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 «Основы научных исследований и дипломное проектирование»
для студентов направления подготовки 10.03.01 «Информационная безопасность»
направленности (профиля) «Организация и технология защиты информации»

Тольятти 2018 г.

Рабочая учебная программа по дисциплине «Основы научных исследований и дипломное проектирование» 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 «Основы научных исследований и дипломное проектирование» 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

обучение студентов подходам, технологиям и методами разработки дипломных проектов в направлении организации и технологии защиты информации, в рамках требований ФГОС к минимуму содержания основной образовательной программы.

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

организационно-управленческая деятельность:

- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
- 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
ОК-8	способность к самоорганизации и самообразованию.
ОПК-4	способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.
ОПК-6	способность применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности.

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*:** основы профессиональной деятельности (ОК-8); технологии сбора, накопления, обработки, передачи и распространения информации (ОПК-4); состав мероприятий по охране труда и технике безопасности (ОПК-6).	Лекции	Собеседование
***Умеет*:** получать новые знания и умения для	Практические работы	Защита практических работ

достижения цели, использовать профессиональную информацию для самосовершенствования и гармоничного развития личности (ОК-8); использовать, обобщать и анализировать информацию, ставить цели, выбирать оптимальный путь достижения (ОПК-4); разрабатывать мероприятия по охране труда и технике безопасности (ОПК-6).		
***Имеет практический опыт*:** применения полученных теоретических знаний в практической деятельности (ОК-8). использования методов научного познания в профессиональной области (ОПК-4). разработки мероприятий по охране труда и технике безопасности (ОПК-6).	Решение разноуровневых и проблемных задач	Защита практических работ

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к профессиональному циклу, базовой части.
Её освоение осуществляется: в 8 семестре.

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Код компетенции(й)
	Предшествующие дисциплины	
1	«Проектирование информационных систем»	ОПК-4
2	«Организационное и правовое обеспечение информационной безопасности»	ОК-4, ОПК-5
3	«Программно-аппаратные средства защиты информации»	ОПК-7, ПК-6
4	«Техническая защита информации»	ОПК-7. ПК-15, ПСК-1
5	«Информационно-аналитическая деятельность по обеспечению комплексной безопасности»	ОПК-4, ОПК-7

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
Итого часов Зачетных единиц	108 ч. 3 з.е.	108 ч. 3 з.е.
Лекции (час)	18	4
Практические (семинарские) занятия (час)	28	8
Лабораторные работы (час)	-	-
Самостоятельная работа (час)	62	92
Курсовой проект (+,-)	-	-
Контрольная работа (+,-)	-	-
Экзамен, семестр /час.	-	-
Дифференцированный зачет, семестр	8 СЕМЕСТР	9 СЕМЕСТР (4 ч.)
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 учебной работы, включая самостоятельную работу студентов и трудоемкость (в академических часах)			Средства и технологии оценки
		Лекции	практ. занятия	Самост. работа	
1	***Тема 1. Цели и задачи дипломного проектирования. Структура и содержание ДП.*** Структура дипломного проекта. Соотношение отдельных частей дипломного проекта. Введение. Обоснование актуальности выбранной темы. Аналитическая часть. Характеристики и анализ предметной области объекта. Описание основных теоретических положений, методов, способов, подходов и средств, используемых для решения поставленной задачи. Описание объекта и средств проектирования. Выводы по рассмотренным вопросам с обоснованием главных направлений проектных решений. Проектная часть. Реализация и описание разработок в рамках выбранной темы и с учетом специфики конкретного объекта и аспектов исследования, подходов, методов и средств решения конкретных задач. Обоснование проектных решений по технологии сбора, передачи, обработки и передачи информации. Эффективность проектируемой системы. Экономическое обоснование результатов, полученных в ходе дипломного проектирования.	2/1	2/2	5/12	Опрос по теме лекции, защита отчёта по практической работе
2	***Тема 2. Основные элементы системы защиты информации. Анализ угроз и каналов утечки информации.*** Основные понятия в области обеспечения информационной безопасности. Принципы обеспечения информационной безопасности. Общая схема обеспечения информационной безопасности. Основные виды угроз безопасности. Классификация угроз.	2/1	4/2	6/10	Опрос по теме лекции, защита отчёта по практической работе

№ п/п	Раздел дисциплины	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в академических часах)			Средства и технологии оценки
		Лекции	практ. занятия	Самост. работа	
3	***Тема 3. Определение модели нарушителя, характерного для заданных исходных данных и угроз.*** Модель нарушителя. Классификация нарушителей по уровню знаний о КС, по уровню возможностей, по времени действия, по месту действия. Ограничения и предположения о характере действий возможных нарушителей.	2/0	4/0	6/10	Опрос по теме лекции, защита отчёта по практической работе
4	***Тема 4. Определение и оценка рисков.*** Основные стандарты, описывающие процесс управления рисками. Риск информационной безопасности. Менеджмент рисков информационной безопасности. Критерии оценки риска. Критерии воздействия. Критерии допустимости риска. Область применения и границы менеджмента рисков информационной безопасности. Оценка рисков информационной безопасности. Методологии оценки.	2/0	2/0	5/10	Опрос по теме лекции, защита отчёта по практической работе
5	***Тема 5. Мероприятия по организационно-правовой защите информации.*** Роль организационных средств в системе средств обеспечения информационной безопасности. Меры обеспечения информационной безопасности. Нормативно-правовые меры. Морально-этические меры. Административные меры. Политика безопасности. Три уровня детализации политики безопасности. Основные элементы политики безопасности.	2/1	4/0	8/10	Опрос по теме лекции, защита отчёта по практической работе
6	***Тема 6. Мероприятия по программно-аппаратной защите информации.*** Основные категории требований к программной и программно-аппаратной реализации средств защиты информации. Задачи программно-аппаратной защиты информации. Концептуальная модель безопасности информации. Основные виды программных и программно-аппаратных средств защиты информации. Основные подходы к защите данных от НСД. Использование	2/0	4/0	8/10	Опрос по теме лекции, защита отчёта по практической работе

№ п/п	Раздел дисциплины	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в академических часах)			Средства и технологии оценки
		Лекции	*практ. занятия*	*Самост. работа*	
	межсетевых экранов для защиты информационных процессов.				
7	***Тема 7. Мероприятия по инженерно-технической защите информации.*** Классификация источников и носителей информации. Виды носителей информации. Способы записи и съема информации с носителя. Классификация и структура технических каналов утечки информации. Категории объектов защиты. Технические средства защиты информации. Мероприятия по инженерно-технической защите информации.	2/0	4/0	8/10	Опрос по теме лекции, защита отчёта по практической работе
8	***Тема 8. Структура и основные элементы комплексной системы защиты информации в организации.*** Международный стандарт ISO 27001. Комплексный подход к обеспечению информационной безопасности. Структура и основные элементы комплексной системы защиты информации в организации. Подсистемы информационной безопасности.	2/0	2/2	8/10	Опрос по теме лекции, защита отчёта по практической работе
9	***Тема 9. Планирование основных этапов выполнения проекта и организация контроля.*** Планирование основных этапов выполнения проекта и организация контроля. Методология управления проектом. Структура и длительность задач проекта. Определение показателей прямой экономической эффективности. Оценка экономической эффективности внедрения мероприятий проекта в реальную информационную среду.	2/1	2/2	8/10	Опрос по теме лекции, защита отчёта по практической работе
Промежуточная аттестация по дисциплине		***18/4***	***28/8***	***62/92***	Дифференцированный зачет

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

4.2. Содержание практических работ

№	Наименование практических работ	Обьем часов	Наименование темы дисциплины
1	*Практическая работа 1.* *Тема: «Цели и задачи дипломного проектирования. Структура и содержание ДП. Постановка задачи исследования».* *Цель занятия*: Определить цель, задачи и структуру дипломного проекта.	2/2	*Тема 1. Цели и задачи дипломного проектирования. Структура и содержание ДП.*
2	*Практическая работа 2.* *Тема: «Основные элементы системы защиты информации. Анализ угроз и каналов утечки информации».* *Цель занятия*: Провести анализ существующей ИС предприятия и системы защиты информации предприятия..	4/2	*Тема 2. Основные элементы системы защиты информации. Анализ угроз и каналов утечки информации.*
3	*Практическая работа 3.* *Тема: «Определение модели нарушителя, характерного для заданных исходных данных и угроз».* *Цель занятия*: Провести анализ существующей ИС предприятия и определить модель нарушителя, характерного для заданных исходных данных и угроз.	4/0	*Тема 3. Определение модели нарушителя, характерного для заданных исходных данных и угроз.*
4	*Практическая работа 4.* *Тема: «Определение и оценка рисков».* *Цель занятия:* Провести анализ, определение и оценку рисков для системы защиты информации предприятия.	2/0	*Тема 4. Определение и оценка рисков.*
5	*Практическая работа 5.* *Тема: «Мероприятия по организационно-правовой защите информации».* *Цель занятия:* Провести анализ существующей ИС предприятия и системы защиты информации предприятия..	4/0	*Тема 5. Мероприятия по организационно-правовой защите информации.*
6	*Практическая работа 6.* *Тема: «Мероприятия по программно-аппаратной защите информации».* *Цель занятия:* Провести анализ существующей системы защиты информации предприятия и определить мероприятия по программно-аппаратной защите информации.	4/0	*Тема 6. Мероприятия по программно-аппаратной защите информации.*
7	*Практическая работа 7.* *Тема: «Мероприятия по инженерно-технической защите информации».* *Цель занятия*: Провести анализ существующей системы защиты информации предприятия и определить мероприятия по инженерно-технической защите информации.	4/0	*Тема 7. Мероприятия по инженерно-технической защите информации.*
8	*Практическая работа 8.* *Тема: «Структура и основные элементы комплексной системы защиты информации в организации».* *Цель занятия*: Провести анализ существующей системы защиты информации.	2/2	*Тема 8. Структура и основные элементы комплексной системы защиты информации в организации.*
9	*Практическая работа 9.* *Тема: «Планирование основных этапов выполнения*	2/2	*Тема 9. Планирование основных этапов выполнения проекта и*

	проекта и организация контроля. *Оценка экономической эффективности внедрения мероприятий проекта в реальную информационную среду».* *Цель занятия*: использовать методики управления проектами на практике для разработки данного проекта, изучить методику расчёта экономической эффективности проекта.		*организация контроля.*
	Итого	*28/8*	

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

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
ОК-8, ОПК-4, ОПК-6	Работа с литературой	Конспект	Собеседование	20/30/-
ОК-8, ОПК-4, ОПК-6	Ответы на контрольные вопросы	Конспект	Тест	20/30/-
ОК-8, ОПК-4, ОПК-6	Подготовка доклада на конференцию	Доклад	Опубликование тезисов доклада	22/32/-
			Итого	62/92/-

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

Содержание заданий для самостоятельной работы

Вопросы для самоконтроля

1. Структура дипломного проекта. Соотношение отдельных частей дипломного проекта.
2. Обоснование актуальности выбранной темы.
3. Аналитическая часть. Характеристики и анализ предметной области объекта.
4. Описание основных теоретических положений, методов, способов, подходов и средств, используемых для решения поставленной задачи. Описание объекта и средств проектирования.
5. Проектная часть. Реализация и описание разработок в рамках выбранной темы и с учетом специфики конкретного объекта и аспектов исследования, подходов, методов и средств решения конкретных задач.
6. Обоснование проектных решений по технологии сбора, передачи, обработки и передачи информации.
7. Эффективность проектируемой системы. Экономическое обоснование результатов, полученных в ходе дипломного проектирования.
8. Основные элементы системы защиты информации.
9. Основные понятия в области обеспечения информационной безопасности.
10. Принципы обеспечения информационной безопасности.
11. Общая схема обеспечения информационной безопасности.
12. Основные виды угроз безопасности. Классификация угроз.
13. Модель нарушителя.

14. Классификация нарушителей по уровню знаний о КС, по уровню возможностей, по времени действия, по месту действия.
15. Ограничения и предположения о характере действий возможных нарушителей.
16. Основные стандарты, описывающие процесс управления рисками.
17. Риск информационной безопасности. Менеджмент рисков информационной безопасности.
18. Критерии оценки риска. Критерии воздействия. Критерии допустимости риска.
19. Область применения и границы менеджмента рисков информационной безопасности.
20. Оценка рисков информационной безопасности. Методологии оценки.
21. Роль организационных средств в системе средств обеспечения информационной безопасности.
22. Меры обеспечения информационной безопасности. Нормативно-правовые меры. Морально-этические меры. Административные меры.
23. Политика безопасности. Три уровня детализации политики безопасности.
24. Основные элементы политики безопасности.
25. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации.
26. Задачи программно-аппаратной защиты информации.
27. Концептуальная модель безопасности информации.
28. Основные виды программных и программно-аппаратных средств защиты информации.
29. Основные подходы к защите данных от НСД.
30. Использование межсетевых экранов для защиты информационных процессов.
31. Классификация источников и носителей информации. Виды носителей информации.
32. Способы записи и съема информации с носителя.
33. Классификация и структура технических каналов утечки информации.
34. Категории объектов защиты.
35. Технические средства защиты информации. Мероприятия по инженерно-технической защите информации.
36. Международный стандарт ISO 27001. Комплексный подход к обеспечению информационной безопасности.
37. Структура и основные элементы комплексной системы защиты информации в организации.
38. Подсистемы информационной безопасности.
39. Планирование основных этапов выполнения проекта и организация контроля.
40. Методология управления проектом. Структура и длительность задач проекта.
41. Определение показателей прямой экономической эффективности.
42. Оценка экономической эффективности внедрения мероприятий проекта в реальную информационную среду.

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: «Цели и задачи дипломного проектирования. Структура и содержание ДП.», «Основные		

	элементы системы защиты информации. Анализ угроз и каналов утечки информации».		

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.*** ***Тема: «Цели и задачи дипломного проектирования. Структура и содержание ДП. Постановка задачи исследования».***	*Цель занятия*: Определить цель, задачи и структуру дипломного проекта. *Задачи:* 1. Изучить содержание основных разделов дипломного проекта по учебному пособию. 2. Сформулировать тему проекта; 3. Определить цель и задачи исследования. Задачи могут формулироваться в форме перечня мероприятий аналитической и проектной части; В соответствии с рекомендациями учебного пособия определить детальную структуру проекта с кратким содержанием разделов и частей проекта..
2.	***Практическая работа 2.*** ***Тема: «Основные элементы системы защиты информации. Анализ угроз и***	*Цель занятия*: Провести анализ существующей ИС предприятия и системы защиты информации предприятия..

	каналов утечки информации».	*Задачи:* Для предметной области, определенной в практической работе № 1, определить: 1) Виды информации, используемой в деятельности предприятия. Дать характеристику каждому виду информации на предприятии. 2) Провести анализ всех видов информации с точки зрения её возможной утечки и несанкционированного доступа. 3) Определить основные виды угроз и способов их реализации для основных объектов защиты для заданного предприятия/ 4) Провести предварительный анализ и выявление возможных каналов утечки информации Провести предварительный анализ для возможных каналов утечки информации и опасности утечки
3.	***Практическая работа 3.*** ***Тема: «Определение модели нарушителя, характерного для заданных исходных данных и угроз».***	*Цель занятия*: Провести анализ существующей ИС предприятия и определить модель нарушителя, характерного для заданных исходных данных и угроз. *Задачи:* Для исходных данных практических работ №1-2: Определить модель нарушителя, характерного для заданных исходных данных и угроз.
4.	***Практическая работа 4.*** ***Тема: «Определение и оценка рисков».***	***Цель занятия:*** Провести анализ, определение и оценку рисков для системы защиты информации предприятия. *Задачи:* Для исходных данных практических работ №1-3: Определить и оценить риски, связанные с угрозами по разработанной модели нарушителя..
5.	***Практическая работа 5.*** ***Тема: «Мероприятия по организационно-правовой защите информации».***	*Цель занятия:* Провести анализ существующей ИС предприятия и системы защиты информации предприятия.. *Задачи:* Для задач, решаемых на основе применения организационных мер по защите информации выбранного объекта, необходимо рассмотреть совокупность нормативных и распорядительных документов, определяющих политику информационной безопасности объектов, Для задач, решаемых с правовым обеспечением защиты информации на предприятиях, должен быть выбран и обоснован комплекс правовых мер и мероприятий, обеспечивающих защиту выбранного объекта. Для задач, связанных с защитой и обработкой конфиденциальных документов, необходимо рассмотреть типовой состав технологических стадий входного, выходного и внутреннего

		документопотоков,
6.	***Практическая работа 6.*** ***Тема: «Мероприятия по программно-аппаратной защите информации».***	*Цель занятия:* Провести анализ существующей системы защиты информации предприятия и определить мероприятия по программно-аппаратной защите информации. *Задачи:* Рассмотреть модели компьютерных систем, модели безопасного взаимодействия и управления безопасностью в информационных системах, модели сетевых средств безопасности, методы декомпозиции моделей угроз.
7.	***Практическая работа 7.*** ***Тема: «Мероприятия по инженерно-технической защите информации».***	*Цель занятия*: Провести анализ существующей системы защиты информации предприятия и определить мероприятия по инженерно-технической защите информации. *Задачи:* ***Для задач, решаемых на основе инженерно-технической защиты информации*** выбранного объекта, необходимо провести анализ существующих методов, способов и средств его инженерно-технической охраны в соответствии с видами угроз, основ организации и методического обеспечения такой защиты.
	Практическая работа 8. ***Тема: «Структура и основные элементы комплексной системы защиты информации в организации».***	*Цель занятия*: Провести анализ существующей системы защиты информации. *Задачи*:***Для решения задач комплексной защиты информации*** на предприятии должен быть проведен системный анализ основ защиты информации, должны быть рассмотрены модели комплексной системы защиты информации (КСЗИ):
	Практическая работа 9. ***Тема: «Планирование основных этапов выполнения проекта и организация контроля.*** ***Оценка экономической эффективности внедрения мероприятий проекта в реальную информационную среду».***	*Цель занятия*: использовать методики управления проектами на практике для разработки данного проекта, изучить методику расчёта экономической эффективности проекта. *Задачи:* разработать план проекта на выбранную тему и рассчитать его экономическую эффективность.

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

Курсовая работа по дисциплине учебным планом не предусмотрена.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (зачет, 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.
ОК-8, ОПК-4, ОПК-6	*текущий*	*устный опрос*	*1-46*
ОК-8, ОПК-4, ОПК-6	*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*:** основы профессиональной деятельности (ОК-8); технологии сбора, накопления, обработки, передачи и распространения информации (ОПК-4); состав мероприятий по охране труда и технике безопасности (ОПК-6).	1. Основные направления общей системы мер в сфере информационной безопасности; организационное обеспечение информационной безопасности; разработка специализированного программного обеспечения; изготовление и использование специальных аппаратных средств; совершенствование криптографических (математических) методов защиты информации; усиление административных мер наказания персонала; открытие доступа к информации; 2. Основными задачами организационно-управленческой деятельности (менеджмента) в сфере информационной безопасности являются: обеспечение комплексности всех решений, реализуемых в процессе обеспечения информационной безопасности; обеспечение непрерывности и целостности процессов информационной безопасности; разработка специализированного программного обеспечения; изготовление и использование специальных аппаратных средств; 3. Основными задачами организационно-управленческой деятельности (менеджмента) в сфере информационной безопасности являются: решение методических задач, лежащих в основе эффективного управления информационной безопасностью, таких, как вопросы управления рисками, экономическое моделирование и т.п.; управление человеческими ресурсами и поведением персонала с учетом необходимости решения задач информационной безопасности. изготовление и использование специальных аппаратных средств; совершенствование криптографических (математических) методов защиты информации; 4. Под организационным обеспечением и менеджментом в сфере информационной безопасности обычно принято понимать; решение управленческих вопросов на уровне отдельных субъектов (предприятий, организаций) или групп организаций, которые совместно решают определенные задачи, требующие защиты информации. изготовление и использование специальных аппаратных средств; совершенствование криптографических (математических)

	методов защиты информации; разработка специализированного программного обеспечения; 5. Международные организации, действующие в сфере информационной безопасности решают задачу разработки технических и организационных решений, таких как: протоколы глобальных сетей; архитектуры, алгоритмы, протоколы публичных средств шифрования данных; правила построения глобальных сетей обмена данными и других элементов глобальной инфраструктуры информационной безопасности. рынок программных и аппаратных средств, обеспечивающих защиту информации; систему подготовки, переподготовки и повышения квалификации специалистов в сфере информационной безопасности; 6. Основными объектами государственной и международной стандартизации могут выступать: методы шифрования и криптографической защиты данных; технологии идентификации пользователей информационных систем; методы аутентификации; методы тестирования (проверки) и оценки информационных систем на предмет их защищенности; рынок программных и аппаратных средств, обеспечивающих защиту информации; система подготовки, переподготовки и повышения квалификации специалистов в сфере информационной безопасности; 7. Все негативные воздействия на информационные активы, защиту от которых (воздействий) предполагает информационная безопасность, могут быть разделены на основные виды: нарушение конфиденциальности информации; разрушение (утеря, необратимое изменение) информации; Внедрение разработанных политик безопасности. Анализ соблюдения требований внедренной политики безопасности и формулирование требований по ее дальнейшему совершенствованию. 8. Все негативные воздействия на информационные активы, защиту от которых (воздействий) предполагает информационная безопасность, могут быть разделены на основные виды: разрушение (утеря, необратимое изменение) информации; недоступность информационных ресурсов – возникновение ситуаций, когда пользователи теряют возможность доступа к необходимым данным. Проведение предварительного исследования состояния информационной безопасности. Собственно разработку политики безопасности. 9. Общий жизненный цикл политики информационной безопасности включает в себя ряд основных шагов. Проведение предварительного исследования состояния информационной безопасности. Собственно разработку политики безопасности. метки безопасности; принудительное управление доступом. 10. Общий жизненный цикл политики информационной безопасности включает в себя ряд основных шагов.

	Внедрение разработанных политик безопасности. Анализ соблюдения требований внедренной политики безопасности и формулирование требований по ее дальнейшему совершенствованию. архитектуры, алгоритмы, протоколы публичных средств шифрования данных; правила построения глобальных сетей обмена данными. 11. Самостоятельное структурное подразделение предприятия, непосредственно выполняющее ключевые функции защиты информационных ресурсов, это: департамент информационной безопасности; департамент работы с персоналом; департамент управления производством; 12. Основными задачами департамента информационной безопасности предприятия. как правило, являются: организация и координация работ по обеспечению комплексной защиты информации на предприятии; контроль за выполнением установленных требований; оценка эффективности работы подразделений и персонала предприятия по обеспечению информационной безопасности; выполнение отдельных административных и технических функций по обеспечению информационной безопасности, разрушение (утеря, необратимое изменение) информации; недоступность информационных ресурсов – возникновение ситуаций, когда пользователи теряют возможность доступа к необходимым данным. 13. На этапе локализации и устранения последствий инцидента происходит: определение конкретных параметров нарушения (нападения), его характера; предварительный анализ действий нарушителя и сценария произошедшего (происходящего) нападения, алгоритма работы появившегося вируса и т.п.; блокирование действий нарушителя (если нарушение является длящимся); блокирование работы информационной с целью недопущения дальнейших разрушительных действий, распространения вредоносных программ или утечки конфиденциальной информации. анализ целей и мотивов нападавших; анализ фундаментальных (организационных и технических) причин, которые сделали нападение возможным и успешным (если оно было успешным); 14. Основные задачи на этапе локализации ущерба, причиненного произошедшим нарушением (инцидентом): смена скомпрометированных паролей отдельных пользователей; переустановка поврежденных операционных систем, а также поврежденного программного обеспечения; восстановление нарушенной конфигурации (настроек) программного обеспечения и операционных систем; восстановление поврежденной информации (баз данных, файлов), как из ранее созданных резервных копий, так и другими способами. анализ последствий (в том числе и долгосрочных) нападения для всей деятельности предприятия; анализ и оценка работы персонала и взаимоотношений с предприятиями-партнерами.

***Умеет*:** получать новые знания и умения для достижения цели, использовать профессиональную информацию для самосовершенствования и гармоничного развития личности (ОК-8); использовать, обобщать и анализировать информацию, ставить цели, выбирать оптимальный путь достижения (ОПК-4); разрабатывать мероприятия по охране труда и технике безопасности (ОПК-6).	1. В рамках системы менеджмента в сфере информационной безопасности проводят работу по нескольким направлениям: формирование и практическая реализация комплексной многоуровневой политики информационной безопасности предприятия и системы внутренних требований, норм и правил; организация департамента (службы, отдела) информационной безопасности; разработка системы мер и действий на случай возникновения непредвиденных ситуаций ("Управление инцидентами"); проведение аудитов (комплексных проверок) состояния информационной безопасности на предприятии. методы шифрования и криптографической защиты данных; технологии идентификации пользователей информационных систем; 2. Отдельные процессы, процедуры, механизмы и инструменты защиты информации могут быть направлены: на ограничение и разграничение доступа; на открытие доступа к информации; информационное скрытие; введение избыточной информации и использование избыточных информационных систем (средств хранения, обработки и передачи информации); 3. Отдельные процессы, процедуры, механизмы и инструменты защиты информации могут быть направлены: на ограничение и разграничение доступа; использование методов надежного хранения, преобразования и передачи информации; нормативно-административное побуждение и принуждение; на усиление административных мер наказания персонала; 4. Создание и развитие безопасной информационной инфраструктуры может включать в себя: надежную инфраструктуру передачи информации и рынок услуг доступа к таким каналам связи; рынок программных и аппаратных средств, обеспечивающих защиту информации; систему подготовки, переподготовки и повышения квалификации специалистов в сфере информационной безопасности; нормативно-административное побуждение и принуждение; на усиление административных мер наказания персонала; 5. Создание и развитие безопасной информационной инфраструктуры может включать в себя: общие правила использования информации, а также ее передачи, совместной эксплуатации информационных сетей (в том числе протоколы информационного обмена); систему обмена информацией и распространения знаний о существующих уязвимостях тех или иных информационных технологий, возможных угрозах информационной безопасности и способах их нейтрализации; законодательную и правоприменительную систему, обеспечивающую охрану имущественных и иных интересов всех участников информационного обмена нормативно-административное побуждение и принуждение; на усиление административных мер наказания персонала; 6. Согласно Оранжевой книге, политика безопасности должна включать в себя по крайней мере следующие

	элементы: произвольное управление доступом; безопасность повторного использования объектов; рынок программных и аппаратных средств, обеспечивающих защиту информации; систему подготовки, переподготовки и повышения квалификации специалистов в сфере информационной безопасности; 7. Согласно Оранжевой книге, политика безопасности должна включать в себя по крайней мере следующие элементы: метки безопасности; принудительное управление доступом. архитектуры, алгоритмы, протоколы публичных средств шифрования данных; правила построения глобальных сетей обмена данными. 8. Британский стандарт BS 7799:1995 рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы: вводный, подтверждающий озабоченность высшего руководства проблемами информационной безопасности; организационный, содержащий описание подразделений, комиссий, групп и т.д., отвечающих за работы в области информационной безопасности; классификационный, описывающий имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты; штатный, характеризующий меры безопасности, применяемые к персоналу; метки безопасности; принудительное управление доступом. 9. Британский стандарт BS 7799:1995 рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы: раздел, освещающий вопросы физической защиты ; управляющий раздел, описывающий подход к управлению компьютерами и компьютерными сетями; раздел, описывающий правила разграничения доступа к производственной информации; произвольное управление доступом; безопасность повторного использования объектов; 10. Британский стандарт BS 7799:1995 рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы: раздел, характеризующий порядок разработки и сопровождения систем; раздел, описывающий меры, направленные на обеспечение непрерывной работы организации; юридический раздел, подтверждающий соответствие политики безопасности действующему законодательству. методы шифрования и криптографической защиты данных; технологии идентификации пользователей информационных систем; 11. Политика информационной безопасности среднего уровня должна содержать следующие основные разделы. Общее описание той сферы деятельности, на которую она распространяется. Область применения политики безопасности – перечень всех лиц, организаций, информационных систем, к которым она

	применяется. Часть политики безопасности, определяющая конкретные правила, критерии и требования к процедурам обращения информации, элементам информационной инфраструктуры и т.п. раздел, освещающий вопросы физической защиты ; управляющий раздел, описывающий подход к управлению компьютерами и компьютерными сетями; 12. Политика информационной безопасности среднего уровня должна содержать следующие основные разделы. Закрепление за определенными сотрудниками обязанностей по выполнению необходимой работы с целью решения задач в рамках данной политики безопасности. Основные процедуры разрешения появляющихся затруднений, а также перечень лиц, ответственных за непосредственную работу с персоналом по вопросам, относящимся к данной политике безопасности. раздел, характеризующий порядок разработки и сопровождения систем; раздел, описывающий меры, направленные на обеспечение непрерывной работы организации; 13. Основные задачи на этапе оценки и анализа процесса нападения и его обстоятельств: анализ целей и мотивов нападавших; анализ фундаментальных (организационных и технических) причин, которые сделали нападение возможным и успешным (если оно было успешным); анализ последствий (в том числе и долгосрочных) нападения для всей деятельности предприятия; анализ и оценка работы персонала и взаимоотношений с предприятиями-партнерами. восстановление нарушенной конфигурации (настроек) программного обеспечения и операционных систем; восстановление поврежденной информации (баз данных, файлов), как из ранее созданных резервных копий, так и другими способами. 14. В общем случае организационные процедуры (регламенты) реагирования на чрезвычайные ситуации (инциденты) должны включать в себя: регламенты альтернативных процессов обработки информации на период выхода из строя основных информационных ресурсов; определение групп персонала, ответственных за выполнение тех или иных функций в случае возникновения чрезвычайной ситуации; техническую и организационную документацию, необходимую для восстановления информационных систем и данных после чрезвычайной ситуации; Проведение предварительного исследования состояния информационной безопасности. Собственно разработку политики безопасности. 15. В общем случае организационные процедуры (регламенты) реагирования на чрезвычайные ситуации (инциденты) должны включать в себя: техническую и организационную документацию, необходимую для восстановления информационных систем и данных после чрезвычайной ситуации; порядок хранения архивных (резервных) копий данных и программных приложений обработки данных; соглашения с поставщиками программных и аппаратных средств

	о срочной поставке компонент, вышедших из строя и требующих замены в случае чрезвычайной ситуации. Внедрение разработанных политик безопасности. Анализ соблюдения требований внедренной политики безопасности и формулирование требований по ее дальнейшему совершенствованию.
***Имеет практический опыт*:** применения полученных теоретических знаний в практической деятельности (ОК-8). использования методов научного познания в профессиональной области (ОПК-4). разработки мероприятий по охране труда и технике безопасности (ОПК-6).	1. Назовите основные принципы, методы и средства обеспечения защиты информации в автоматизированной системе. 2. Сформулируйте подробную структуру политики информационной безопасности. 3. Приведите примеры двух разделов второго уровня политики информационной безопасности. 4. Приведите типовой план (программу) аудита информационной безопасности на предприятии. 5. Приведите структуру процедуры мониторинга обеспечения уровня защищенности информации автоматизированной системы в рамках концепции ITSM. 6. Приведите подробную структуру документированной процедуры реагирования на чрезвычайные ситуации (инциденты).

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. Кузнецов, И. Н. Рефераты, курсовые и дипломные работы. Методика подготовки и оформления[Электронный ресурс] : учеб.-метод. пособие / И. Н. Кузнецов. - 7-е изд. - Документ Bookread2. - М. : Дашков и К, 2018. - 339 с. - Режим доступа: http://znanium.com/bookread2.php?book=415062
2. Овчаров, А. О. Методология научного исследования [Электронный ресурс] : учеб. по направлению 38.04.01 "Экономика" / А. О. Овчаров, Т. Н. Овчарова. - Документ Bookread2. - М. : ИНФРА-М, 2017. - 304 с. - Режим доступа: http://znanium.com/bookread2.php?book=894675
3. Рузавин, Г. И. Методология научного познания[Электронный ресурс] : учеб. пособие для студентов и аспирантов вузов / Г. И. Рузавин. - Документ Bookread2. - М. : ЮНИТИ-ДАНА, 2015. - 288 с. - Режим доступа: http://znanium.com/bookread2.php?book=881053
4. Тихонов, В. А. Теоретические основы научных исследований [Текст] : учеб. пособие по специальности "Информ. безопасность автоматизир. систем" / В. А. Тихонов, В. А. Ворона, Л. В. Митрякова. - М. : Горячая линия -Телеком, 2016. - 320 с. : ил..
5. Шкляр, М. Ф. Основы научных исследований[Электронный ресурс] : учеб. пособие / М. Ф. Шкляр. - 6-е изд. - Документ Bookread2. - М. : Дашков и К, 2018. - 206 с. - Режим доступа: http://znanium.com/bookread2.php?book=340857
6. Учебно-методическое пособие по дисциплине "Основы научных исследований и дипломное проектирование" [Текст] : для студентов направления подгот. 10.03.01 "Информ. безопасность" / Поволж. гос. ун-т сервиса (ФГБОУ ВО "ПВГУС"), Каф. "Приклад. информатика в экономике" ; сост. С. М. Бобровский. - Тольятти : ПВГУС, 2017. - 83 с.

Списки дополнительной литературы

7. Агапов, Е. П. Методика исследований в социальной работе [Текст] : учеб. пособие / Е. П. Агапов. - М. : Дашков и К, 2010. - 223 с.
8. Баловсяк, Н. В. Реферат, курсовая, диплом на компьютере [Текст] / Н. В. Баловсяк. - СПб. : Питер, 2007. - 173 с. : рис.
9. Безуглов, И. Г. Основы научного исследования[Текст] : учеб. пособие для аспирантов и студентов-дипломников / И. Г. Безуглов, В. В. Лебединский, А. И. БезугловМоск. откр. соц. ун-т. - М. : Акад. проект, 2008. - 194 с. : ил., табл.
10. Вертакова, Ю. В. Исследование социально-экономических и политических процессов[Текст] : учеб. пособие для вузов по направлению "Экономика" и экон. специальностям / Ю. В. Вертакова, О. В. Согачева. - М. : КноРус, 2009. - 336 с. : ил., табл.
11. Воронцов, Г. А. Труд студента. Ступени успеха на пути к диплому [Электронный ресурс] : учеб. пособие для студентов вузов / Г. А. Воронцов. - 2-е изд., перераб. и доп. - Документ Bookread2. - М. : ИНФРА-М, 2014. - 256 с. - Режим доступа: http://znanium.com/bookread2.php?book=448923

12. Захарова, В. В. Как написать и защитить диплом[Текст] : учеб. пособие для экон. специальностей / В. В. Захарова, В. С. Соколов. - М. : ФОРУМ [и др.], 2008. - 63 с. : табл.
13. Исследование социально-экономических и политических процессов [Текст] : учеб.-метод. пособие / И. А. Аглуллин [и др.] Рос. акад. гос. службы при Президенте РФ ; под общ. ред. А. Н. Данчула. - Изд. 2-е, стер. - М. : РАГС, 2009. - 227 с. : ил., граф.
14. Колесникова, Н. И. От конспекта к диссертации[Текст] : учеб. пособие по развитию навыков письменной речи / Н. И. Колесникова. - 3-е изд., испр. - М. : ФлинтаНаука, 2006. - 288 с. : ил.
15. Кузнецов, И. Н. Научное исследование: Методика проведения и оформление [Текст] / И. Н. Кузнецов. - Изд. 3-е, перераб. и доп. - М. : Дашков и К, 2007. - 457 с.
16. Кузнецов, И. Н. Рефераты, курсовые и дипломные работы. Методика подготовки и оформления[Текст] : учеб.-метод. пособие / И. Н. Кузнецов. - М. : Дашков и К, 2009. - 339 с.
17. Леонович, Е. Н. Эффективное курсовое и дипломное проектирование: алгоритмы и технологии [Текст] : учеб. пособие [для написания курсовой и диплом. работ] / Е. Н. Леонович, Н. В. Микляева[под ред. Н. В. Микляевой]. - М. : Форум, 2012. - 184 с.
18. Невежин, В. П. Как написать, оформить и защитить выпускную квалификационную работу[Текст] : учеб. пособие по направлениям подгот. бакалавров, дипломир. специалистов и магистров / В. П. Невежин. - М. : ФОРУМ, 2012. - 111 с. : табл.Н
19. овиков, Ю. Н. Подготовка и защита бакалаврской работы, магистерской диссертации, дипломного проекта [Электронный ресурс] : учеб. пособие / Ю. Н. Новиков. - Изд. 2-е, стер. - Документ Reader. - СПб. [и др.] : Лань, 2017. - 31 с. - Режим доступа: https://e.lanbook.com/reader/book/94211/#1
20. Рузавин, Г. И. Методология научного познания[Текст] : учеб. пособие для студентов и аспирантов вузов / Г. И. Рузавин. - М. : ЮНИТИ-ДАНА, 2009. - 287 с.
21. Рыжков, И. Б. Основы научных исследований и изобретательства [Электронный ресурс] : учеб. пособие для студентов вузов по направлениям подгот. (специальностям) "Природообустройство", "Вод. ресурсы и водопользование" / И. Б. Рыжков. - Изд. 2-е, стер. - Документ HTML. - СПб. [и др.] : Лань, 2013. - 222 с. - Режим доступа: https://e.lanbook.com/reader/book/30202/#1
22. Тихонов, В. А. Научные исследования: концептуальные, теоретические и практические аспекты [Текст] : [учеб. пособие для вузов] / В. А. Тихонов, В. А. Ворона. - М. : Горячая линия - Телеком, 2009. - 296 с. : ил.
23. Шкляр, М. Ф. Основы научных исследований[Текст] : учеб. пособие / М. Ф. Шкляр. - М. : Дашков и К, 2007. - 243 с.

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
4.	*MSAT*	Программа анализа рисков ИБ	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 «Основы научных исследований и дипломное проектирование»

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	9	8	+	+	+	+	+	+	+	+	+								
2.	Дополнительные задания:																			
2.1.	Доклад на научной конференции	1	14									+								
2.2	Публикация научной статьи	1	14									+								
	Форма контроля												+							Диф.зачет