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 «Защита информационных процессов в компьютерных системах и телекоммуникационных сетях»
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 «Защита информационных процессов в компьютерных системах и телекоммуникационных сетях» разработана в соответствии с Федеральным государственным образовательным стандартом направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Минобрнауки РФ от 1 декабря 2016 г. N 1515.

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

Согласовано Директор научной библиотеки _____ В.Н.Еремина

Согласовано Начальник управления информатизации _____ В.В.Обухов

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

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

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

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

1.1. Цели освоения дисциплины

изучение студентами основных угроз информации в компьютерных системах; особенностей защиты информации на узлах компьютерной сети, требований к программной и программно-аппаратной реализации средств защиты информации, требований к защите автоматизированных систем от НСД.

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

проектно-технологическая деятельность:

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

эксплуатационная деятельность:

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

администрирование подсистем информационной безопасности объекта;

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.

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*:** принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; основы администрирования вычислительных сетей для выполнения задач	Лекции	Собеседование

программно-аппаратной защиты информации (ОПК-7).		
***Умеет*:** осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе, для выполнения задач программно-аппаратной защиты информации (ОПК-7).	Лабораторные работы	Защита лабораторных работ
***Имеет практический опыт*:** анализа сетевого трафика, результатов работы средств обнаружения вторжений. противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации (ОПК-7).	Решение разноуровневых и проблемных задач	Защита лабораторных работ

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к профессиональному циклу, базовой (общепрофессиональной) части.

Её освоение осуществляется: в 8 семестре.

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Код компетенции(й)
	Предшествующие дисциплины	
1.	Основы информационной безопасности	ОК-5, ОПК-7
2.	Аппаратные средства вычислительной техники	ПК-1, ПК-6

3.	Криптографическая защита информации	ОК-4, ОПК-7, ПК-1
4.	Техническая защита информации	ОПК-7, ПК-15, ПСК-1
5.	Программно-аппаратные средства защиты информации	ОПК-7, ПК-6

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

Распределение фонда времени по семестрам и видам занятий

Виды занятий	очная форма обучения	очно-заочная форма обучения	заочная форма обучения
8 семестр			
Итого часов Зачетных единиц	72 ч. 2 з.е.	72 ч. 2 з.е.	- -
Лекции (час)	16 ч.	2 ч.	-
Практические (семинарские) занятия (час)	-	-	-
Лабораторные работы (час)	20 ч.	6 ч.	-
Самостоятельная работа (час)	36 ч.	60 ч.	-
Курсовой проект (работа) (+,-)	-	-	-
Контрольная работа (+,-)	-	-	-
Экзамен, семестр/час.	-	4 ч.	-
Зачет, семестр	8 семестр	8 семестр	-
Контрольная работа, семестр	-	-	-

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

4.1. Содержание дисциплины

№ п/п	Раздел дисциплины	Виды учебных занятий, включая самостоятельную работу студентов и трудоемкость (в академических часах)				Средства и технологии оценки
		Лекции, час	Практические занятия, час	Лабораторные работы, час	Самостоятельная работа, час	
6 семестр						
1.	Тема 1. Основные угрозы информации в компьютерных системах.	2/1/-	-/-/-	2/2/-	4/8/-	Устный опрос, защита лабораторных работ
2.	Тема 2. Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера;	2/1/-	-/-/-	-/-/-	4/8/-	Устный опрос
3.	Тема 3. Специфика	2/1/-	-/-/-	2/2/-	6/10/-	Устный опрос,

	возникновения угроз в открытых сетях;					защита лабораторных работ
4.	Тема 4. Особенности защиты информации на узлах компьютерной сети;	2/1/-	-/-/-	6/-/-	6/10/-	Устный опрос, защита лабораторных работ
5.	Тема 5. Системные вопросы защиты программ и данных. Администрирование серверных систем и приложений.	2/-/-	-/-/-	4/2/-	6/8/-	Устный опрос, защита лабораторных работ
6.	Тема 6. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации. Использование межсетевых экранов для защиты информационных процессов.	4/-/-	-/-/-	4/-/-	6/8/-	Устный опрос, защита лабораторных работ
7.	Тема 7. Требования к защите автоматизированных систем от НСД.	2/-/-	-/-/-	2/2/-	4/8/-	Устный опрос, защита лабораторных работ
	Промежуточная аттестация по дисциплине	16/4/-	-/-/-	20/8/-	36/60/-	Зачет

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

4.2. Содержание лабораторных работ

№	Наименование лабораторных работ	Обьем часов	Наименование темы дисциплины
6 семестр			
1.	Лабораторная работа №1. Основные угрозы информации в компьютерных системах	2/2/-	Тема 1. Основные угрозы информации в компьютерных системах.
2.	Лабораторная работа №2. Специфика возникновения угроз в открытых сетях	2/2/-	Тема 3. Специфика возникновения угроз в открытых сетях;
3.	Лабораторная работа №3. Особенности защиты информации на узлах компьютерной сети с использованием криптографических методов	6/-/-	Тема 4. Особенности защиты информации на узлах компьютерной сети;
4.	Лабораторная работа №4. Администрирование серверных систем и приложений	4/2/-	Тема 5. Системные вопросы защиты программ и данных. Администрирование серверных систем и приложений.
5.	Лабораторная работа №5. Использование межсетевых экранов для защиты информационных процессов	4/-/-	Тема 6. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации. Использование межсетевых экранов для защиты информационных процессов.

6.	Лабораторная работа №6. Требования к защите автоматизированных систем от НСД	2/2/-	Тема 7. Требования к защите автоматизированных систем от НСД.
	Итого	20/8/-	

Примечание:
-/-/-, объем часов соответственно для очной, очно-заочной, 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	Объем часов
ОПК-7	Работа с литературой	Конспект	Собеседование	12/33/-
ОПК-7	Ответы на контрольные вопросы	Конспект	Тест	12/15/-
ОПК-7	Подготовка доклада на конференцию	Доклад	Опубликование тезисов доклада	12/12/-
			Итого	36/60/-

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

Содержание заданий для самостоятельной работы

Вопросы для самоконтроля

1. Основные угрозы информации в компьютерных системах.
2. Особенности построения систем защиты информации в зависимости от источника угроз.
3. Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера.
4. Специфика возникновения угроз в открытых сетях.
5. Особенности защиты информации на узлах компьютерной сети.
6. Системы обнаружения атак. Назначение, основные виды, особенности использования.
7. Использование мониторов безопасности повышения защищённости компьютерной системы.
8. Системные вопросы защиты программ и данных.
9. Политика информационной безопасности. Общая структура документа.
10. Особенности реализации политик безопасности в компьютерных системах.
11. Анализ и управление информационными рисками.
12. Причины возникновения и области ИТ рисков.
13. Организация и содержание работ по анализу рисков.
14. Методология OCTAVE для анализа и управления информационными рисками.
15. Администрирование серверных систем и приложений.
16. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации.
17. Система лицензирования и сертификации средств защиты. Аттестация защищенных систем. Структуры в РФ, обеспечивающие лицензирование и сертификацию.
18. Нормативная база и ответственность за защиту информации в компьютерных системах.

19. Руководящий документ Гостехкомиссии по оценке защищенности АС.
20. Американские стандарты по защите информации «Розовая книга». Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».
21. Европейский стандарт по безопасности. ITSEC. Функциональные требования. Вопросы гарантий и эффективности.
22. 0бщие критерии оценки защищенности информационных технологий (Common Criteria (CC). Подход к безопасности компьютерных систем в CC и базовые концепции. Профиль защиты.
23. Использования шифрования для повышения защищённости компьютерных систем.
24. Использование криптографического хэширования для контроля целостности программ и данных
25. Межсетевые экраны. Назначение, основные виды, особенности использования. Использование межсетевых экранов для защиты информационных процессов.
26. Виртуальные частные сети. Назначение, основные виды, особенности использования.
27. Механизмы защиты баз данных. Разграничение доступа. Механизм ролей.
28. Обеспечение надёжности баз данных. Особенности резервного копирования. Журналирование изменений.
29. Организация информационной безопасности в Microsoft SQL Server. Общие сведения.
30. Схемы и роли в Microsoft SQL Server. Управление доступом с применением схем и ролей в Microsoft SQL Server.
31. Использование представлений и хранимых процедур для обеспечения безопасного доступа в Microsoft SQL Server.
32. Сравнение механизмов безопасности СУБД SQL Server и Oracle.
33. Требования к защите автоматизированных систем от НСД.
34. Использование средств разграничения доступа для повышения защищённости компьютерных систем.
35. Биометрические системы аутентификации пользователей
36. Уязвимости платформы Windows. Переполнение буфера. Сплайсинг функций.

6. Методические указания для обучающихся по освоению дисциплины

Инновационные образовательные технологии

Вид образовательных технологий, средств передачи знаний, формирования умений и практического опыта	№ темы / тема лекции	№ практического (семинарского) занятия/наименование темы	№ лабораторной работы / цель
Слайд-лекция	Тема 1. Основные угрозы информации в компьютерных системах.		

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 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 лабораторных работах

Лабораторные работы

№	Наименование лабораторной работы	Задания по лабораторной работе
6 семестр		
1.	Лабораторная работа №1. Основные угрозы информации в компьютерных системах	1. По согласованию с преподавателем определить исходные данные: 2. Определить основные виды объектов защиты для данного предприятия. Для каждого вида объектов привести конкретные примеры. Объекты защиты выбирать в составе оборудования, инфраструктуры, персонала предприятия. 3. Определить основные виды угроз и способов их реализации для основных объектов защиты для заданного предприятия. 4. Для каждого вида угроз определить основные способы и средства предотвращения угроз. 5. Сформулировать основные элементы системы инженерно-технической защиты информации для заданного предприятия..
2.	Лабораторная работа №2. Специфика возникновения угроз в открытых сетях	1. Перечислите и охарактеризуйте стандартные правила, определяющие параметры сессии сканирования. На базе одного из них создайте собственное правило. 2. Проведите сканирование указанных преподавателем компьютеров в учебной лаборатории. 3. Опишите результаты проверки.
3.	Лабораторная работа №3.	1. Работая под первой учетной записью,

	Особенности защиты информации на узлах компьютерной сети с использованием криптографических методов	запросите сертификат (если он не был получен ранее), после чего зашифруйте папку с тестовым файлом. 2. Убедитесь, что другой пользователь не сможет прочитать зашифрованный файл. 3. Снова зайдите под первой учетной записью. В оснастке Certificates, удалите сертификат пользователя. Завершите сессию пользователя в системе и войдите заново. Попробуйте открыть зашифрованный файл.
4.	Лабораторная работа №4. Администрирование серверных систем и приложений	1. Получите перечень компьютеров и контроллеров домена. Для 1-2 компьютеров выясните установленную операционную систему и используемые ими ip-адреса. 2. Получите перечень предоставляемых в общий доступ каталогов на вашем компьютере и на компьютерах, данные о которых Вы собирали на этапе 1. Опишите хранимые там данные и охарактеризуйте степень их важности. 3. Для указанных ресурсов и выбранных пользователей опишите действующие разрешения на доступ.
5.	Лабораторная работа №5. Использование межсетевых экранов для защиты информационных процессов	Откройте окно управления межсетевым экраном. Опишите действующие настройки. Создайте новое разрешающее правило.
6.	Лабораторная работа №6. Требования к защите автоматизированных систем от НСД	Работая под учетной записью Administrator, создадим новую папку Test. Выполните переключение пользователей. Удалите группу Users из ACL для папки. Проверьте действующее эффективное разрешение. Выполните передачу права владения группе TestGroup.

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 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.
ОПК-7	*текущий*	*устный опрос*	*1-46*
ОПК-7	*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*:** принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; основы администрирования вычислительных сетей для выполнения задач программно-аппаратной защиты информации (ОПК-7).	1. Кто является основным ответственным за определение уровня классификации информации? A. Руководитель среднего звена. B. Высшее руководство. C. Владелец. D. Пользователь. 2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? A. Сотрудники. B. Хакеры. C. Атакующие. D. Контрагенты (лица, работающие по договору). 3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству? A. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования. B. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации. C. Улучшить контроль за безопасностью этой информации. D. Снизить уровень классификации этой информации. 4. Что самое главное должно продумать руководство при классификации данных? A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным. B. Необходимый уровень доступности, целостности и конфиденциальности. C. Оценить уровень риска и отменить контрмеры.

	D. Управление доступом, которое должно защищать данные. 5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены? A. Владельцы данных. B. Пользователи. C. Администраторы. D. Руководство. 6. Что такое процедура? A. Правила использования программного и аппаратного обеспечения в компании. B. Пошаговая инструкция по выполнению задачи. C. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах. D. Обязательные действия. 7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании? A. Поддержка высшего руководства. B. Эффективные защитные меры и методы их внедрения. C. Актуальные и адекватные политики и процедуры безопасности. D. Проведение тренингов по безопасности для всех сотрудников. 8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков? A. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски. B. Когда риски не могут быть приняты во внимание по политическим соображениям. C. Когда необходимые защитные меры слишком сложны. D. Когда стоимость контрмер превышает ценность актива и потенциальные потери. 9. Что такое политики безопасности? A. Пошаговые инструкции по выполнению задач безопасности. B. Общие руководящие требования по достижению определенного уровня безопасности. C. Широкие, высокоуровневые заявления руководства. D. Детализированные документы по обработке инцидентов безопасности. 10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер? A. Анализ рисков. B. Анализ затрат / выгоды. C. Результаты ALE. D. Выявление уязвимостей и угроз, являющихся причиной риска.

***Умеет*:** осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе, для выполнения задач программно-аппаратной защиты информации (ОПК-7).	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..
***Имеет практический опыт*:** анализа сетевого трафика, результатов работы средств обнаружения вторжений. противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации (ОПК-7).	1. Перечислите и охарактеризуйте стандартные правила, определяющие параметры сессии сканирования. На базе одного из них создайте собственное правило. 2. Проведите сканирование компьютеров в учебной лаборатории. 3. Опишите результаты проверки.

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. 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
2. Каратунова, Н. Г. Защита информации. Курс лекций [Электронный ресурс] : учеб.-метод. пособие / Н. Г. КаратуноваКубан. соц.-экон. ин-т, Каф. математики и информатики. - Документ Bookread2. - Краснодар : Кубан. соц.-экон. ин-т, 2014. - 188 с. - Режим доступа: http://znanium.com/bookread2.php?book=503511
3. Никифоров, С. Н. Методы защиты информации. Защищенные сети [Электронный ресурс] : учеб. пособие / С. Н. Никифоров. - Документ Reader. - СПб. [и др.] : Лань, 2018. - 94 с. - Режим доступа: https://e.lanbook.com/reader/book/110935/#1
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
5. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс] : учеб. пособие для вузов по направлению 09.03.01 "Информатика и вычисл. техника" / В. Ф. Шаньгин. - Документ Bookread2. - М. : ФОРУМ [и др.], 2018. - 592 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=937502

Списки дополнительной литературы

6. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Текст] : учеб. пособие для вузов по специальностям "Компьютер. безопасность", "Комплекс. обеспечение информ. безопасности автоматизир. систем" / А. А. Афанасьев [и др.] под ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. - М. : Горячая линия - Телеком, 2009. - 550 с.
7. Башлы, П. Н. Информационная безопасность[Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Документ Bookread2. - М. : РИОР, 2013. - 222 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=405000#
8. Введение в информационную безопасность[Текст] : учеб. пособие для вузов / А. А. Малюк [и др.] под ред. В. С. Горбатова. - М. : Горячая линия - Телеком, 2011. - 288 с. : ил.
9. Грибунин, В. Г. Комплексная система защиты информации на предприятии [Текст] : учеб. пособие для вузов по специальностям "Орг. и технология защиты информ.", "Комплекс. защита объектов информатизации" / В. Г. Грибунин, В. В. Чудовский. - М. : Академия, 2009. - 412 с. : ил., табл.
10. Грушо, А. А. Теоретические основы компьютерной безопасности [Текст] : учеб. пособие для вузов по специальности "Информ. безопасность" / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. - М. : Академия, 2009. - 268 с. : ил.
11. Защита информации. Система стандартов. Основные положения [Электронный ресурс] : ГОСТ Р 52069.0-2013 : нац. стандарт РФ : введ. 2013-09-01 Федер. агентство по техн. регулированию и метрологии. - Документ Adobe Acrobat. - М. : [б. и.], 2014. - 939 КБ, 12 с. : схем. - Режим доступа: http://elib.tolgas.ru
12. Малюк, А. А. Теория защиты информации [Текст] / А. А. Малюк. - М. : Горячая линия - Телеком, 2013. - 184 с. : табл.

13. Олифер, В. Г. Безопасность компьютерных сетей[Текст] / В. Г. Олифер, Н. А. Олифер. - М. : Горячая линия -Телеком, 2016. - 644 с. : ил.
14. Платонов, В. В. Программно-аппаратные средства защиты информации [Электронный ресурс] : учеб. для вузов по направлению подгот. "Информ. безопасность" / В. В. Платонов. - Документ Adobe Acrobat. - М. : Академия, 2013. - 63,7 МБ, 332 с. : ил., табл. - Режим доступа: http://elib.tolgas.ru
15. Проскурин, В. Г. Защита программ и данных[Текст] : учеб. пособие для вузов по направлению подгот. "Информ. безопасность" (бакалавр) и специальностям: "Компьютер. безопасность", "Информ. безопасность автоматизир. систем" / В. Г. Проскурин. - М. : Академия, 2012. - 208 с. : ил.
16. 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.
17. Хорев, П. Б. Программно-аппаратная защита информации [Текст] : учеб. пособие для вузов по направлениям "Информ. безопасность" и "Информатика и вычисл. техника" / П. Б. Хорев. - М. : ФОРУМ, 2009. - 351 с. : ил.
18. 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.
19. Лабораторный практикум по дисциплине "Защита информационных процессов в компьютерных системах и и телекоммуникационных сетях"[Электронный ресурс] : 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. - Документ Adobe Acrobat. - Тольятти : ПВГУС, 2016. - 2,17 МБ, 84 с. - Режим доступа: http://elib.tolgas.ru.

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 лабораторным работам
2.	Microsoft Windows	Операционная система	Выполнение лабораторных работ

3.	Internet Explorer, Mozilla Firefox, Opera, Chrome	Браузер	Выполнение лабораторных работ
4.	Windows Server, Microsofr ISA сервер, ОС Linux Server	Операционная система	Выполнение лабораторных работ
6.	WireShark	Сетевой снифффер	Выполнение лабораторных работ
7.	GPG или аналог	Программный пакет	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 «Защита информационных процессов в компьютерных системах и телекоммуникационных сетях»

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 лабораторных работ	6	12			+		+		+		+		+		+				
2.	Дополнительные задания:																			
2.1.	Доклад на научной конференции	1	8															+		
2.2	Публикация научной статьи	1	20															+		
	Форма контроля																		+	Зачет