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 «Техническая защита информации»
для студентов направления подготовки 10.03.01 «Информационная безопасность»
направленности (профиля) «Организация и технология защиты информации»

Тольятти 2018 г.

Рабочая учебная программа по дисциплине «Техническая защита информации» 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 «Техническая защита информации» 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

теоретическая и практическая подготовленность бакалавра к организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях.

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

установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

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

проведение проектных расчетов элементов систем обеспечения информационной безопасности;

организационно-управленческая деятельность:

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
ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.
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.
ПСК-1	способность разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение.

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*:** технические каналы утечки информации,	Лекции	Собеседование

возможности технических разведок (ОПК-7); способы и средства защиты информации от утечки по техническим каналам (ПК-15); методы и средства контроля эффективности технической защиты информации (ПСК-1);		
***Умеет*:** анализировать и оценивать угрозы информационной безопасности объекта (ОПК-7); применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем (ПК-15); разработать комплекс мер по обеспечению информационной безопасности объекта в области технической защиты информации (ПСК-1);	Лабораторные работы	Защита лабораторных работ
***Имеет практический опыт*:** применения методов технической защиты информации (ОПК-7); формирования требований по защите информации (ПК-15); разработки комплекса мер по обеспечению информационной безопасности объекта в области технической защиты информации (ПСК-1).	Решение разноуровневых и проблемных задач	Защита лабораторных работ

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к профессиональному циклу, базовой части.
Её освоение осуществляется: в 5 семестре.

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Код компетенции(й)
	Предшествующие дисциплины	
1	«Физика»	ОПК-1
2	«Основы информационной безопасности»	ОК-5; ОПК-7
	Последующие дисциплины	
1	«Проектирование систем информационной безопасности»	ПК-4; ПК-7; ПСК-1
2	«Защита информационных процессов в компьютерных системах и телекоммуникационных сетях»	ОПК-7
3	«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	216 ч. 6 з.е.	216 ч. 6 з.е.
Лекции (час)	54	10
Практические (семинарские) занятия (час)	-	-
Лабораторные работы (час)	70	12
Самостоятельная работа (час)	65	185
Курсовая работа (+,-)	+	+
Контрольная работа (+,-)	-	-
Экзамен, семестр /час.	5 СЕМЕСТР/ 27 ч.	5 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

№ n/n	Раздел дисциплины	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в академических часах)			Средства и технологии оценки
		Лекции	Лабораторные занятия	Самост. работа	
1	***Тема 1. Объекты информационной защиты. Виды информации, защищаемой техническими средствами.*** Объекты информационной защиты. Виды информации, защищаемой техническими средствами. Сущность инженерной защиты и технической охраны источников информации. Принципы инженерно-технической защиты информации. Понятие о конфиденциальной информации. Основные свойства информации как предмета инженерно-технической защиты.	6/1	4/4	9/24	Опрос по теме лекции, защита отчёта по лабораторной работе
2	***Тема 2. Демаскирующие признаки объектов защиты.*** Понятие о демаскирующих объектах, сигналах и веществах. Демаскирующие признаки объектов защиты. Классификация демаскирующих признаков. Видовые демаскирующие признаки. Сигнальные демаскирующие признаки. Вещественные демаскирующие признаки.	2/0	6/4	8/20	Опрос по теме лекции, защита отчёта по лабораторной работе
3	***Тема 3. Источники и носители информации, защищаемой техническими средствами.*** Источники и носители информации, защищаемой техническими средствами. Классификация источников и носителей информации. Принципы записи и съема информации с носителей. Способы записи и съема	4/1	12/0	8/22	Опрос по теме лекции, защита отчёта по лабораторной работе

№ n/n	Раздел дисциплины	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в академических часах)			Средства и технологии оценки
		Лекции	Лабораторные занятия	Самост. работа	
	информации с носителя..				
4	***Тема 4. Виды угроз безопасности информации, защищаемой техническими средствами.*** Безопасность информации. Угрозы безопасности информации. Несанкционированное распространение (утечка) информации. Виды угроз безопасности информации, защищаемой техническими средствами. Оценка величины угрозы.	4/1	12/0	8/24	Опрос по теме лекции, защита отчёта по лабораторной работе
5	***Тема 5. Принципы добывания и обработки информации техническими средствами.*** Особенности утечки информации. Классификация и структура технических каналов утечки информации. Материально-вещественные каналы утечки информации и их особенности. Оптические каналы утечки информации и их особенности. Радиоэлектронные каналы утечки информации и их особенности. Акустические каналы утечки информации и их особенности. Основные способы и принципы работы, основные виды и классификация средств наблюдения объектов, подслушивания и перехвата сигналов..	8/1	6/0	8/24	Опрос по теме лекции, защита отчёта по лабораторной работе
6	***Тема 6.*** **Методы, способы и средства инженерно-технической защиты информации.** Категории объектов защиты. Особенности задач охраны различных типов объектов. Системный подход к инженерно-технической защите информации.	10/2	6/0	8/24	Опрос по теме лекции, защита отчёта по лабораторной работе

№ п/п	Раздел дисциплины	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в академических часах)			Средства и технологии оценки
		Лекции	Лабораторные занятия	Самост. работа	
	Структура системы обеспечения безопасности объектов. Основные этапы проектирования системы защиты информации техническими средствами. Структура комплекса системы защиты информации техническими средствами. принципы моделирования объектов защиты и технических каналов утечки информации; способы оценки угроз безопасности информации и расходов на техническую защиту..				
7	***Тема 7. Организация инженерно-технической защиты информации.*** Организационные и технические меры инженерно-технической защиты информации в государственных и коммерческих структурах. Контроль эффективности защиты информации. Способы оценки расходов на техническую защиту информации..	10/2	12/0	8/24	Опрос по теме лекции, защита отчёта по лабораторной работе
8	***Тема 8. Технические средства в организации режима охраны.*** Технические средства в организации режима охраны. Роль и место технических средств в организации режима охраны, современная концепция защиты объектов; основные составляющие систем ТСО: датчики, приборы визуального наблюдения, системы сбора и обработки информации, средства связи, питания и тревожно-вызывной сигнализации; Практическая реализация систем ТСО: охрана режимных помещений, проект охраны	10/2	12/0	8/23	Опрос по теме лекции, защита отчёта по лабораторной работе

№ n/n	Раздел дисциплины	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в академических часах)			Средства и технологии оценки
		Лекции	Лабораторные занятия	Самост. работа	
	объектов.				
Промежуточная аттестация по дисциплине		***54/10***	***70/12***	***65/185***	Экзамен

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

4.2. Содержание лабораторных работ

№	Наименование лабораторных работ	Обьем часов	Наименование темы дисциплины
1	*Лабораторная работа 1:* Объекты информационной защиты. Виды информации, защищаемой техническими средствами. *Цель:* изучить классификацию объектов информационной защиты, виды информации, защищаемой техническими средствами.	4/4	Тема 1. Объекты информационной защиты. Виды информации, защищаемой техническими средствами.
2	*Лабораторная работа 2:* Демаскирующие признаки объектов защиты. *Цель:* изучить основные виды демаскирующих признаков объектов защиты.	6/4	Тема 2. Демаскирующие признаки объектов защиты.
3	*Лабораторная работа 3:* Источники и носители информации, защищаемой техническими средствами. *Цель:* изучить основные виды источников и носителей информации, защищаемой техническими средствами.	6/4	Тема 3. Источники и носители информации, защищаемой техническими средствами.
4	*Лабораторная работа 4:* Технические каналы утечки информации. *Цель:* изучить основные виды технических каналов утечки информации.	6/0	Тема 3. Источники и носители информации, защищаемой техническими средствами.
5	*Лабораторная работа 5:* Виды угроз безопасности информации, защищаемой техническими средствами. *Цель:* изучить основные виды угроз безопасности информации, защищаемой техническими средствами.	6/0	Тема 4. Виды угроз безопасности информации, защищаемой техническими средствами.
6	*Лабораторная работа 6:* Средства наблюдения объектов, подслушивания и перехвата сигналов. *Цель:* изучить основные виды средств наблюдения объектов, подслушивания и перехвата сигналов..	6/0	Тема 4. Виды угроз безопасности информации, защищаемой техническими средствами.

7	*Лабораторная работа 7:* Основные элементы системы инженерно-технической защиты информации. *Цель:* изучить основные элементы системы инженерно-технической защиты информации..	6/0	Тема 5. Принципы добывания и обработки информации техническими средствами.
8	*Лабораторная работа 8:* Мероприятия по защите информации. *Цель:* изучить основные мероприятия по защите информации.	6/0	Тема 6. Методы, способы и средства инженерно-технической защиты информации.
9	*Лабораторная работа 9:* Мероприятия по защите компьютерной сети. *Цель:* изучить основные мероприятия по защите компьютерной сети..	6/0	Тема 7. Организация инженерно-технической защиты информации.
10	*Лабораторная работа 10:* Мероприятия по защите компьютерной сети. *Цель:* изучить основные мероприятия по защите компьютерной сети..	6/0	Тема 7. Организация инженерно-технической защиты информации.
11	*Лабораторная работа 11:* Модель нарушителя. *Цель:* изучить модель нарушителя.	6/0	Тема 8. Технические средства в организации режима охраны.
12	*Лабораторная работа 12:* Средства и системы инженерно-технической защиты информации. *Цель:* изучить основные средства и системы инженерно-технической защиты информации.	6/0	Тема 8. Технические средства в организации режима охраны.
	Итого	*70/12*	

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
ОПК-7, ПК-15, ПСК-1	Работа с литературой	Конспект	Собеседование	20/60/-
ОПК-7, ПК-15, ПСК-1	Ответы на контрольные вопросы	Конспект	Тест	20/60/-
ОПК-7, ПК-15, ПСК-1	Подготовка доклада на конференцию	Доклад	Опубликование тезисов доклада	25/65/-
			Итого	65/185/-

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

Содержание заданий для самостоятельной работы

Вопросы для самоконтроля

1. Что понимают под угрозой безопасности данных
2. Виды информации, защищаемой техническими средствами.
3. Сущность инженерной защиты и технической охраны источников информации. Принципы инженерно-технической защиты информации.
4. Виды угроз безопасности информации, защищаемой техническими средствами.
5. Классификация и структура технических каналов утечки информации.
6. Материально-вещественные каналы утечки информации и их особенности.
7. Оптические каналы утечки информации и их особенности.
8. Радиоэлектронные каналы утечки информации и их особенности.
9. Акустические каналы утечки информации и их особенности.
10. Способы и средства информационного скрытия акустических сигналов и речевой информации.
11. Понятие о демаскирующих объектах, сигналах и веществах..
12. Демаскирующие признаки объектов защиты. Классификация демаскирующих признаков.
13. Источники и носители информации, защищаемой техническими средствами.
14. Принципы записи и съема информации с носителей.
15. Принципы добывания и обработки информации техническими средствами.
16. Основные способы и принципы работы средств наблюдения объектов.
17. Основные виды и классификация средств наблюдения объектов.
18. Основные способы и принципы работы средств подслушивания и перехвата сигналов.
19. Основные виды и классификация средств подслушивания и перехвата сигналов.
20. Системный подход к инженерно-технической защите информации.
21. Основные этапы проектирования системы защиты информации техническими средствами.
22. Структура комплекса системы защиты информации техническими средствами.
23. Принципы моделирования объектов защиты и технических каналов утечки информации.
24. Способы оценки угроз безопасности информации.
25. Способы оценки расходов на техническую защиту информации.
26. Способы и принципы работы средств защиты информации от наблюдения, подслушивания и перехвата.
27. Основные виды и классификация средств защиты информации от наблюдения, подслушивания и перехвата.
28. Организационные меры инженерно-технической защиты информации в государственных и коммерческих структурах.
29. Технические меры инженерно-технической защиты информации в государственных и коммерческих структурах.
30. Контроль эффективности защиты информации.
31. Роль и место технических средств в организации режима охраны.
32. Современная концепция защиты объектов.
33. Основные составляющие систем ТСО..

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: «Объекты информационной защиты. Виды информации, защищаемой техническими средствами.», «Демаскирующие признаки объектов защиты».		

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 лабораторных 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, Лабораторные 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 лабораторныхзанятиях 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 лабораторных работах

Лабораторные работы

№	Наименование лабораторной работы	Задания по лабораторной работе
1.	*Лабораторная работа 1:* Объекты информационной защиты. Виды информации, защищаемой техническими средствами.	*Цель:* изучить классификацию объектов информационной защиты, виды информации, защищаемой техническими средствами. *Задание:* для заданной предметной области определить объекты информационной защиты, виды информации, защищаемой техническими средствами.
2.	*Лабораторная работа 2:* Демаскирующие признаки объектов защиты.	*Цель:* изучить основные виды демаскирующих признаков объектов защиты. *Задание:* 1. Для каждого вида объектов защиты определить демаскирующие признаки объектов защиты, составить список признаков с краткой характеристикой каждого признака. 2. Для каждого вида объектов защиты для каждого демаскирующего признака провести его предварительный анализ и оценку. Сделать вывод о наиболее критичных с точки зрения защиты информации демаскирующих признаках.
3.	*Лабораторная работа 3:* Источники и носители информации, защищаемой техническими средствами.	*Цель:* изучить основные виды источников и носителей информации, защищаемой техническими средствами. *Задание:* Для каждого вида объектов защиты определить источники и носители информации, защищаемой техническими средствами. При этом рассмотреть принципы и основные способы записи и съема информации с носителей.
4.	*Лабораторная работа 4:* Технические каналы утечки информации.	*Цель:* изучить основные виды технических каналов утечки информации. *Задание:* 1) Оценить виды информации с точки зрения её возможной утечки и несанкционированного доступа. 2) Провести предварительный поиск и выявление возможных каналов утечки информации. 3) Провести предварительный анализ возможных каналов утечки информации и опасности утечки
5.	*Лабораторная работа 5:* Виды	*Цель:* изучить основные виды угроз

	угроз безопасности информации, защищаемой техническими средствами.	безопасности информации, защищаемой техническими средствами. *Задание:* Определить основные виды угроз безопасности информации, защищаемой техническими средствами.
6.	*Лабораторная работа 6:* Средства наблюдения объектов, подслушивания и перехвата сигналов.	*Цель:* изучить основные виды средств наблюдения объектов, подслушивания и перехвата сигналов. *Задание:* 1) Определить основные виды средств наблюдения объектов, подслушивания и перехвата сигналов, применяемых для выявленных возможных каналов утечки информации. 2) Сделать подробный анализ средств наблюдения объектов, подслушивания и перехвата сигналов по одному из направлений.
7.	*Лабораторная работа 7:* Основные элементы системы инженерно-технической защиты информации.	*Цель:* изучить основные элементы системы инженерно-технической защиты информации. *Задание:* 1) Определить основные виды угроз и способов их реализации для основных объектов защиты для заданного предприятия. 2) Для каждого вида угроз определить основные способы и средства предотвращения угроз. 3) Сформулировать основные элементы системы инженерно-технической защиты информации для заданного предприятия.
8.	*Лабораторная работа 8:* Мероприятия по защите информации.	*Цель:* изучить основные мероприятия по защите информации. *Задание:* 1. Провести предварительный анализ возможных каналов утечки информации и опасности утечки для заданного помещения. 2. Определить основные виды угроз и способов их реализации для заданного помещения. 3. Для каждого вида угроз определить основные способы и средства предотвращения угроз. 4. Сформулировать основные мероприятия по инженерно-технической защите информации для заданного помещения:
9.	*Лабораторная работа 9:* Мероприятия по защите компьютерной сети.	*Цель:* изучить основные мероприятия по защите компьютерной сети.

		Задание: 1. Провести предварительный анализ возможных каналов утечки информации и опасности утечки для компьютерной сети здания. 2. Определить основные виды угроз и способов их реализации для компьютерной сети здания. 3. Сформулировать основные мероприятия по инженерно-технической защите информации в компьютерной сети организации
10.	*Лабораторная работа 10:* Мероприятия по защите компьютерной сети..	*Цель:* изучить основные мероприятия по защите компьютерной сети. *Задание:* 1. Провести предварительный анализ возможных каналов утечки информации и опасности утечки для компьютерной сети здания. 2. Определить основные виды угроз и способов их реализации для компьютерной сети здания. 3. Сформулировать основные мероприятия по инженерно-технической защите информации в компьютерной сети организации
11.	*Лабораторная работа 11:* Модель нарушителя.	*Цель:* изучить модель нарушителя. *Задание:* 1. Определить основные угрозы систем инженерно-технической защиты информации. 2. Определить модель нарушителя, характерного для заданных исходных данных и угроз по п.1 3. Оценить риски, связанные с угрозами по разработанной модели нарушителя.
12.	*Лабораторная работа 12:* Средства и системы инженерно-технической защиты информации.	*Цель:* изучить основные средства и системы инженерно-технической защиты информации. *Задание:* 1. Выбрать и определить основные технические средства защиты информации от наблюдения ,подслушивания и перехвата, которые намечаются для применения в системе ИТЗИ организации. 2. Для каждого технического средства определить его технические характеристики, показатели назначения, паспортные данные и.т.д. 3. Сравнить технические характеристики и данные выбранных технических средств с другими

		аналогичными средствами в данном классе, обосновать выбор данного вида и модели технического средства. 4. Оценить, насколько могут сократиться риски, определенные в лабораторной работе 7, в случае применения выбранных технических средств. Обосновать новую оценку риска.

Лабораторные 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 лабораторных 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, Лабораторные 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 «Техническая защита информации» по правилам оформления должна соответствовать требованиям к курсовым работам, утвержденным на кафедре.

Структура работы:

Введение.

1. Аналитическая часть

- Описание предметной области: структура предприятия, основные виды деятельности и процессы, основные объекты инфраструктуры.
- Структура информационной системы предприятия.
- Задачи обеспечения ИБ на предприятии и задачи инженерно-технической защиты информации на предприятии. Анализ и выявление объектов защиты.
- Анализ и выявление возможных каналов утечки информации и несанкционированного доступа к ресурсам, основных угроз.

2. Проектная часть.

- Определение контролируемой зоны объектов предприятия.
- Определение каналов утечки информации и несанкционированного доступа к ресурсам с привязкой к объектам.
- Анализ и выбор основных подходов к инженерно-технической защите информации на предприятии.
- Определение основных элементов системы ИТЗИ предприятия.
- Составление плана ТЗИ на объекте. Планирование защитных мероприятий по различным направлениям (по объектам, по видам угроз, по видам дестабилизирующего воздействия).
- Анализ и выбор технических средств защиты информации для реализации мероприятий по ТЗИ и использования в КСЗИ предприятия.

3. Экономическая часть.

Анализ и определение основных направлений и статей затрат на мероприятия по ИТЗИ предприятия.

Расчет единовременных затрат на мероприятия по ИТЗИ предприятия по отдельным направлениям, например:

- Затраты на совершенствование объектов инфраструктуры;
- Затраты на приобретение оборудования, приборов и средств контроля и измерения, средств инженерно-технического оснащения;
- Затраты на обучение персонала;
- Затраты на аутсорсинг, использование услуг внешних организаций;
- Затраты на внешнюю сертификацию и лицензирование.

Расчет постоянных затрат на мероприятия по ИТЗИ предприятия по отдельным направлениям, например:

- Затраты на регулярно проводимые мероприятия с системе ЗИ.
- Затраты на техобслуживание и ремонт.

Оценка экономической эффективности мероприятия по ИТЗИ предприятия по соотношению повышения эффективности ИТЗИ и затрат.

Заключение.

Библиографический список.

Приложения.

ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ РАБОТ по дисциплине «Техническая защита информации»

1. Разработка системы инженерно-технической защиты информации предприятия.
2. Совершенствование системы инженерно-технической защиты информации предприятия.
3. Разработка методов инженерной защиты и технической охраны источников информации.
4. Разработка модели угроз безопасности информации, защищаемой техническими средствами.
5. Определение, классификация и структура технических каналов утечки информации.
6. Разработка способов и средств информационного скрытия акустических сигналов и речевой информации.
7. Разработка комплексной системы защиты информации техническими средствами.
8. Моделирование объектов защиты и технических каналов утечки информации.
9. Оценка угроз безопасности информации по техническим каналам.
10. Анализ рисков, связанных с угрозами безопасности информации по техническим каналам.
11. Способы и принципы работы средств защиты информации от наблюдения, подслушивания и перехвата.
12. Определение и классификация средств защиты информации от наблюдения, подслушивания и перехвата.
13. Организационные меры инженерно-технической защиты информации в государственных структурах.
14. Организационные меры инженерно-технической защиты информации в коммерческих структурах.
15. Технические меры инженерно-технической защиты информации в государственных структурах.
16. Технические меры инженерно-технической защиты информации в коммерческих структурах.
17. Практическая реализация систем ТСО. Охрана режимных помещений.
18. Практическая реализация систем ТСО. Проект охраны объектов.
19. Основные составляющие систем ТСО. Датчики (извещатели).

20. Основные составляющие систем ТСО. Приборы визуального наблюдения.
21. Основные составляющие систем ТСО. Системы сбора и обработки информации.
22. Основные составляющие систем ТСО. Средства связи, питания и тревожно-вызывной сигнализации.

Выбор варианта темы курсовой работы определяет преподаватель. При этом уточняется предметная область и состав проектной части.

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.
ОПК-7, ПК-15, ПСК-1	*текущий*	*устный опрос*	*1-46*
ОПК-7, ПК-15, ПСК-1	*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*:** технические каналы утечки информации, возможности технических разведок (ОПК-7); способы и средства защиты информации от утечки по техническим каналам (ПК-15); методы и средства контроля эффективности технической защиты информации (ПСК-1);	1. Из перечисленных моделей: 1) Адепт-50; 2) игровая; 3) Хартстона; 4) с полным перекрытием; 5) Белла-ЛаПадула; 6) LWM — моделями политики безопасности на основе дискретных компонент являются *1, 3* 1, 3, 5 4, 5, 6 1, 2, 3 2. Из перечисленного: 1) протоколирование; 2) тестирование программ; 3) аутентификация; 4) обработка угроз; 5) резервное копирование — группами требований к документированию системы защиты информации являются *1, 2, 4* 2, 3, 4 3, 4, 5 1, 2, 3 3. Из перечисленного: 1) случайная; 2) преднамеренная; 3) стихийная; 4) детерминированная; 5) объективная; 6) субъективная — угрозы безопасности по природе происхождения классифицируются как *1, 2* 1, 2, 3, 4 5, 6 3, 4 4. Из перечисленного: 1) технические; 2) общие; 3) организационные; 4) конкретные; 5) программные — группами требований к системам защиты информации являются *2, 3, 4* 1, 2, 4 3, 4, 5 1, 2, 3

	5. Из перечисленного: 1) оповещение о попытках нарушения защиты; 2) идентификация; 3) аутентификация; 4) учет носителей информации; 5) управление потоками информации — подсистема управления доступом системы защиты информации должна обеспечивать *2, 3, 5* 1, 2, 5 3, 4, 5 1, 2, 3 6. Достоинствами аппаратной реализации криптографического закрытия данных являются *высокая производительность и простота* целостность и безопасность доступность и конфиденциальность практичность и гибкость 7. Эффективная программа безопасности требует сбалансированного применения: 1. Технических и нетехнических методов 2. Контрмер и защитных механизмов 3. Физической безопасности и технических средств защиты 4. Процедур безопасности и шифрования 8. Активный перехват информации это перехват, который: заключается в установке подслушивающего устройства в аппаратуру средств обработки информации; основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций; неправомерно использует технологические отходы информационного процесса; осуществляется путем использования оптической техники; осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера. 9. К внутренним нарушителям информационной безопасности относится: клиенты; пользователи системы; посетители; любые лица, находящиеся внутри контролируемой территории; представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации. персонал, обслуживающий технические средства. сотрудники отделов разработки и сопровождения ПО; технический персонал, обслуживающий здание 10. Перехват, который осуществляется путем использования оптической техники называется: активный перехват; пассивный перехват; аудиоперехват;

	видеоперехват; просмотр мусора. 11. Что такое несанкционированный доступ (нсд)? Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа Создание резервных копий в организации Правила и положения, выработанные в организации для обхода парольной защиты Вход в систему без согласования с руководителем организации 12. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется: активный перехват; пассивный перехват; аудиоперехват; видеоперехват; 13. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется: активный перехват; пассивный перехват; аудиоперехват; видеоперехват; просмотр мусора. 14. Что из ниже перечисленного работает по принципу подавления радиоканала между трубкой и базой? +блокираторы сотовой связи -генераторы белого шума -излучатели -кодеры -волоконно-оптические каналы 15. Какой блокиратор утечки информации работает в диапазоне подавляемого канала? +технический -динамический -статический -цифровой -аналоговый 16. Генератор шума, корреляционные характеристики которого могут динамически меняться во время переговоров это? +маскиратор речи -блокатор сигнала -кодер сигнала -изолятор -декодер сигнала 17. Какой вид защищен от помех, создаваемых источниками электромагнитного излучения, стойки к колебаниям температуры и влажности? +оптическое волокно -тонкий коаксиал

	-толстый коаксиал -витая пара -дуга 18. Какой канал утечки акустической информации образуется при облучении лазерным лучом вибрирующих под действием акустического речевого сигнала отражающих поверхностей помещений? +оптико-электронный (лазерный) канал -оптический (лазерный) канал -электронный канал -дуговой канал -блочный - лазерный канал 19. Что относится к пассивным средствам защиты информации? +Фильтры -Детекторы поля -Сканирующие приемники -Комплекс радио контроля -Нелинейные локаторы 20. Надежная защита от утечек информации за счет влияния побочных электромагнитных излучений и наводок (ПЭМИН) через цепи электропитания, заземления или по радио эфиру это? +генераторы белого шума -излучатели белого шума -блокираторы белого шума -кодеры -декодеры
***Умеет*:** анализировать и оценивать угрозы информационной безопасности объекта (ОПК-7); применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем (ПК-15); разработать комплекс мер по обеспечению информационной безопасности объекта в области технической защиты информации (ПСК-1);	1. Широкополосные генераторы радиошума, предназначенные для защиты от утечки информации за счет побочных электромагнитных излучений и наводок, а также подавления радио микрофонов и видео передатчиков ? +штора -SEL SP -Октава -Гром ЗИ -Соната 2. Генераторы белого шума, предназначенные для маскировки побочных электромагнитных излучений и наводок на линии электропитания и телефонной линии. +Гром ЗИ -Штора -SEL SP -Октава -Соната 3. Система технических средств и среда распространения сигналов для односторонней передачи данных от источника к получателю. +канал связи -канал передачи -средства защиты

	-блокиратор связи -де блокиратор связи 4. Какой скремблер обеспечивает более низкую степень защиты? +статический -аналоговый -цифровой -динамический -блочный 5. Как можно настраивать детектор поля при поиске ультра коротко волновых передатчиков? + изменение длины телескопической антенны -увеличение длины телескопической антенны -уменьшение длины телескопической антенны -изменение ширины телескопической антенны -уменьшение ширины телескопической антенны 6. При наличии хорошего электромагнитного детектора, оптимальный перехват иной раз удается выполнять на расстоянии? +10—80 см от телефонной линии -20-80 см от телефонной линии -30-70 см от телефонной линии -0-100 см от телефонной линии 7. Радио микрофон с дистанционным (кодовым) включением через любой телефон? +«электронное ухо» -«электронный микрофон» -«громкоговоритель» -«электронный приемник» 8. Средства аппаратной защиты, включающие средства защиты кабельной системы, систем электропитания относится к? + техническим мерам защиты и правовым мерам защиты -организационным мерам защиты - меры скрытия копирования участков магнитной ленты из ОЗУ в ПЗУ 9. Защита от сбоев серверов, рабочих станций и локальных компьютеров относится к? +Аппаратным и техническим средствам защиты -Программным средствам защиты -Средствам защиты идентификации и аутентификации - Организационным и общим средствам защиты 10. При наличии хорошего электромагнитного детектора, оптимальный перехват иной раз удается выполнять на расстоянии? +10—80 см от телефонной линии -20-80 см от телефонной линии -30-70 см от телефонной линии -0-100 см от телефонной линии 11. Как еще называют радиомикрофон с дистанционным (кодовым) включением через любой телефон? +«электронное ухо» -«электронный микрофон»

	-«громкоговоритель» -«электронный приемник» 12. Способы перехвата акустической утечки -визуальные методы, фотографирование, видео съемка, наблюдение; -Прямое копирование -Утечка информации вследствие несоблюдения коммерческой тайны; -информация на бумаге или других физических носителях информации +запись звука, подслушивание и прослушивание 13. Узконаправленные микрофон. - микрофон, действие которого основано на использовании свойств электрического конденсатора +разновидность конденсаторного микрофона - студийный микрофон - процессный преобразователь микрофона - процессный преобразователь микрофона электрического конденсатора 14. Потенциальные угрозы, против которых направлены технические меры защиты информации + Потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей - Потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения - Потери информации из-за не достаточной установки резервных систем электропитании и оснащение помещений замками. - Потери информации из-за не достаточной установки сигнализации в помещении. - Процессы преобразования, при котором информация удаляется 15. Какой технический канал утечки отвечает за распространение звуковых колебаний в любом звукопроводящем материале или среде? + Акустические и виброакустические - Электрические - Оптические - Радиоканалы 16. Какой технический канал утечки отвечает за напряжение и токи в различных токопроводящих коммуникациях?\ - Акустические и виброакустические + Электрические - Оптические - Радиоканалы 17. Какой технический канал утечки отвечает за электромагнитные излучения радиодиапазона? - Акустические и виброакустические - Электрические - Оптические + Радиоканалы 18. Какой технический канал утечки отвечает за

	электромагнитные излучения в видимой, инфракрасной и ультрафиолетовой частях спектра? - Акустические и виброакустические - Электрические + Оптические - Радиоканалы 19. В документах ФСТЭК России НЕ выделяется среди типовых технических каналов утечки канал утечки акустической информации канал утечки видовой информации канал побочных электромагнитных излучений и наводок канал цепи заземления 20. Транспондер - это радиозакладка с дистанционным управлением полуактивная радиозакладка радиозакладка с системой управления включением передатчика от голоса инфракрасная закладка сетевая закладка
***Имеет практический опыт*:** применения методов технической защиты информации (ОПК-7); формирования требований по защите информации (ПК-15); разработки комплекса мер по обеспечению информационной безопасности объекта в области технической защиты информации (ПСК-1).	1. Выбрать и определить основные технические средства защиты информации от наблюдения ,подслушивания и перехвата, которые намечаются для применения в системе ИТЗИ организации. 2. Для каждого технического средства определить его технические характеристики, показатели назначения, паспортные данные и.т.д. 3. Сравнить технические характеристики и данные выбранных технических средств с другими аналогичными средствами в данном классе, обосновать выбор данного вида и модели технического средства. 4. Оценить, насколько могут сократиться риски, определенные в лабораторной работе 7, в случае применения выбранных технических средств. Обосновать новую оценку риска.

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 Лабораторные 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. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам[Текст] / Г. А. Бузов. - М. : Горячая линия -Телеком, 2015. - 585 с. : ил.
2. 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.
3. Защита информации [Электронный ресурс] : учеб. пособие для вузов по направлению подгот. Инфокоммуникац. технологии и системы связи квалификации (степ.) "бакалавр" и квалификации (степ.) "магистр" / А. П. Жук [и др.]. - 2-е изд. - Документ HTML. - М. : РИОР [и др.], 2015. - 393 с. - Режим доступа: http://znanium.com/bookread.php?book=474838
4. Хорев, П. Б. Программно-аппаратная защита информации [Электронный ресурс] : учеб. пособие для вузов по направлению "Информ. безопасность" / П. Б. Хорев. - 2-е изд., испр. и доп. - Документ Bookread2. - М. : ФОРУМ, 2015. - 351 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=489084

Списки дополнительной литературы

5. Бузов, Г. А. Защита от утечки информации по техническим каналам [Текст] : учеб. пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. - М. : Горячая линия - Телеком, 2005. - 414 с. : ил.
6. Бузов, Г. А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации[Текст] : [справ. изд.] / Г. А. Бузов. - М. : Горячая линия - Телеком, 2010. - 237 с. : ил.
7. Виноградов, Ю. А. Охранная техника [Текст] / Ю. А. Виноградов. - М. : СОЛОН-Пресс, 2008. - 191 с. : ил.
8. 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.
9. Душин, В. К. Теоретические основы информационных процессов и систем [Текст] : учеб. для вузов по специальностям "Информ. системы и технологии", "Сервис БРЭА", "Информ. сервис", "Сервис компьютерной и микропроцессорной техники" / В. К. Душин. - 3-е изд. - М. : Дашков и К, 2009. - 348 с. : ил., схем.
10. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации [Текст] : учеб. пособие для студентов вузов по специальностям 090103 "Орг. и технология защиты информ.", 090104 "Комплексная защита объектов информатизации" / В. Я. Ищейнов, М. В. Мецатунян. - 2-е изд., перераб. и доп . - М. : Форум [и др.], 2014. - 255 с.
11. Кондратьев, А. В. Организация и содержание работ по выявлению и оценке основных видов ТКУИ, защита информации от утечки [Текст] : [справ. пособие] / А. В. Кондратьев. - М. : МАСКОМ, 2011. - 256 с. : ил. 16 с.
12. Контроль защищенности речевой информации в помещениях. Аттестационные испытания выделенных помещений по требованиям безопасности информации [Текст] : учеб. пособие по направлениям подгот. и специальностям укрупн. группы "Информ. безопасность" / В. С. Горбатов [и др.] под общ. ред. Ю. Н. Лаврухина. - М. : НИЯУ МИФИ, 2014. - 248 с. : ил.
13. Контроль защищенности информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок. Аттестационные испытания по

требованиям безопасности информации [Текст] : учеб. пособие по направлениям подгот. и специальностям укрупн. группы "Информ. безопасность" / А. А. Голяков [и др.] под общ. ред. Ю. Н. Лаврухина. - М. : НИЯУ МИФИ, 2014. - 208 с. : ил.
14. Мельников, В. П. Информационная безопасность и защита информации [Текст] : учеб. пособие для вузов по специальности "Информ. системы и технологии" / В. П. Мельников, А. М. Петраковпод ред. С. А. Клейменова. - 6-е изд., стер. - М. : Академия, 2012. - 336 с. : ил., табл.
15. Панин, В. В. Основы теории информации [Текст] : учеб. пособие для вузов по специальности "Электроника и автоматика физич. установок" / В. В. Панин. - 2-е изд., испр. и доп. - М. : БИНОМ. Лаб. знаний, 2007. - 436 с. : табл.
16. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей [Текст] : учеб. пособие для вузов по специальностям "Компьютерная безопасность", "Комплекс. обеспеч. информ. безопасности автоматизир. систем" / В. В. Платонов. - М. : Академия, 2006. - 239 с. : ил.
17. Семененко, В. А. Информационная безопасность[Текст] : учеб. пособие для вузов / В. А. СеменекоМоск. гос. индустр. ун-т. - 2-е изд., стер. - М. : МГИУ, 2005. - 215 с. : ил.
18. Технические средства и методы защиты информации [Текст] : учеб. пособие для вузов по специальностям "Компьютер. безопасность", "Комплекс. обеспеч. информ. безопасности автоматизир. систем", "Информ. безопасность телекоммуникац. систем" / А. П. Зайцев [и др.] под ред. А. П. Зайцева, А. А. Шелупанова. - 4-е изд., испр. и доп. - М. : Горячая линия - Телеком, 2009. - 615 с. : ил.
19. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства[Текст] : учеб. пособие для вузов по направлению "Информатика и вычисл. техника" / В. Ф. Шаньгин. - М. : ДМК Пресс, 2008. - 542 с. : ил.
20. Щербаков, А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты [Электронный ресурс] : электрон. учеб. пособие для вузов / А. Ю. Щербаков. - М. : Кн. мир, 2009. - 13,7 МБ. - CD-ROM.

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 лабораторных работ
3.	Internet Explorer? FireFox	Браузер.	Выполнение лабораторных 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 «Техническая защита информации»

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	Срок прохождения контрольных точек																	Итого	Зачетно - экзаменационная сессия
				сентябрь				октябрь					ноябрьь				декабрь					
				неделя				неделя					неделя				неделя					
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
I	**Обязательные:**																					
1.1	Лабораторная работа № 1.	1	4		+																	
1.2	Лабораторная работа № 2.	1	5				+															
1.3	Лабораторная работа № 3.	1	5						+													
1.4	Лабораторная работа № 4.	1	5								+											
1.5	Лабораторная работа № 5.	1	5										+									
1.6	Лабораторная работа № 6.	1	5												+							
1.7	Лабораторная работа № 7.	1	5														+					
1.8	Лабораторная работа № 8	1	5																+			
1.8	Лабораторная работа № 9	1	5																+			
1.8	Лабораторная работа № 10	1	5																+			
1.8	Лабораторная работа № 11	1	5																+			
1.9	Посещаемость лекций	16	1	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
																					70	
1.10	Курсовая работа	1	20															+			20	
	Итого:		90																		90	
2.	**Творческий рейтинг**																					
2.1	Участие в олимпиадах, конкурсах и т.д.	1	10															+			10	
	Итого:		100																		100	
III.	**Форма контроля**																	+				Экзамен