МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
"Курский государственный университет"

Кафедра информационной безопасности

УТВЕРЖДЕНО

протокол заседания
Ученого совета от 24.04.2017 г., №10

Рабочая программа дисциплины
Криптографические протоколы

Направление подготовки: 10.03.01 Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Квалификация: бакалавр

Факультет физики, математики, информатики

Форма обучения: очная

Общая трудоемкость 5 ЗЕТ

Виды контроля в семестрах:
экзамен(ы) 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	9			
Вид занятий	УП	РП	УП	РП
Лекции	36	36	36	36
Лабораторные	36	36	36	36
В том числе инт.	8	8	8	8
Итого ауд.	72	72	72	72
Контактная работа	72	72	72	72
Сам. работа	72	72	72	72
Часы на контроль	36	36	36	36
Итого	180	180	180	180

Курск 2017

Рабочая программа дисциплины Криптографические протоколы / сост. ; Курск. гос. ун-т. - Курск, 2017. - с.

Рабочая программа составлена в соответствии со стандартом, утвержденным приказом Минобрнауки России от 1 декабря 2016 г. № 1515 "Об утверждении ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата)" (Зарегистрировано в Минюсте России 20 декабря 2016 г. № 44821)

Рабочая программа дисциплины "Криптографические протоколы" предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность профиль Безопасность компьютерных систем

Составитель(и):

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Ознакомление студентов с основными понятиями теории криптографических протоколов; овладение основными идеями и методами современной теории криптографических протоколов; ознакомление студентов с основными криптографическими протокола распределения ключей, протоколами аутентификации, различными промежуточными и более развитыми протоколами; развитие навыка построения криптографического протокола из элементарных протоколов, и развития логического мышления в рамках этой задачи; овладение навыком разложения любого криптографического протокола на промежуточные с целью создания программного обеспечения, обслуживающего исполнение протокола. Овладение основными идеями и методами классической и современной криптографии, зна- комство со средствами криптографической защиты информации, знание основополагающих документов в области защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.Б

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ОПК-7: Способностью определять информационные ресурсы , подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объектов защиты
Знать:
профессиональные функции в соответствии с направлением и профилем подготовки
теоретические основы исследования информационных процессов предприятий, организаций, их классификацию
Правила установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы информационной безопасности по установленным требованиям
Уметь:
Производить сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности
администрирование подсистем информационной безопасности объекта;
выполнять вычислительные эксперименты с использованием стандартных программных средств для реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объектов защиты
Владеть:
Методикой сбора и анализа исходных данных для проектирования систем защиты информации и определение требований, а так же сравнительный анализ подсистем по показателям информационной безопасности
Методом проведения администрирования подсистем информационной безопасности объекта
Навыками позволяющими выполнять вычислительные эксперименты с использованием стандартных программных средств для реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объектов защиты

ПСК-1.4: Способностью проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей
Знать:
Основные угрозы компьютерных систем систем
основные понятия и базовые содержательные положения информационной безопасности и защиты информации
современную доктрину информационной безопасности её цели и принципы защиты информации.
Уметь:
Проводить сбор и анализ исходных данных для проектирования систем защиты информации.
Проводить сравнительный анализ подсистем по показателям информационной безопасности
Проведить вычислительные эксперименты с использованием стандартных программных средств;
Владеть:
Навыками проведение экспериментов по заданной методике, а так же способом обработка и анализа результатов
Навыками проведение предварительного технико-экономического обоснования проектных расчётов
Методикой проведение вычислительных экспериментов с использованием стандартных программных средств;

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем	Вид занятий	Семестр / Курс	Часов	Интеракт.
	Раздел 1. Раздел 1	Раздел			
1.1	Понятие криптографического протокола. Общие сведения о криптографических протоколах	Лек	8	4	2

1.2	Лабораторная работа №1	Лаб	8	4	0
1.3	Идентификация и аутентификация	Лек	8	4	2
1.4	Лабораторная работа №2	Лаб	8	4	0
1.5	Протокол взаимоблокировки. Протокол Ву-Лама. Протоколы обмена ключами	Лек	8	4	2
1.6	Лабораторная работа №3	Лаб	8	4	0
1.7	Протокол Диффи-Хеллмана	Лек	8	4	0
1.8	Лабораторная работа №4	Лаб	8	4	0
1.9	Развитые протоколы обмена ключами с аутенти-фикацией сторон. Протокол Kerberos	Лек	8	6	2
1.10	Лабораторная работа №5	Лаб	8	4	0
1.11	Типичные атаки на протоколы аутентификации	Ср	8	2	0
1.12	Лабораторная работа №6	Лаб	8	4	0
1.13	Типичные атаки на протоколы аутентификации. Атака на основе безымянных сообщений	Лек	8	4	0
1.14	Лабораторная работа №7	Лаб	8	4	0
1.15	Протоколы защиты данных в сети Internet	Лек	8	4	0
1.16	Лабораторная работа №8	Лаб	8	4	0
1.17	Протоколы защиты данных в сети Internet	Лек	8	6	0
1.18	Лабораторная работа №9	Лаб	8	4	0
1.19	Самостоятельная работа №1	Ср	8	10	0
1.20	Самостоятельная работа №2	Ср	8	8	0
1.21	Самостоятельная работа №3	Ср	8	8	0
1.22	Самостоятельная работа №4	Ср	8	4	0
1.23	Самостоятельная работа №5	Ср	8	6	0
1.24	Самостоятельная работа №6	Ср	8	8	0
1.25	Самостоятельная работа №7	Ср	8	10	0
1.26	Самостоятельная работа №8	Ср	8	12	0
1.27	Самостоятельная работа №9	Ср	8	4	0
1.28	Итоговое занятие	Экзамен	8	36	0

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания для текущей аттестации

Оценочные материалы для проведения текущего контроля по дисциплине "Криптографические протоколы" были рассмотрены и одобрены на заседании кафедры "Программное обеспечение и администрирование информационных систем " от 30 марта 2017 г., протокол №8"

5.2. Фонд оценочных средств для промежуточной аттестации

Оценочные материалы для проведения промежуточного контроля по дисциплине "Криптографические протоколы" были рассмотрены и одобрены на заседании кафедры "Программное обеспечение и администрирование информационных систем " от 30 марта 2017 г., протокол №8"

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Заглавие	Эл. адрес	Кол-
Л1.1	Бабенко Л. К. - Криптографическая защита информации: симметричное шифрование: Учебное пособие - М.: Издательство Юрайт, 2017.	http://www.biblio-online.ru/book/6946C235-8650-4A29-B75B-68E0EF829422	1

6.1.2. Дополнительная литература

	Заглавие	Эл. адрес	Кол-
Л2.1	Осипян В.О., Осипян К.В. - Криптография в задачах и упражнениях: [Учеб. пособие] - М.: Гелиос АРВ, 2004.		10

6.1.3. Методические разработки

	Заглавие	Эл. адрес	Кол-
Л3.1	Крыжевич Л. С. - Криптографические протоколы: учеб.-метод. пособие для студ. ФФМИ Курск. гос. ун-та - Курск: [б. и., 2013].		1

6.3.1 Перечень программного обеспечения

7.3.1.1	195:
7.3.1.2	Microsoft Windows 7 (Open License: 47818817)
7.3.1.3	Microsoft Office Professional 2007 (Open License: 43219389)
7.3.1.4	Adobe Acrobat Reader DC (Бесплатное программное обеспечение)
7.3.1.5	7-Zip (Свободная лицензия GNU LGPL)
7.3.1.6	GoogleChrome (Свободная лицензия BSD)
7.3.1.7	PacketTracer — программная модель оборудования Cisco.
7.3.1.8	Snort (Свободная лицензия GNU GPL)
7.3.1.9	Wireshark (Свободное программное обеспечение GNU GPL 2)
7.3.1.10	GNS 3 — программная модель обору-дования Cisco.
7.3.1.11	
7.3.1.12	146:
7.3.1.13	Microsoft Windows 7 (OpenLicense: 47818817)
7.3.1.14	Ms OfficeProfessional 2007 (OpenLicense: 47818817
7.3.1.15	Google Chrome (Свободная лицензия BSD)
7.3.1.16	7-Zip (Свободная лицензия GNU LGPL)
7.3.1.17	Adobe Acrobat Reader DC (Бесплатное программное обеспечение)
7.3.1.18	
7.3.1.19	аудитория 208
7.3.1.20	Microsoft Windows 7 (Open License: 47818817)
7.3.1.21	MsOffice Professional 2007 (Open License: 43219389)
7.3.1.22	Adobe Acrobat Reader DC (Бесплатное программное обеспечение)
7.3.1.23	7-Zip (Свободная лицензия GNU LGPL)
7.3.1.24	Google Chrome (Свободная лицензия BSD)
7.3.1.25	Visual Studio Community (Проприетарная академическая лицензия)
7.3.1.26	RStudio (Свободная лицензия GNU Affero General Public License v3)
7.3.1.27	

6.3.2 Перечень информационных справочных систем

7.3.2.1	Каталог библиотеки КГУ. - Режим доступа: http://195.93.165.10:2280
7.3.2.2	Электронная библиотека.- Режим доступа: http://elibrary.ru
7.3.2.3	Университетская информационная система «Россия» – http://uisrussia.msu.ru

7.3.2.4	Электронная библиотечная система «КнигаФонд» − http://www.knigafund.ru/
7.3.2.5	Электронная библиотечная система издательства «Лань» − http://e.lanbook.com/
7.3.2.6	Электронная библиотечная система «IPRbooks» − http://www.iprbookshop.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Лаборатория сетей и систем передачи информации для про-ведения занятий лекционного типа, занятий семинарского ти-па, групповых и индивидуальных консультаций, текущего кон-троля и промежуточной атте-стации,
7.2	305000, Курская область, г. Курск, ул. Радищева, д. № 33, 195.
7.3	Комплекты учебных столов и стульев - 10 шт;
7.4	Комплекты компьютерных столов и стульев (12 шт)
7.5	Кресло преподавателя – 1 шт.
7.6	Стол преподавателя с радиусом 1800х770х700 – 1 шт.
7.7	Стол учебный 1200х750х500 – 6 шт.
7.8	Доска, автоматизированное рабо-чее место (9 шт),
7.9	Лабораторный комплекс «Сетевая безопасность» СБ-1
7.10	
7.11	Помещение для самостоятельной работы обучающихся – аудитория, оснащенная компьютерной техни-кой с возможностью подключения к сети "Интернет" и с обеспечени-ем доступа в электронную инфор-мационно-образовательную среду университета.
7.12	305000, Курская область, г. Курск, ул. Радищева, д. № 33, 146.
7.13	Столов – 61
7.14	Посадочных мест – 162
7.15	Компьютеров:
7.16	Для пользователей – 40
7.17	Для библиотекаря – 2
7.18	Моноблоков MSI (27) - модель MS-A912, 2гб оперативной памяти, Athlon CPU D525 1.80GHz
7.19	Моноблоков Asus (13) - модель ET2220I, 4гб оперативной памяти, Intel Core i3-3220 CPU 3.30 GHz
7.20	
7.21	Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации,
7.22	305000, г. Курск, ул. Радищева, 33, 208
7.23	Доска ученическая (настенная) – 1 шт.
7.24	Мультимедиа-проектор – 1 шт.
7.25	Компьютер Ноутбук ASUS X553S – 1 шт.
7.26	Парта – 38 шт.
7.27	Стул – 45 шт.
7.28	Жалюзи – 4 шт.
7.29	

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Студентам необходимо ознакомиться с содержанием рабочей программы, с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, методическими разработками, имеющимся на кафедре.

1.1. Указания по подготовке к занятиям лекционного типа

Изучение дисциплины требует систематического и последовательного накопления знаний, поэтому студентам рекомендуется перед очередной лекцией просмотреть по конспекту материал предыдущей. При затруднениях в восприятии материала следует обращаться к основным литературным источникам, к лектору (по графику его консультаций) или к преподавателю на занятиях семинарского типа.

1.2. Указания по подготовке к лабораторным занятиям

Лабораторные занятия имеют следующую структуру:

- тема занятия;
- цели проведения занятия по соответствующим темам;
- задания состоят из выполнения практических заданий, примеров;
- рекомендуемая литература.

«Методические указания по подготовке к практическим занятиям по дисциплине «Криптографические протоколы»

утверждены на заседании кафедры от 30 марта 2017 г., протокол №8", находятся на кафедре «Программного обеспечения и администрирования информационных систем» в свободном доступе для студентов.

1.3. Методические указания по выполнению самостоятельной работы

Самостоятельная работа студентов включает в себя выполнение практических заданий, самостоятельное изучение отдельных вопросов по теме. По каждой теме учебной дисциплины студентам предлагается перечень заданий для самостоятельной работы, которые содержатся в «Методических указаниях по самостоятельной работе по дисциплине «Криптографические протоколы»», утвержденных на заседании кафедры от 30 марта 2017 г., протокол №8" и находятся на кафедре « Программного обеспечения и администрирования информационных систем» в свободном доступе для студентов.

1.4. Методические указания по работе с литературой

Основная литература к данной дисциплине - это учебники и учебные пособия.
Дополнительная литература - это монографии, сборники научных трудов, журнальные и газетные статьи, различные справочники, энциклопедии, интернет ресурсы.

В учебнике/ учебном пособии/ монографии следует ознакомиться с оглавлением и научно-справочным аппаратом, прочитать аннотацию и предисловие. Целесообразно ее пролистать, рассмотреть иллюстрации, таблицы, диаграммы, приложения. Такое поверхностное ознакомление позволит узнать, какие главы следует читать внимательно, а какие прочитать быстро.
Студенту следует использовать следующие виды записей при работе с литературой:
Конспект - краткая схематическая запись основного содержания научной работы. Целью является не переписывание произведения, а выявление его логики, системы доказательств, основных выводов.
Цитата - точное воспроизведение текста. Заключается в кавычки. Точно указывается страница источника.
Тезисы - концентрированное изложение основных положений прочитанного материала.
Аннотация - очень краткое изложение содержания прочитанной работы.
Резюме - наиболее общие выводы и положения работы, ее концептуальные итоги и другие виды.