Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Худин Александр Николаевич
Должность: Ректор
Дата подписания: 26.01.2021 12:23:17
Уникальный программный ключ:
08303ad8de1c60b987361de7085acb509ac3da143f415362ffaf0ee37e73fa19

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
Технологии обнаружения сетевых атак

Направление подготовки: 10.03.01 Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Квалификация: бакалавр

Факультет физики, математики, информатики

Форма обучения: очная

Общая трудоемкость 4 ЗЕТ

Виды контроля в семестрах:
экзамен(ы) 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	36	36	36	36
Лабораторные	36	36	36	36
В том числе инт.	16	16	16	16
Итого ауд.	72	72	72	72
Контактная работа	72	72	72	72
Сам. работа	36	36	36	36
Часы на контроль	36	36	36	36
Итого	144	144	144	144

Курск 2017

Рабочая программа дисциплины Технологии обнаружения сетевых атак / 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 "Технологии обнаружения сетевых атак" предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность профиль Безопасность компьютерных систем

Составитель(и):

© Курский государственный университет, 2017

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности систем и их информационной инфраструктуры; развитие профессиональной культуры, формирование научного мировоззрения и развитие системного мышления; привитие стремления к поиску оптимальных, простых и надежных решений.

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

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:
основные принципы построения защищенных распределенных компьютерных систем
Уметь:
формализовать задачу управления безопасностью информационных систем
Владеть:
навыками выявления и устранения уязвимостей компьютерной сети

ПК-1: Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
Знать:
основные принципы построения систем обнаружения компьютерных атак
Уметь:
анализировать защищенность систем
Владеть:
навыками организации защищенного удаленного доступа к информационным ресурсам и способами настройки стандартных систем обнаружения компьютерных атак

ПК-2: Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
Знать:
способы обнаружения и нейтрализации последствий вторжений в компьютерные системы
Уметь:
администрировать системы обнаружения компьютерных атак
Владеть:
навыками проведения анализа рисков и администрирования безопасности распределенных компьютерных систем

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)					
Код занятия	**Наименование разделов и тем**	**Вид занятий**	**Семестр / Курс**	**Часов**	**Интеракт.**
	Раздел 1. Системный подход к обеспечению защиты от компьютерных атак	Раздел			
1.1	Компьютерные системы и их компоненты как объекты защиты.	Лек	7	2	2
1.2	Примеры современных КС. Характеристика компо-нентов КС с точки зрения уязвимости к воздействию угроз безопасности.	Лаб	7	2	2
1.3	Физические основы уязвимостей компонентов КС.	Ср	7	2	0
1.4	Угрозы безопасности и каналы их воздействия.	Лек	7	4	0
1.5	Классификация и характеристика каналов и способов воздействия угроз безопасности на КС.	Лаб	7	4	0
1.6	Терминология и классификации Гостехкомисии, ФСТЭК России.	Ср	7	4	0
1.7	Направления и методы защиты информации.	Лек	7	2	0
1.8	Направления защиты программ, данных и других компонентов КС. Классификация методов и средств защиты информации.	Лаб	7	2	0
1.9	Историческое развитие средств ЗИ.	Ср	7	2	0
1.10	Методика построения защищенных компьютерных систем.	Лек	7	2	0
1.11	Характеристика системы ЗИ для сложных КС. Методика построения комплексных систем защиты КС.	Лаб	7	2	0
1.12	Сущность системного подхода	Ср	7	2	0
1.13	Организационные методы и средства защиты компьютерных систем.	Лек	7	4	0
1.14	Установление режимов доступа к информации, циркулирующей в КС. Администрирование КС.	Лаб	7	4	0
1.15	Характеристика типовых организационных документов в системе ЗИ.	Ср	7	4	0
1.16	Технологические направления повышения защищенности компьютерных систем.	Лек	7	2	0
1.17	Особенности использования в этих целях технологий “клиент-сервер” и распределенных баз данных. Web-технологии.	Лаб	7	2	0
1.18	Тенденции развития современных вычислительных платформ.	Ср	7	2	0
	Раздел 2. Средства выявления и локализации уязвимостей компьютерных систем к воздействию угроз безопасности.	Раздел			
2.1	Системы обнаружения атак (Intrusion Detection Systems, IDS).	Лек	7	4	4
2.2	Системы обнаружения атак (Intrusion Detection Systems, IDS).	Лаб	7	4	2
2.3	Системы обнаружения атак (Intrusion Detection Systems, IDS).	Ср	7	4	0

	Раздел 3. Практика применения	Раздел			
3.1	Методы и средства оценки защищенности компьютерных систем	Лек	7	4	2
3.2	Средства моделирования атак и воздействия различных угроз на компоненты КС.	Лаб	7	4	4
3.3	Сравнительные характеристики коммерческих систем контроля защищенности КС.	Ср	7	4	0
3.4	Средства контроля доступа к компонентам компьютерных систем.	Лек	7	2	0
3.5	Считывающие устройства. Электронные ключи. Биометрические систе-мы контроля доступа. Программы для создания защищенных файлов, папок, логических дисков.	Лаб	7	2	0
3.6	Основные направления применения систем контроля доступа.	Ср	7	2	0
3.7	Методы и средства обеспечения безопасности электропитания компьютерных систем.	Лек	7	2	0
3.8	Методология организации бесперебойного электропитания. Устройства обеспечения бесперебойного электропитания (UPS) и управления ими.	Лаб	7	2	0
3.9	Направления применения и характеристики технических средств обеспечения электропитания КС.	Ср	7	2	0
3.10	Методы и средства гарантированного уничтожения информации.	Лек	7	4	0
3.11	Характеристика носителей и стандартных способов записи/удаления информации. Описание технических средств гарантированного удаления информации.	Лаб	7	4	0
3.12	Физические основы методов хранения информации.	Ср	7	4	0
3.13	Методы и средства выявления и локализации утечек информации по техническим каналам.	Лек	7	4	0
3.14	Инженерные СЗИ от ПЭМИН. Классификация и характеристика пассивных и активных СЗИ от ПЭМИН.	Лаб	7	4	0
3.15	Методики расчета параметров ПЭМИН.	Ср	7	4	0

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания для текущей аттестации

Оценочные материалы для текущего контроля по дисциплине «Технологии обнаружения сетевых атак» рассмотрены и одобрены на заседании кафедры программного обеспечения информационных систем КГУ от «30» марта 2017 г. протокол №8, является приложением к рабочей программе.

5.2. Фонд оценочных средств для промежуточной аттестации

Оценочные материалы для промежуточного контроля по дисциплине «Технологии обнаружения сетевых атак» рассмотрены и одобрены на заседании кафедры программного обеспечения информационных систем КГУ от «30» марта 2017 г. протокол №8, является приложением к рабочей программе.

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

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Заглавие	Эл. адрес	Кол-
Л1.1	Милославская Н. Г. - Сетевые атаки на открытые системы на примере интранета - Москва: МИФИ, 2012.	http://biblioclub.ru/index.php?page=book&id=231630	1

6.1.2. Дополнительная литература

	Заглавие	Эл. адрес	Кол-
Л2.1	Докучаев В.А., Кондратьев М.Г., Крупнов И.А., Маклачкова В.В., Мытенков С.С., Шведов А.В., Докучаев В.А. - Система обнаружения компьютерных атак «Форпост»: учебно-методическое пособие - Москва: Московский технический университет связи и информатики, 2016.	http://www.iprbookshop.ru/61543.html	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	

6.3.2 Перечень информационных справочных систем

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

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 практическим занятиям типа

«Методические указания по подготовке к лабораторным занятиям по дисциплине «Технологии обнаружения сетевых атак» 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 различного рода заданий, которые ориентированы на более глубокое усвоение материала изучаемой дисциплины. По каждой теме учебной дисциплины студентам предлагается перечень заданий для самостоятельной работы, которые содержатся в «Методических указаниях по самостоятельной работе по дисциплине Технологии обнаружения сетевых атак» 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

Следует характеризовать структуру рекомендуемой литературы:

К каждой теме учебной дисциплины подобрана основная и дополнительная литература.

Основная литература - 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 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.

Тезисы - концентрированное изложение основных положений прочитанного материала.