

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 03.02.2022 15:17:47
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

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

Кафедра Информационный и электронный сервис

РАБОЧАЯ УЧЕБНАЯ ПРОГРАММА

по дисциплине Методы и средства защиты компьютерной техники

для студентов направления подготовки
09.03.04 «Программная инженерия»
направленности (профиля) «Разработка программно-информационных систем»

Тольятти 2018 г.

Рабочая учебная программа по дисциплине «Методы и средства защиты компьютерной техники» включена в основную профессиональную образовательную программу направления подготовки 09.03.04 «Программная инженерия» направленности (профиля) «Разработка программно-информационных систем» решением Президиума Ученого совета

Протокол № 4 от 28.06.2018 г.

Начальник учебно-методического отдела _____  Н.М.Шемендю
28.06.2018 г.

Рабочая учебная программа по дисциплине «Методы и средства защиты компьютерной техники» разработана в соответствии с Федеральным государственным образовательным стандартом направления подготовки 09.03.04 «Программная инженерия» утвержденный приказом Министерства образования и науки Российской Федерации от 12 марта 2015 г. N 229

Составил: к.т.н., доцент Г.П. Жуков

СОГЛАСОВАНО:

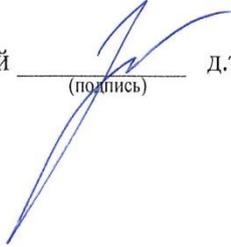
Директор научной библиотеки  В.Н.Еремина

СОГЛАСОВАНО:

Начальник управления информатизации  В.В.Обухов

Рабочая программа утверждена на заседании кафедры «Информационный и электронный сервис»

Протокол № 11 от «27» июня 2018 г.

Заведующий кафедрой 
(подпись) д.т.н., профессор В.И. Воловач

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

Целями освоения дисциплины являются: изучение основных понятий и определений защиты информации; источников риска и форм атак на компьютерную информацию; политики безопасности и законодательно – правовые и организационные методы защиты компьютерной информации; изучение методов и средств защиты компьютерной информации.

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

производственно-технологическая деятельность:

- использование типовых методов для контроля, оценки и обеспечения качества программной продукции;
- обеспечение соответствия разрабатываемого программного обеспечения и технической документации российским и международным стандартам, техническим условиям, ведомственным нормативным документам и стандартам предприятия.

1.3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины у обучающихся формируются следующие компетенции:

Код компетенции	Наименование компетенции
1	2
ПК-4	владением концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества

1.4. Перечень планируемых результатов обучения по дисциплине

Результаты освоения дисциплины	Технологии формирования компетенции по указанным результатам	Средства и технологии оценки по указанным результатам
<p>Знает: концепции и атрибуты качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества (ПК-4)</p>	<p><i>Лекции</i></p>	<p><i>Собеседование, опрос, оценка</i></p>
<p>Умеет: разрабатывать концепции и атрибуты качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества (ПК-4)</p>	<p><i>Лабораторные работы</i></p>	<p><i>Защита лабораторных работ, оценка</i></p>
<p>Имеет практический опыт: разработки концепции и атрибутов качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества (ПК-4).</p>	<p><i>Лабораторные работы</i></p>	<p><i>Защита лабораторных работ, оценка</i></p>

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам по выбору.

Ее освоение осуществляется в 7 (очная форма) / 8 (заочная форма) / 9 (заочная форма (февраль)) семестрах.

№	Наименование дисциплин, определяющих	Код компетенции(й)
---	--------------------------------------	--------------------

п/п	междисциплинарные связи	
	Предшествующие дисциплины	
1	Информатика	ОПК-4
	Последующие дисциплины	
3	Сети и телекоммуникации	ПК-2

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	заочная форма обучения (февраль)	заочная форма обучения
Итого часов	<u>144</u> ч.	<u>144</u> ч.	<u>144</u> ч.
Зачетных единиц	<u>4</u> з.е.	<u>4</u> з.е.	<u>4</u> з.е.
Лекции (час)	18	4	4
Практические (семинарские) занятия (час)	-	-	-
Лабораторные работы (час)	30	10	10
Самостоятельная работа (час)	69	121	121
Курсовой проект (работа) (+,-)	-	-	-
Контрольная работа (+,-)	-	-	-
Экзамен, семестр /час.	7/27	9/9	8/9
Зачет (дифференцированный зачет), семестр	-	-	-
Контрольная работа, семестр	-	-	-

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

4.1. Содержание дисциплины

№ п/п	Раздел дисциплины	Виды учебных занятий, включая самостоятельную работу студентов и трудоемкость (в академических часах)				Средства и технологии оценки
		Лекции, час	кисе (семинарские) занятия	Лабораторные работы, час	Самостоятельная работа, час	
1	Основы информационной безопасности. Основные нормативно - правовые руководящие документы.	4/0,5/0,5	-/-/-	-/-/-	14/20/20	Конспект

	Стандарты информационной безопасности. Лицензирование и сертификация в области информационной безопасности					
2	Угрозы информации. Компьютерные преступления	2/0,5/0, 5	-/-/-	4/2/2	10/20/20	Конспект, защита лабораторны х работ
3	Виды возможных нарушений компьютерных информационных систем	4/1/1	-/-/-	8/2/2	10/20/20	Конспект, защита лабораторны х работ
4	Информационная безопасность операционных и информационных систем	4/1/1	-/-/-	14/4/4	10/20/20	Конспект, защита лабораторны х работ
5	Методы и средства защиты компьютерной информации	2/1/1	-/-/-	-/-/-	10/20/20	Конспект, защита лабораторны х работ
6	Организация информационной безопасности компании. Анализ политики информационной безопасности компании. Управление средствами информационной безопасности компании. Управление обновлениями программных средств. Разграничение доступа к сетевому оборудованию. Аудит и мониторинг компьютерной информационной безопасности.	2/-/-	-/-/-	4/2/2	15/21/21	Конспект, защита лабораторны х работ
	Аттестация по дисциплине	18/4/4	-/-/-	30/10/10	69/121/1 21	Экзамен

Примечание:

-/-/-, объем часов соответственно для очной формы обучения, заочной формы обучения (февраль), заочной формы обучения

4.2.Содержание практических (семинарских) занятий

Практические работы учебным планом не предусмотрены

4.3.Содержание лабораторных работ

№	Наименование лабораторных работ	Объем	Наименование темы
---	---------------------------------	-------	-------------------

		часов	дисциплины
1	Лабораторная работа 1. Политика и стандарты безопасности. Законодательно – правовые и организационные методы защиты компьютерной информации	4/2/2	Угрозы информации. Компьютерные преступления.
2	Лабораторная работа 2. Криптографические методы защиты информации. Алгоритмы шифрования	8/2/2	Виды возможных нарушений компьютерных информационных систем
3	Лабораторная работа 3. Методы и средства защиты информации от несанкционированного доступа. Алгоритмы аутентификации пользователей	14/2/2	Информационная безопасность операционных и информационных систем
4	Лабораторная работа 4. Требования к системам защиты информации. Многоуровневая защита корпоративных сетей. Защита информации в сетях. Построение комплексных систем защиты информации	4/2/2	Организация информационной безопасности компании. Анализ политики информационной безопасности компании. Управление средствами информационной безопасности компании. Управление обновлениями программных средств. Разграничение доступа к сетевому оборудованию. Аудит и мониторинг компьютерной информационной безопасности.
	Итого	30/10/10	

Примечание:

–/–/–, объем часов соответственно для очной формы обучения, заочной формы обучения (февраль), заочной формы 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
1	2	3	4	5
ПК-4	Выполнение индивидуальных заданий в виде доклада и презентации на заданную тему.	Доклад, презентация	Собеседование	69/121/121
Итого				69/121/121

Примечание:

–/–/–, объем часов соответственно для очной формы обучения, заочной формы обучения (февраль), заочной формы обучения

Рекомендуемая литература

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>.

Содержание заданий для самостоятельной работы

Темы рефератов

1. Информационная безопасность РФ.
2. Компьютерные преступления.
3. Антивирусные программные средства
4. Алгоритмы шифрования.

Письменные работы могут быть представлены в различных формах:

- реферат - письменный доклад или выступление по определённой теме, в котором собрана информация из одного или нескольких источников. Рефераты могут являться изложением содержания научной работы, художественной книги и т. п.
- другое.

Вопросы (тест) для самоконтроля

1. Классификация угроз безопасности компьютерным системам.
2. Кто осуществляет общее руководство системой информационной безопасности в РФ
3. Назовите Законы РФ о защите информации.
4. Назовите криптографические методы защиты информации.
5. Защита компьютерной информации с помощью сервисного программного обеспечения.

Индивидуальные (групповые) задания для самостоятельной работы

1. Построить комплексную схему защит информации объекта
2. Выполнить принципиальную схему многоуровневной комплексной системы защиты информации
3. Выполнить защиту документа MS Word (MS Excel) паролем.

6. Методические указания для обучающихся по освоению дисциплины

Иновационные образовательные технологии

Вид образовательных технологий,	№ темы / тема лекции	№ практического (семинарского) занятия/наименовани	№ лабораторной работы / цель

средств передачи знаний, формирования умений и практического опыта		е темы	
Слайд-лекции	<p>1/Основы информационной безопасности. Основные нормативно - правовые руководящие документы. Стандарты информационной безопасности. Лицензирование и сертификация в области информационной безопасности</p> <p>2/Угрозы информации. Компьютерные преступления</p> <p>3/Виды возможных нарушений компьютерных информационных систем</p> <p>4/Информационная безопасность операционных и информационных систем</p> <p>5/Методы и средства защиты компьютерной информации</p> <p>6/Организация информационной безопасности компании. Анализ политики</p>	-	<p>1/ закрепить знания о Российском законодательстве по защите компьютерной информации. Изучить компьютерные преступления</p> <p>2/ освоить основы криптографических методов защиты информации. Алгоритмы шифрования</p> <p>3/ освоить основы работы в программе шифрования, Методы и средства защиты информации от несанкционированного доступа. Алгоритмы аутентификации пользователей</p> <p>4/ получить практический навык выполнения исследования и разработки способов комплексной защиты информации</p>

	информационной безопасности компании. Управление средствами информационной безопасности компании. Управление обновлениями программных средств. Разграничение доступа к сетевому оборудованию. Аудит и мониторинг компьютерной информационной безопасности.		
--	--	--	--

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 компетенции и оценка текущей успеваемости по дисциплине. По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации, если это предусмотрено технологической картой дисциплины. Списки учебных пособий, научных трудов, которые студентам следует прочесть и законспектировать, темы лабораторных работ и вопросы к ним, вопросы к экзамену и другие необходимые материалы указаны в разработанном для данной дисциплины учебно-методическом комплексе.

Основной формой освоения дисциплины является контактная работа с преподавателем - лекции, лабораторные работы, консультации (в том числе индивидуальные), в том числе проводимые с применением дистанционных технологий.

По дисциплине часть тем (разделов) изучается студентами самостоятельно. Самостоятельная работа предусматривает подготовку к аудиторным занятиям, выполнение заданий (письменных работ, творческих проектов и др.) подготовку к промежуточной аттестации (экзамену).

На лекционных занятиях и лабораторных работах 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

Содержание заданий для практических занятий
Практические занятия по дисциплине учебным планом не предусмотрена
Лабораторные работы

№	Наименование лабораторных работ	Задание по лабораторным работам
1	Российское законодательство по защите компьютерной информации. Компьютерные преступления	1. Основные понятия защиты компьютерной информации. 2. Компьютерные преступления и особенности их раскрытия. 3. Законодательство РФ в области информационной безопасности
2	Криптографические методы защиты информации. Алгоритмы шифрования	1. Криптографические методы защиты информации. 2. Зашифровать заданный текст.
3	Методы и средства защиты информации от несанкционированного доступа. Алгоритмы аутентификации пользователей	1. Исследование способов комплексной защиты информации. Построение комплексных систем защиты информации 2. Оценка эффективности компьютерных средств защиты информации
4	Требования к системам защиты информации. Многоуровневая защита корпоративных сетей. Защита информации в сетях. Построение комплексных систем защиты информации	1. Общие положения о системе защиты информации . 2. Концепция создания комплексной системы защиты информации. 3. Выбор и разработка комплексной системы защиты информации.

Лабораторные работы обеспечивают:

формирование умений и навыков обращения с приборами и другим оборудованием, 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 (проектов)

Курсовая работа (проект) по дисциплине учебным планом не предусмотрена.

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

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

Код оцениваемой компетенции (или ее части)	Тип контроля	Вид контроля	Количество элементов
ПК-4	<i>текущий</i>	<i>устный опрос</i>	<i>1-20</i>
ПК-4	<i>Промежуточный</i>	<i>компьютерный тест</i>	<i>1-80</i>

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

Результаты освоения дисциплины	Оценочные средства (перечень вопросов, заданий и др.)
<i>Знает: ПК-4</i> концепции и атрибуты качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества	<ol style="list-style-type: none"> 1. Кто в РФ осуществляет общее руководство системой информационной безопасности 2. В каком году был принят закон РФ «Об информации, информационных технологиях и о защите информации» 3. Аутентификация субъекта — это 4. Как классифицируются угрозы безопасности информационным системам 5. Политика безопасности - это 6. Алгоритмы криптографического преобразования информации - это 7. Доступ к информации различают 8. Санкционированный доступ к информации — это 9. Несанкционированный доступ к информации характеризуется 10. Угрозы безопасности ИС по природе возникновения бывают 11. Идентификация субъекта — это 12. Защищенная система — это 13. Субъект доступа к информации — это 14. Санкционированный доступ к информации — это

	<p>15. Несанкционированный доступ к информации характеризуется</p> <p>16. Ответственным за защиту компьютерной системы от несанкционированного доступа к информации является</p> <p>17. В РФ какая существует ответственность за неправомерный доступ к компьютерной информации</p>
<p>Умеет: ПК-4 разрабатывать концепции и атрибуты качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества.</p>	<p>18. Пользоваться парольной системой защитой компьютерной информации.</p> <p>19. Выполнить принципиальную схему многоуровневной комплексной системы защиты информации</p> <p>20. Выполнить защиту документа MS Word (MS Excel) паролем.</p>
<p>Имеет практический опыт: ПК-4 разработки концепции и атрибутов качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества.</p>	<p>21. Создания резервных копий документов.</p> <p>22. Построить комплексную схему защит информации объекта</p> <p>23. Выполнить защиту документа MS Word (MS Excel) паролем.</p>

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 на различных этапах их формирования, 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		
<i>Уровневая шкала оценки компетенций</i>	<i>100 балльная шкала, %</i>	<i>100 балльная шкала, %</i>	<i>5-балльная шкала, дифференцированная оценка/балл</i>	<i>недифференцированная оценка</i>
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. Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] : учеб. пособие / С. А. Нестеров. - Изд. 4-е, стереотип. - Документ Reader. - СПб. [и др.] : Лань, 2018. - 321 с. - Режим доступа: <https://e.lanbook.com/reader/book/103908/#1>.
3. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование [Электронный ресурс] : учеб. пособие / С. Н. Никифоров. - Документ Reader. - СПб. [и др.] : Лань, 2018. - 120 с. - Режим доступа: <https://e.lanbook.com/reader/book/107307/#1>.
4. Никифоров, С. Н. Методы защиты информации. Шифрование данных [Электронный ресурс] : учеб. пособие / С. Н. Никифоров. - Документ Reader. - СПб. [и др.] : Лань, 2018. - 158 с. - Режим доступа: <https://e.lanbook.com/reader/book/106734/#1>.

Дополнительная литература

5. Баранова, Е. К. Информационная безопасность и защита информации [Электронный ресурс] : учеб. пособие по направлению «Приклад. информатика» / Е. К. Баранова, А. В. Бабаш. – 3-е изд., перераб. и доп. - Документ Bookread2. - М. : РИОР [и др.], 2017. - 324 с. - Режим доступа: <http://znanium.com/bookread2.php?book=763644>.
6. 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. - Слов. терминов. - Режим доступа: <http://znanium.com/bookread2.php?book=405000#>. - ISBN 978-5-369-001178-2.

7. Задачи и цели сетевого администрирования, понятие о сетевых протоколах и службах [Электронный ресурс] : лекция. - Режим доступа: <http://www.intuit.ru/studies/courses/991/216/lecture/5559>.
8. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах [Текст] : учеб. пособие для вузов по направлению "Информатика и вычисл. техника" / П. Б. Хорев. - 3-е изд., стер. - М. : Академия, 2007. - 255 с. : ил.

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

Интернет-ресурсы

1. ИНТУИТ. Национальный Открытый Университет [Электронный ресурс]. – Режим доступа: <http://www.intuit.ru/>. – Загл. с экрана.
2. Компьютерные атаки и технологии их обнаружения [Электронный ресурс]. – Режим доступа: <http://www.web-protect.net/attack.htm>. - Загл. с экрана.
3. Пароли для профессионалов [Электронный ресурс]. – Режим доступа: <http://kraytek.ru/bezopasnost/paroli-profi>. - Загл. с экрана.
4. Электронная библиотечная система Поволжского государственного университета сервиса [Электронный ресурс]. - Режим доступа: <http://elib.tolgas.ru/>. - Загл. с экрана.
5. 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 (при необходимости)

Краткая характеристика применяемого программного обеспечения

№ п/п	Программный продукт	Характеристика	Назначение при освоении дисциплины
1	Операционная система Microsoft Windows	Microsoft Windows Server Microsoft Windows Server (кодовое имя «Longhorn Server») версия серверной операционной системы производства компании Microsoft.	<i>Выполнение и оформление отчета лабораторных работ</i>
2	Пакет Microsoft Office (MS Word, MS Excel, MS PowerPoint).	Microsoft Office . Пакет обеспечивает совместимости можно использовать имеющиеся версии Word, Excel и PowerPoint для открытия, изменения и сохранения файлов в новых форматах Word, Excel и PowerPoint.	<i>Выполнение и оформление отчета лабораторных работ</i>
3	Программа шифрования	Программа позволяет выполнять операции шифрования и цифровой подписи сообщений, файлов и другой информации, представленной в электронном виде, в том числе прозрачное	<i>Выполнение и оформление отчета лабораторных работ</i>

		шифрование данных на запоминающих устройствах.	
4	Браузер Internet Explorer	Программу-браузер разрабатывала корпорация Microsoft. Входила в комплект операционных систем семейства Windows вплоть до Windows.	<i>Выполнение и оформление отчета лабораторных работ</i>
5	Программа архиватор	Создание архивов, их обновление и проверка целостности (тестирование). Распаковка архивов, а также также (разделённых на части файлов).	<i>Выполнение и оформление отчета лабораторных работ</i>
6	Программа резервного копирования данных	обладает всеми необходимыми для подавляющего большинства частных пользователей и небольших компаний функциями. Программа обеспечивает защиту информации. – универсальная программа, осуществляющая резервное копирование.	<i>Выполнение и оформление отчета лабораторных работ</i>

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 используются учебные аудитории, оснащенные персональными компьютерами с операционной системой Microsoft Windows; пакетом Microsoft Office; ПО для архивирования данных, резервного копирования данных.

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 «Методы и средства защиты компьютерной информации»

Факультет информационно-технического сервиса

кафедра «Информационный и электронный сервис»

направление подготовки 09.03.04 «Программная инженерия»

направленности (профиля) «Разработка программно-информационных систем»

№	Виды контрольных точек	Кол-во контрольных точек	Количество баллов за 1 контрольную точку	Срок прохождения контрольных точек																	Зачетно - экзаменационная сессия
				сентябрь				октябрь					ноябрь				декабрь				
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
I	Обязательные:																				
1.1.	Посещение лекций	9	1		+	+	+	+	+	+	+	+	+								
1.2.	Вып. лабораторные раб.	4	12				+		+							+		+			
1.3.	Промежуточное тестирование	1	5									+									
1.4.	Итоговое тестирование	1	8															+			
	Творческий рейтинг																				
1.5.	Написание творческ. раб.	1	до 10															+			
1.6.	Участ.в олимп., конк. и т.д.	1	10																+		
1.7.	Индивидуальная работа	1	до 10												+						
II.	Форма контроля												к.н.							ЭКЗ	

