Вид деятельности студентов (задания на самостоятельную работу)	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Обьем часов
ПК-5, ПК-7, ПК-13, ПК-14, ПК-15	Работа с литературой	Конспект	Собеседование	40/80/-
ПК-5, ПК-7, ПК-13, ПК-14, ПК-15	Ответы на контрольные вопросы	Конспект	Тест	20/36/-
ПК-5, ПК-7, ПК-13, ПК-14, ПК-15	Подготовка доклада на конференцию	Доклад	Опубликование тезисов доклада	19/37/-
			Итого	79/153/-

Рекомендуемая литература: 1, 2, 3, 4, 5, 6, 7.

Содержание заданий для самостоятельной работы

Вопросы для самоконтроля

1. Роль и место организационной защиты информации в системе комплексной защиты информации.
2. Основные термины и определения в области организационной защиты информации.
3. Задачи и функции, возлагаемые на руководителей и должностных лиц предприятия в решении задач по организационной защите информации.
4. Основные принципы и условия организационной защиты информации на предприятии.
5. Средства, используемые для обеспечения защиты конфиденциальной информации.
6. Стратегия обеспечения безопасности в организации. Подходы к построению Службы ЗИ
7. Организационно-планирующие документы по ЗИ, разрабатываемые в организации (на предприятии)
8. Положение «о подразделении по ЗИ организации». Назначение положения и модели его составления. Разработка и оформление положения
9. Должностные инструкции, сотрудника подразделения по ЗИ организации. Организация разработки должностной инструкции по ЗИ. Требования к проекту должностной инструкции сотрудника ЗИ. Особенности разработки нетипичных должностных инструкций
10. Понятия об организационной структуре управления подразделением по ЗИ. Требования, предъявляемые к ОСУ подразделением по ЗИ. Виды ОСУ подразделения по ЗИ
11. Система защиты государственной тайны на предприятии. Ее составные элементы.

12. Моделирование системы защиты информации (СЗИ). Виды моделей СЗИ. Архитектурное построение СЗИ.
13. Принципы отнесения сведений к государственной тайне и их засекречивания.
14. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию.
15. Степени секретности сведений, составляющих государственную тайну, и грифы секретности их носителей.
16. Порядок отнесения сведений к государственной тайне.
17. Порядок засекречивания сведений и их носителей. Реквизиты носителей сведений, составляющих государственную тайну.
18. Перечень сведений, отнесенных к государственной тайне, порядок и особенности его формирования. Полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты.
19. Основания и порядок рассекречивания сведений, составляющих государственную тайну, и их носителей.
20. Функции в области рассекречивания сведений, составляющих государственную тайну, возлагаемые на Межведомственную комиссию по защите государственной тайны.
21. Порядок исполнения запросов граждан, предприятий, учреждений, организаций и органов государственной власти Российской Федерации о рассекречивании сведений, составляющих государственную тайну.
22. Основные положения допуска должностных лиц и граждан к сведениям, составляющим государственную тайну.
23. Порядок оформления (переоформления) допуска должностных лиц и граждан к государственной тайне.
24. Формы допуска. Особый порядок допуска к государственной тайне. Условия прекращения допуска к государственной тайне.
25. Обязанности лиц, допущенных к сведениям, составляющим государственную тайну. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне.
26. Основания для отказа должностному лицу и гражданину в допуске к государственной тайне.
27. Понятие внутриобъектового режима на предприятии. Основные цели, подходы и принципы организации внутриобъектового режима.
28. Роль и место внутриобъектового режима на предприятии в общей системе защиты конфиденциальной информации.
29. Силы и средства, используемые при организации внутриобъектового режима на предприятии.
30. Цели и задачи пропускного режима на предприятии. Основные понятия, используемые при его организации и обеспечении.
31. Принципы организации пропускного режима на предприятии. Основные элементы системы организации пропускного режима, используемые силы и средства.
32. Особенности организации пропускного режима на предприятиях, имеющих особый статус. Ответственность за нарушение пропускного режима.
33. Планирование мероприятий по защите сведений конфиденциального характера при подготовке совещаний (заседаний, конференций, симпозиумов), в ходе которых предполагается обсуждение вопросов, содержащих такие сведения.
34. Работа по исключению утечки сведений и информации конфиденциального характера.
35. Цели и задачи службы охраны предприятий, выполняющих работы с конфиденциальной информацией.
36. Основные способы организации и осуществления охраны предприятий, выполняющих работы с конфиденциальной информацией.
37. Основные направления деятельности должностных лиц предприятия по организации его охраны. Особенности охраны предприятий, имеющий особый статус.

38. Особенности организации охраны предприятий, выполняющих работы с конфиденциальной информацией, подразделениями вневедомственной охраны при органах внутренних дел МВД России и частными предприятиями, выполняющими функции защиты информации.
39. Основные положения организации защиты конфиденциальной информации в ходе подготовки и командирования сотрудников предприятия (организации) в органы государственной власти, на другие предприятия и в организации.
40. Порядок и последовательность оформления необходимых документов о командировании сотрудников предприятия в органы государственной власти, на другие предприятия (в организации).
41. Какие типовые организационные структуры можно выделить в рамках государственной системы защиты информации?
42. Какие услуги организационно-технологического характера предлагаются специализированными предприятиями в системе защиты информации?
43. Какие основные функции выполняют сертификационно-испытательные центры и лаборатории в области обеспечения и защиты информации?
44. Оптимизация структуры управления службы защиты информации.
45. Мероприятия по контролю и мониторингу направлений деятельности службы защиты информации.
46. Оценка рисков при функционировании службы защиты информации.
47. Оценка эффективности работы службы защиты информации.
48. Технология управления службы защиты информации.
49. Порядок оформления документов, необходимых для получения лицензий, сертификатов, аттестатов в области защиты информации.
50. Разработка и применение методов локальной и комплексной автоматизации процессов деятельности службы защиты информации.
51. Интеграция службы защиты информации с подсистемами, обеспечивающими различные направления безопасности в организации.

6. Методические указания для обучающихся по освоению дисциплины

Инновационные образовательные технологии

Вид образовательных технологий, средств передачи знаний, формирования умений и практического опыта	№ темы / тема лекции	№ практического (семинарского) занятия/наименование темы	№ лабораторной работы / цель
Слайд-лекция	слайд-лекции по темам 1, 2: «Введение. Основные понятия, связанные с функционированием службы защиты информации», «Место и роль службы защиты информации в системе защиты информации; задачи и функции службы».		

В начале семестра студентам необходимо ознакомиться с технологической картой дисциплины, выяснить, какие результаты освоения дисциплины заявлены (знания, умения, практический опыт). Для успешного освоения дисциплины студентам необходимо выполнить задания, предусмотренные рабочей учебной программой дисциплины и пройти контрольные точки в сроки, указанные в технологической карте (раздел 11). От качества и полноты их выполнения будет зависеть уровень сформированности компетенций и оценка текущей успеваемости по дисциплине. По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации. Списки учебных пособий, научных трудов, которые студентам следует прочесть и законспектировать, темы практических работ, вопросы к экзамену и другие необходимые материалы указаны в разработанном для данной дисциплины учебно-методическом пособии.

Основной формой освоения дисциплины является контактная работа с преподавателем – лекции, Практические работы, консультации, в том числе проводимые с применением дистанционных технологий.

По дисциплине часть тем изучается студентами самостоятельно. Самостоятельная работа предусматривает подготовку к аудиторным занятиям, выполнение заданий, подготовку к промежуточной аттестации (зачету, экзамену).

На лекционных и практических занятиях вырабатываются навыки и умения обучающихся по применению полученных знаний в конкретных ситуациях, связанных с будущей профессиональной деятельностью. По окончании изучения дисциплины проводится промежуточная аттестация (экзамен).

Регулярное посещение аудиторных занятий не только способствует успешному овладению знаниями, но и помогает организовать время, т.к. все виды учебных занятий распределены в семестре планомерно, с учетом необходимых временных затрат.

6.1. Методические указания для обучающихся по освоению дисциплины на практических работах

Практические работы

№	Наименование практической работы	Задания по практической работе
1.	*Практическая работа 1:* Разработка организационно-правовых аспектов деятельности службы защиты информации.	Ознакомиться и изучить основные принципы разработки организационно-правовых аспектов деятельности службы защиты информации.
2.	*Практическая работа 2:* Разработка организационно-правовых аспектов деятельности службы защиты информации.	Ознакомиться и изучить основные принципы разработки организационно-правовых аспектов деятельности службы защиты информации.
3.	*Практическая работа 3:* Разработка организационной структуры службы защиты информации.	Ознакомиться с принципами системного подхода при создании организационной структуры. Разработать организационную систему управления службой защиты информации в рамках общей структуры организации.
4.	*Практическая работа 4:* Разработка модели системы защиты информации для службы защиты информации.	Разработать модель системы защиты информации на основе модели политики безопасности для конкретной организации.
5.	*Практическая работа 5:* Оценка производительности труда по результатам оптимизации процессов в службе защиты информации.	Провести оценку производительности труда персонала службы защиты информации в соответствие с предложенной методикой.
6.	*Практическая работа 6:* Экспертная оценка мероприятий по защите	Проводить экспертную оценку мероприятий по защите информации в службе защиты

	информации в службе защиты информации.	информации.
7.	*Практическая работа 7:* Мониторинг и корректировка внутренних мер по защите информации в службе защиты информации.	Разработать мероприятия по мониторингу работы службы защиты информации.

Практические работы обеспечивают: демонстрацию применения теоретических знаний на практике, закрепление и углубление теоретических знаний, контроль знаний и умений в формулировании выводов, развитие интереса к изучаемой дисциплине.

Применение практических работ позволяет вовлечь в активную работу всех обучающихся группы и сформировать интерес к изучению дисциплины.

Самостоятельный поиск ответов на поставленные вопросы и задачи в ходе лабораторной работы приобретают особую значимость в восприятии, понимании содержания дисциплины.

Изученный на лекциях материал лучше усваивается, Практические работы демонстрируют практическое их применение.

6.2. Методические указания для выполнения контрольных работ

Контрольная работа по дисциплине учебным планом не предусмотрена.

6.3. Методические указания для выполнения курсовых работ

Цели, задачи и основное содержание курсовой работы.

При освоении дисциплины «Организация и управление службой защиты информации» важнейшей формой контроля самостоятельной работы студента является выполнение и защита курсовой работы.

Цель написания курсовой работы: научиться применять полученные теоретические знания для решения конкретных задач. Теоретические знания – это изученный понятийный аппарат дисциплины, методы системного анализа, функционального моделирования, методики разработки организационно-правового, технического, программно-аппаратного обеспечения функционирования службы защиты информации. Конкретные задачи, поставленные перед автором курсовой работы, зависят от темы.

Задачи написания курсовой работы сводятся к тому, что студент должен научиться:

− логично, последовательно, с соблюдением требований научного стиля излагать материал курсовой работы;

− обобщать сведения, полученные из учебной, научной литературы, периодических изданий и официальных Интернет-ресурсов;

− выбирать методы исследования и анализа систем защиты информации в рамках деятельности конкретной организации в целом в соответствии с типом системы определять методику анализа;

− проводить анализ целей и функций, задач управления службой защиты информации, в том числе определять цель системы и строить структуры целей и функций;

− строить математические, графовые модели структуры управления СЗИ;

− использовать методы аудита и мониторинга СЗИ, разработки критериев оценки деятельности СЗИ, а также методов экспертной оценки;

− анализировать процессы и структуры управления системами защиты информации и вносить предложения по их совершенствованию.

Таким образом, в ходе выполнения курсовой работы студент приобретает опыт выработки методики формирования организационно-правового обеспечения службы защиты информации на основе системного анализа с использованием возможностей вычислительной техники и программного обеспечения, а также изучает один из методов исследования и моделирования организационно-управленческих аспектов службы защиты информации.

Структура и объем курсовой работы.

Общий объем курсовой работы – 30-35 страниц. Курсовая работа должна иметь обязательные составные части, располагаемые в последовательности:

- титульный лист;
- содержание;
- введение;
- основная часть;
- заключение;
- библиографический список;
- приложения.

Дополнительно прилагаются задание на курсовую работу и бланк рецензии. Они размещаются после титульного листа и не нумеруются.

Титульный лист оформляется по установленной форме.

Задание на курсовую работу выдается руководителем по установленной форме и утверждается заведующим кафедрой.

Рецензия. Бланк рецензии оформляется по установленной форме. Рецензию пишет руководитель после представления курсовой работы на проверку.

Содержание (1-2 страницы). Содержание отражает последовательность составных частей курсовой работы: введение, названия глав и параграфов, заключение, библиографический список, приложения. В содержании указывается название пункта и номер страницы, с которой начинается его изложение. При этом главы и параграфы нумеруются арабскими цифрами, остальные пункты не нумеруются.

Введение (3-4 страницы). Содержит обоснование актуальности темы, постановку проблемы и отражение состояния вопроса. Обязательно четко выделить цель и задачи курсовой работы. Формулировка цели работы является логическим продолжением сформулированной проблемы, актуальности темы и должна быть созвучна наименованию темы. Обычно цель формулируется с помощью отглагольных существительных (получение, анализ, разработка и т.п.) и должна ёмко отражать то, что собирается достичь исследователь в ходе выполнения работы.

Для достижения поставленной цели необходимо сформулировать конкретные задачи курсовой работы. Это делается в форме перечисления (изучить..., установить..., выявить..., разработать..., проанализировать..., сделать выводы… и т. д.). Поскольку из формулировок задач исследования составляются обычно заголовки параграфов работы, то задачи рекомендуется формулировать более тщательно.

Также необходимо выделить объект исследования (например, указывается наименование предприятия) и кратко указать материалы и методы, используемые в процессе исследования.

Основная часть (22-25 страниц). Основная часть состоит из двух глав. В первой главе излагаются теоретические аспекты темы, проводятся анализ предприятия или организации с учетом особенностей организации системы защиты информации, во второй главе – преимущественно разработка решений поставленной проблемы, выбор оптимального варианта решения и формулирование предложений по его внедрению.

Заключение (2-3 страницы). В заключении приводятся самостоятельные выводы о проделанной работе и полученных результатах исследования. Выводы должны быть краткими и аргументированными, рекомендации – конкретными и сопровождаться оценкой от их внедрения в практику.

Библиографический список. Каждая позиция в библиографическом списке должна быть оформлена в соответствии с требованиями ГОСТ 7.1-2003 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления». При оформлении курсовой работы используется алфавитный способ группировки библиографических описаний.

Требования к составу списка:

- общее количество источников - не менее 20;
- статей из периодических изданий, сборников конференций – не менее пяти.

Рекомендуется использовать нормативно-правовые документы, если они соответствуют теме курсовой работы и необходимы для достижения поставленных задач. Допускается включать в библиографический список электронные издания, Интернет-ресурсы, если они содержат статистическую, аналитическую, обзорную информацию, являются официальными сайтами организаций, предприятий, учреждений, а не представляют собой базы рефератов, курсовых и дипломных работ.

Приложения. Содержат дополнительный иллюстративный, табличный материал, документы (или их фрагменты), описание порядка реализации методов системного анализа, не вошедшие в основную часть работы. Объем приложений не ограничен и не включается в объем курсовой работы (30-35 страниц). Содержание приложений должно быть оправдано

темой, целью и задачами исследования.

Примерный перечень тем курсовых работ

1. Разработка организационно-правовых аспектов деятельности системы комплексной защиты информации (на примере конкретной организации).
2. Разработка системы учета и контроля поступивших конфиденциальных документов в комплексной системе защиты информации.
3. Характеристика организационных и технических мер в комплексной службе защиты информации в государственных структурах.
4. Разработка концептуальных основ функционирования систем безопасности предпринимательской деятельности (на примере проектирования конкретной системы).
5. Разработка политики безопасности и принципов управления службой информационной безопасности предприятия.
6. Теория и практика организации защиты информационных систем.
7. Разработка службы информационной безопасности для венчурного фонда.
8. Разработка интегрированной системы защиты в рамках службы защиты информации (на примере конкретной организации).
9. Модернизация службы защиты информации (на примере конкретной организации).
10. Разработка политики безопасности при эксплуатации и сопровождении ИС с целью обеспечения сохранности конфиденциальной информации.

Исходные данные для выполнения курсовой работы

Приступая к выполнению курсовой работы, студент руководствуется индивидуальным заданием, материалами, собранными на предприятии, данными, опубликованными в научной литературе, официальных отчетах, обзорах, релизах. В списке рекомендуемой литературы приведены книги и источники, которые могут быть полезны при написании курсовых работ практически по всем темам. База учебной, научной литературы, официальных изданий должна быть расширена студентом индивидуально, в зависимости от тематики работы.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (экзамен)

Фонды оценочных средств, позволяющие оценить уровень сформированности компетенций и результаты освоения дисциплины, представлены следующими компонентами:

Код оцениваемой компетенции (или) её части	Тип контроля	Вид контроля	Количество элементов, шт.
ПК-5, ПК-7, ПК-13, ПК-14, ПК-15	*текущий*	*устный опрос*	*1-46*
ПК-5, ПК-7, ПК-13, ПК-14, ПК-15	*промежуточный*	*компьютерный тест*	*1-100*

7.1. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

Результаты освоения дисциплины	Оценочные средства
***Знает*:** методы организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5); методы проведения технико-экономического обоснования проектных решений; подсистем и средств обеспечения информационной безопасности (ПК-7); методы, организации комплекса мер по обеспечению информационной безопасности (ПК-13); методики организации работы малого коллектива исполнителей в профессиональной деятельности (ПК-14); методы организации технологического процесса защиты информации ограниченного доступа (ПК-15).	1. Меры защиты информационной безопасности направлены на защиту от: а) нанесения неприемлемого ущерба; б) нанесения любого ущерба; в) вандализма. 2. Что из перечисленного не относится к числу основных аспектов информационной безопасности? а) доступность; б) целостность; в) конфиденциальность; г) правдивое отражение действительности. 3. Что такое защита информации? а) защита от несанкционированного доступа к информации; б) выпуск бронированных упаковок для дисков; в) комплекс мероприятий, направленных на обеспечение информационной безопасности. 4. Что понимается под информационной безопасностью? а) защита здоровья персонала; б) защита от нанесения неприемлемого ущерба субъектам информационных отношений; в) обеспечение информационной независимости России. 5. Самыми опасными угрозами являются: а) непреднамеренные ошибки штатных сотрудников; б) вирусные инфекции; в) атаки хакеров. 6. Дублирование сообщений является угрозой: а) доступности; б) конфиденциальности; в) целостности. 7. Агрессивное потребление ресурсов является угрозой: а) доступности; б) конфиденциальности; в) целостности. 8. Согласно Закону “Об информации, информатизации и

	защите информации", персональные данные – это: а) сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность; б) данные, хранящиеся в персональном компьютере; в) данные, находящиеся в чьей-либо персональной собственности. 9. Действия Закона "О лицензировании отдельных видов деятельности" не распространяется на: а) деятельность по технической защите конфиденциальной информации; б) образовательную деятельность в области защиты информации; в) предоставление услуг в области шифрования информации. 10. Главная цель мер по защите информации, предпринимаемых на административном уровне: а) сформировать программу безопасности и обеспечить её выполнение; б) выполнить положения действующего законодательства; в) отчитаться перед вышестоящими инстанциями. 11. В число целей политики безопасности верхнего уровня входит: а) решение сформировать или пересмотреть комплексную программу безопасности; б) обеспечение базы для соблюдения законов и правил; в) обеспечение конфиденциальности почтовых сообщений. 12. В число этапов жизненного цикла информационного сервиса входят: а) закупка; б) продажа; в) выведение из эксплуатации.
***Умеет*:** применять методы организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5); проводить технико-экономическое обоснование проектных решений; подсистем и средств обеспечения информационной безопасности (ПК-7); использовать методы организации комплекса мер по обеспечению информационной безопасности (ПК-13); применять методики организации работы малого коллектива исполнителей в профессиональной	13. Политика безопасности: а) фиксирует правила разграничения доступа; б) отражает подход организации к защите своих информационных активов; в) описывает способы защиты руководства организации. 14. В число этапов процесса планирования восстановительных работ после реализации угроз входят: а) выявление критически важных функций организации; б) определения перечня возможных аварий; в) проведение тестовых аварий. 15. В число принципов физической защиты входят: а) беспощадный отпор; б) непрерывность защиты в пространстве и времени; в) минимизация защитных средств. 16. Мониторинг, протоколирование и аудит могут использоваться для: а) предупреждения нарушений ИБ; б) обнаружение нарушений; в) восстановление режима ИБ. 17. В число основных принципов архитектурной безопасности входят: а) применение наиболее передовых технических решений;

деятельности (ПК-14); использовать методы организации технологического процесса защиты информации ограниченного доступа (ПК-15).	б) применение простых апробированных решений; в) сочетание простых и сложных защитных средств. 18. Контроль целостности может использоваться для: а) предупреждения нарушений информационной безопасности; б) обнаружения нарушений; в) локализации последствий нарушений. 19. Обеспечение высокой доступности можно ограничить: а) критически важными серверами; б) сетевым оборудованием; в) всей цепочкой от пользователей до серверов. 20. Некоторые авторы включают в число основных аспектов безопасности подотчетность. На Ваш взгляд, это: а) правильно, потому что без подотчетности не может быть безопасности; б) неправильно, потому что подотчетность – не цель, а средство достижения безопасности; в) не имеет значения, потому что все это словесная эквилибристика, далекая от реальной безопасности. 21. Предметная область «Защита информации» согласно ГОСТ Р 50922—96 – это: а) деятельность (процесс), направленная на предотвращение утечки защищаемой информации; б) специальное устройство для защиты информации; в) производственное объединение. 22. Служба защиты информации (СЗИ) – это: а) государственное учреждение по защите информации; б) специализированная организация; в) это самостоятельное структурное подразделение в рамках деятельности организации, тесно связана со службами охраны и объектового режима, составляет основу всей системы обеспечения информационной безопасности. 23. Что нельзя отнести к функциям, выполняемым службой защиты информации: а) финансовое обеспечение деятельности организации; б) организация обучения персонала правилам соблюдения и поддержания информационной безопасной деятельности предприятия; в) материально-техническое и технологическое обеспечение информационной безопасности на предприятии. 24. Что можно отнести к функциям управления подразделением по защите информации? а) планирование, б) контроль; в) разработка программного обеспечения.
***Имеет практический опыт*:** организации и сопровождения аттестации объекта информатизации по требованиям безопасности информации (ПК-5); проведения технико-	25. Функция управления, связанная с определением целей управления подразделением по защите информации, поиском методов, необходимых для достижения поставленных целей на защиту информации и определением системы показателей, определяющих эффективность применения методов для достижения поставленных целей – это:

экономического обоснования проектных решений; подсистем и средств обеспечения информационной безопасности (ПК-7); организации комплекса мер по обеспечению информационной безопасности (ПК-13); организации работы малого коллектива исполнителей в профессиональной деятельности (ПК-14); использования методов организации технологического процесса защиты информации ограниченного доступа (ПК-15).	a) Организация деятельности подразделения по защите информации; b) Контроль деятельности подразделения по защите информации; c) Планирование деятельности подразделения по защите информации. 26. К организационным задачам и функциям службы защиты информации не относится: a) разработка и проектов защиты для каждого вида безопасности их реализация приемки и контроль за постоянной работоспособности; b) организация проведения совместно с другими подразделениями мероприятий в отношении конкурентов, взаимодействия с правоохранительными органами; c) оказание управленческих воздействий на создание/поддержку своевременной реорганизацию структуры управления безопасности предприятия. 27. Управление качеством работы подразделения по защите информации и затратами на защиту информации являются функциями управления: a) результатами защиты информации; b) процессами защиты информации; c) ресурсами, выделяемыми на защиту информации. 28. К факторам, влияющим на организацию службы ЗИ не относится: a) финансовые возможности предприятия; b) решения акционеров предприятия; c) масштабы предприятия. 29. Отраслевое и функциональное, структурное подразделение по ЗИ, осуществляющее исполнительные и организационно-распорядительные функции, отнесённые к его введенью в пределах одного из направлений деятельности по ЗИ – это: a) Служба защиты информации; b) Отдел защиты информации; c) Сектор/группа по защите информации. 30. Такие недостатки как низкая оперативность решения, степень доверия и ответственности к сторонней организации характерны для: a) Создания службы ЗИ, минимизированной по исполняемым функциям; b) Создания службы ЗИ с ограниченными функциями; c) Создания полноценной службы по исполняемым функциям. 31. Лаборатория - это: a) централизованно управляемая, совокупность структурных подразделений по ЗИ объединённая общими целями, функциями и объектами управления; b) структурное подразделение по ЗИ, которое осуществляет исполнительные и организационно-распорядительные функции по исследованию вопросов ЗИ, возможностей реализации, средств и технологий защиты информации; c) структурное подразделение отдела/отделения по ЗИ, осуществляющее исполнительную деятельность,

	возглавляемое главным специалистом или старшим инженером, и объединяющее 2-х или более специалистов по ЗИ, инженеров, техников в одном тематическом направлении деятельности отдела/отделения. 32. На чем должно базироваться правовое обеспечение информационной безопасности? a) соблюдение принципов законности; b) комплексности и индивидуальности; c) системности подходов; d) балансе интересов в информационной сфере; e) взаимодействии и координации. 33. Назовите методы управления подразделением по ЗИ a) экономические; b) правовые; c) юридические; d) социально-психологические; e) принудительные. 34. Через какие стимулы и мотивы воздействуют социально-психологические методы управления подразделением по ЗИ? a) увеличение заработной платы; b) развитие социальных потребностей и интересов; c) развитие межличностных коммуникаций. 35. Каковы требования к технологии управления безопасностью? a) соответствие современному уровню развития информационных технологий; b) выделение максимально возможных средств на защиту информации; c) наличие обособленных субъектов в информационной системе. 36. Какая проблема является основной, с точки зрения соблюдения политики безопасности на предприятии? a) недостаточно грамотное построение пропускного режима b) недостаточно грамотное формулирование должностных инструкций c) недостаточное обучение персонала

7.2. Методические рекомендации к определению процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Рабочая учебная программа дисциплины содержит следующие структурные элементы:

- перечень компетенций, формируемых в результате изучения дисциплины в процессе освоения образовательной программы;

- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности в процессе освоения образовательной программы (далее–задания). Задания по каждой компетенции, как правило, не должны повторяться.

Требования по формированию задания на оценку ЗНАНИЙ:

- обучающийся должен воспроизводить и объяснять учебный материал с требуемой степенью научной точности и полноты;

- применяются средства оценивания компетенций: тестирование, вопросы по основным понятиям дисциплины и т.п.

Требования по формированию задания на оценку УМЕНИЙ:

- обучающийся должен решать типовые задачи (выполнять задания) на основе воспроизведения стандартных алгоритмов решения;

- применяются следующие средства оценивания компетенций: простые ситуационные задачи (задания) с коротким ответом или простым действием, упражнения, задания на соответствие или на установление правильной последовательности, эссе и другое.

Требования по формированию задания на оценку навыков и (или) ОПЫТА ДЕЯТЕЛЬНОСТИ:

- обучающийся должен решать усложненные задачи (выполнять задания) на основе приобретенных знаний, умений и навыков, с их применением в определенных ситуациях;

- применяются средства оценивания компетенций: задания требующие многошаговых решений как в известной, так и в нестандартной ситуациях, задания, требующие поэтапного решения и развернутого ответа, ситуационные задачи, проектная деятельность, задания расчетно-графического типа. Средства оценивания компетенций выбираются в соответствии с заявленными результатами обучения по дисциплине.

Процедура выставления оценки доводится до сведения обучающихся в течение месяца с начала изучения дисциплины путем ознакомления их с технологической картой дисциплины, которая является неотъемлемой частью рабочей учебной программы по дисциплине.

В результате оценивания компетенций по дисциплине студенту начисляются баллы по шкале, указанной в рабочей учебной программе по дисциплине.

7.3. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Успешность усвоения дисциплины характеризуется качественной оценкой на основе листа оценки сформированности компетенций, который является приложением к зачетно-экзаменационной ведомости при проведении промежуточной аттестации по дисциплине.

Критерии оценивания компетенций

Компетенция считается сформированной, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 86 до 100, что соответствует *повышенному уровню* сформированности компетенции.

Компетенция считается сформированной, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 61 до 85,9, что соответствует *пороговому уровню* сформированности компетенции.

Компетенция считается несформированной, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет практические работы, не демонстрирует необходимых умений, доля невыполненных заданий, предусмотренных рабочей учебной программой составляет

55 %, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже 61, что соответствует *допороговому уровню*.

Шкала оценки уровня освоения дисциплины

Качественная оценка может быть выражена: в процентном отношении качества усвоения дисциплины, которая соответствует баллам, и переводится в уровневую шкалу и оценки «отлично» / 5, «хорошо» / 4, «удовлетворительно» / 3, «неудовлетворительно» / 2, «зачтено», «не зачтено». Преподаватель ведет письменный учет текущей успеваемости студента в соответствии с технологической картой по дисциплине.

Шкала оценки результатов освоения дисциплины, сформированности компетенций

Шкалы оценки уровня сформированности компетенции (й)		Шкала оценки уровня освоения дисциплины		
Уровневая шкала оценки компетенций	*100 балльная шкала, %*	*100 балльная шкала, %*	*5-балльная шкала, дифференцированная оценка/балл*	*Недифференцированная оценка*
допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
пороговый	61-85,9	70-85,9	«хорошо» / 4	зачтено
		61-69,9	«удовлетворительно» / 3	зачтено
повышенный	86-100	86-100	«отлично» / 5	зачтено

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Списки основной литературы

1. Ворона, В. А. Теоретические основы обеспечения безопасности объектов информатизации [Текст] : учеб. пособие для вузов по направлению "Информ. безопасность" / В. А. Ворона, В. А. Тихонов, Л. В. Митрякова. - М. : Горячая линия - Телеком, 2016. - 304 с. : ил.
2. Основы управления информационной безопасностью [Текст] : учеб. пособие для вузов по направлениям подгот. (специальностям) укрупн. группы специальностей "Информ. безопасность" / А. П. Курило [и др.]. - 2-е изд., испр. - М. : Горячая линия -Телеком, 2016. - 244 с. : ил.
3. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс] : учеб. пособие для вузов по направлению 09.03.01 "Информатика и вычисл. техника" / В. Ф. Шаньгин. - Документ Bookread2. - М. : ФОРУМ [и др.], 2018. - 592 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=937502
4. Учебно-методический комплекс по дисциплине "Организация и управление службой ЗИ"[Электронный ресурс] : для студентов направления 10.03.01 "Информ. безопасность" / Поволж. гос. ун-т сервиса (ФГБОУ ВО "ПВГУС"), Каф. "Приклад. информатика в экономике" ; сост. Т. В. Альшанская. - Документ Adobe Acrobat. - Тольятти : ПВГУС, 2016. - 758 КБ, 72 с. : ил. - Режим доступа: http://elib.tolgas.ru

Списки дополнительной литературы

5. Анисимов, А. А. Менеджмент в сфере информационной безопасности [Текст] : учеб. пособие / А. А. Анисимов. - М. : БИНОМ. Лаб. знаний, 2010. - 175 с. : ил., табл.

6. Благодатин, А. А. Финансовый словарь [Текст] / А. А. Благодатин, Л. Ш. Лозовский, Б. А. Райзберг. - М. : ИНФРА-М, 2009. - 377 с.
7. Борисов, М. А. Основы организационно-правовой защиты информации [Текст] : [учеб. пособие] / М. А. Борисов, О. А. Романов. - Изд. 2-е. - М. : Кн. дом "ЛИБРОКОМ", 2013. - 208 с.
8. Вдовенко, Л. А. Информационная система предприятия [Электронный ресурс] : учеб. пособие для вузов по экон. направлениям подгот. / Л. А. Вдовенко. - 2-е изд., перераб. и доп. - Документ Bookread2. - М. : Вузов. учеб. [и др.], 2014. - 301 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=501089#
9. Грибунин, В. Г. Комплексная система защиты информации на предприятии [Текст] : учеб. пособие для вузов по специальностям "Орг. и технология защиты информ.", "Комплекс. защита объектов информатизации" / В. Г. Грибунин, В. В. Чудовский. - М. : Академия, 2009. - 412 с. : ил., табл.
10. Информационные системы и технологии управления [Текст] : учеб. для вузов по специальности "Финансы и кредит", "Бухгалт. учет, анализ и аудит", по направлениям "Менеджмент" и "Экономика" / Г. А. Титоренко [и др.] под ред. Г. А. Титоренко. - 3-е изд., перераб. и доп. - М. : ЮНИТИ-ДАНА, 2013. - 591 с. : табл.
11. Калянов, Г. Н. Консалтинг: от бизнес-стратегии к корпоративной информационно-управляющей системе [Текст] : учеб. для вузов по специальности "Приклад. информатика (по областям)" и др. экон. специальностям / Г. Н. Калянов. - 2-е изд. - М. : Горячая линия - Телеком, 2011. - 210 с. : табл.
12. Корпоративные информационные системы управления [Текст] : учебник / Н. М. Абдикеев [и др.] под науч. ред. Н. М. Абдикеева, О. В. Китовой. - М. : Инфра-М, 2010. - 464 с. : ил., табл.
13. Милославская, Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью[Текст] : учеб. пособие для студентов вузов по направлению подгот. 090900 "Информ. безопасность" (уровни - бакалавр, магистр) / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд., испр. - М. : Горячая линия -Телеком, 2014. - 214 с.
14. Райзберг, Б. А. Прикладная теория управления экономическими системами [Текст] : учеб.-метод. пособие / Б. А. РайзбергМоск. психол.-соц. ин-т. - М. : МПСИ, 2011. - 460 с. : табл.
15. Малышева, Е. Ю. Системы автоматизированной обработки экономической информации[Электронный ресурс] : учеб. пособие для вузов по специальности "Приклад. информатика (по обл.)" и др. экон. специальностям / Е. Ю. Малышева, С. М. БобровскийПоволж. гос. ун-т сервиса (ПВГУС). - Документ Adobe Acrobat. - Тольятти : ПВГУС, 2010. - 1,21 МБ, 52 с. : ил. - Режим доступа: http://elib.tolgas.ru
16. Фундаментальные основы защиты информации[Текст] : лаб. практикум для студентов специальности "Орг. и технология защиты информ." и др. специальностей и направлений / Поволж. гос. ун-т сервиса (ПВГУС), Каф. "Соврем. естествознание" ; сост.: А. И. Бочкарев, Т. С. Бочкарева, В. В. Смоленский. - Тольятти : ПВГУС, 2009. - 103 с. : ил.

8.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет" (далее – сеть "Интернет"), необходимых для освоения дисциплины

Интернет-ресурсы

1. ИНТУИТ. Национальный открытый университет [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/. – Загл. с экрана.

2. Российское образование [Электронный ресурс] : федер. портал. - Режим доступа: http://www.edu.ru. - Загл. с экрана.

3. Электронная библиотечная система Поволжского государственного университета сервиса [Электронный ресурс]. - Режим доступа: http://elib.tolgas.ru/. - Загл. с экрана.

4. Электронно-библиотечная система Znanium.com [Электронный ресурс]. - Режим доступа: http://znanium.com/. - Загл. с экрана.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Краткая характеристика применяемого программного обеспечения

№ п/п	Программный продукт	Характеристика	Назначение при освоении дисциплины
1.	Microsoft Office	Пакет прикладных программ	Оформление отчетов по практическим работам
2.	Microsoft Windows	Операционная система	Выполнение практических работ
3.	Консультант-Плюс	, Информационно-справочные системы	Выполнение практических работ

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения занятий лекционного типа используются специальные помещения – учебные аудитории, укомплектованные специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации.

Для проведения лабораторных работ используется лаборатория «Аудитория информационных технологий, информатики и методов программирования», оснащенная лабораторным оборудованием различной степени сложности

Для текущего контроля и промежуточной аттестации используются специальные помещения – учебные аудитории, укомплектованные специализированной мебелью, и (или) компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета.

Для самостоятельной работы обучающихся используются специальные помещения – учебные аудитории для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета.

11. Примерная технологическая карта дисциплины «Организация и управление службой ЗИ»

Институт экономики
кафедра «Прикладная информатика в экономике»
преподаватель _____, направление подготовки 10.03.01 «Информационная безопасность»

№	Виды контрольных точек	Кол-во контр. точек	Кол-во баллов за 1 контр. точку	График прохождения контрольных точек																Зач. неделя
				Февраль				Март				Апрель				Май				
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
1.	Обязательные задания:																			
1.1.	Выполнение практических работ	7	8		+	+	+	+	+	+	+									
1.2.	Выполнение курсовой работы	1	20										+							
2.	Дополнительные задания:																			
2.1.	Доклад на научной конференции	1	10									+								
2.2	Публикация научной статьи	1	14									+								
	Форма контроля												+							Экзамен