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
Методы оценки безопасности компьютерных систем

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) 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	9			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Практические	36	36	36	36
В том числе инт.	8	8	8	8
Итого ауд.	54	54	54	54
Контактная работа	54	54	54	54
Сам. работа	54	54	54	54
Часы на контроль	36	36	36	36
Итого	144	144	144	144

Курск 2017

Рабочая программа дисциплины Методы оценки безопасности компьютерных систем / 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 "Методы оценки безопасности компьютерных систем" 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	изучение видов, практических методов и средств оценки уровня безопасности компьютерных систем.

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

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-6: Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
Знать:
процессы проверки и оценки ИБ ИТ и СОИБ
Уметь:
осуществлять аудит ИБ и организовывать работы по его проведению
Владеть:
терминологией в области аудита ИБ

ПСК-1.1: Способностью участвовать в разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах
Знать:
принципы организации процесса аудита ИБ и подготовки отчетных документов по результатам
Уметь:
составлять программу аудита ИБ, определять его область действия и критерии
Владеть:
практическими приемами проведения аудита ИБ, методами сбора данных

ПСК-1.4: Способностью проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей
Знать:
критерии и стандарты в области аудита ИБ
Уметь:
формулировать выводы и заключение по результатам аудита ИБ
Владеть:
навыками использования инструментальных средств, автоматизированных процессов ИБ

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)					
Код занятия	**Наименование разделов и тем**	**Вид занятий**	**Семестр / Курс**	**Часов**	**Интеракт.**

	Раздел 1. Базовые сведения о проверке и оценке уровня безопасности компьютерных систем	Раздел			
1.1	Проверки и оценки уровня ИБ организации	Лек	8	2	2
1.2	Оценка уязвимостей компьютерной системы	Пр	8	4	0
1.3	Разновидности проверок и оценок уровня ИБ организации. Рынок аналитических услуг в сфере ИБ. Место и роль аудита в модели обеспечения ИБ.	Ср	8	8	0
	Раздел 2. Оценка уровня безопасности компьютерных систем: общие понятия и определения	Раздел			
2.1	Базовые определения.Принципы и формы аудита ИБ организации	Лек	8	2	2
2.2	Оценка уязвимостей компьютерной системы	Пр	8	8	0
2.3	Особенности автоматизированных информационных систем как объектов аудита ИБ.	Ср	8	6	0
2.4	Исходная концептуальная схема (парадигма) проведения аудита ИБ.	Ср	8	8	0
	Раздел 3. Стандарты проведения оценки уровня безопасности компьютерных систем	Раздел			
3.1	Законодательная и нормативная база аудита ИБ.Структура международных стандартов по ИБ. Область применения. Процессная модель управления ИБ.Оценка зрелости системы управления ИБ.	Лек	8	2	2
3.2	ISO 27001 (В 7799 - 2:2005). ISO 27002 (BS 7799 - 1:2005). Стандарты ISO/IEC и ГОСТ ИСО/МЭК 27005, BS 7799-3. Анализ рисков ИБ.	Лек	8	2	0
3.3	Общие критерии (ГОСТ Р ИСО/МЭК 15408). Руководящие документы ФСТЭК России аудит в целях сертификации средств защиты и аттестации объектов нформатизации. Ста Банка России СТО БР ИББС- 1.1. CoBit. Стандарт аудита PCI DSS.	Лек	8	2	0
3.4	Соответствие и взаимодействие международного и российского подходов и методов аудита безопасности.	Ср	8	8	0
3.5	Стандарт аудита PCI DSS.	Ср	8	6	0
	Раздел 4. Методология оценки уровня безопасности компьютерных систем. Организация процесса оценки уровнябезопасности компьютерных систем.	Раздел			
4.1	Основные этапы и методы работ по проведению аудита ИБ. Программа аудита ИБ	Лек	8	2	2

4.2	Сбор свидетельств (исходной информации) для проведения аудита ИБ. Рекомендации по планированию аудита ИБ. Рекомендации по моделированию.	Лек	8	2	0
4.3	Этапы проведения внутреннего и внешнего аудитов ИБ: общее и различия. Стадии аудита ИБ: планирование; подготовка; моделирование; тестирование; анализ; разработка предложений, документирование.	Пр	8	4	0
4.4	Договор о проведении внешнего аудита ИБ. Порядок планирования аудита.	Пр	8	4	0
4.5	Методы аудита: экспертно-аналитические; экспертно-инструментальные; моделирование действий злоумышленника.	Ср	8	4	0
4.6	Методы сбора исходных данных: опрос, наблюдение, анализ. Методы анализа собранных свидетельств.	Ср	8	4	0
4.7	Аудиторская группа: состав, права и обязанности, роли, привлечение технических специалистов. Обязанности проверяемой организации во время аудита ИБ.	Ср	8	2	0
	Раздел 5. Инструментальные средства оценки уровня безопасности компьютерных систем	Раздел			
5.1	Методы и инструментальные средства проведения аудита ИБ	Лек	8	2	0
5.2	Программные средства анализа и управления	Лек	8	2	0
5.3	Оценка уязвимостей компьютерной системы средствами Dallas Lock	Пр	8	8	0
5.4	Инструментарий базового уровня - справочные и методические материалы. Инструментарий для обеспечения повышенного уровня безопасности.	Пр	8	4	0
5.5	ПО идентификации и оценки защищаемых ресурсов, угроз, уязвимостей и мер защиты в сфере компьютерной и физической безопасности предприятия	Пр	8	4	0
5.6	СПВ, их применение и примеры систем. Сохранение доказательств вторжений. Стандарты в области обнаружения вторжений.	Ср	8	8	0
5.7	Промежуточная аттестация	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 «Методы оценки безопасности компьютерных систем» рассмотрены и одобрены на заседании кафедры программного обеспечения и администрирования

информационных систем 30.03.2017 протокол № 8 и являются приложением к рабочей программе.

5.2. Фонд оценочных средств для промежуточной аттестации

Оценочные материалы для проведения промежуточной аттестации по дисциплине «Методы оценки безопасности компьютерных систем» рассмотрены и одобрены на заседании кафедры программного обеспечения и администрирования информационных систем 30.03.2017 протокол № 8 и являются 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	Шаньгин В.Ф. - Информационная безопасность и защита информации: учебное пособие - Саратов: Профобразование, 2017.	http://www.iprbookshop.ru/63594.html	1

6.1.2. Дополнительная литература

	Заглавие	Эл. адрес	Кол-
Л2.1	Нестеров С. А. - Информационная безопасность: Учебник и практикум - М.: Издательство Юрайт, 2017.	http://www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7	1
Л2.2	Артемов А. В. - Информационная безопасность - Орел: МАБИВ, 2014.	http://biblioclub.ru/index.php?page=book&id=428605	1
Л2.3	- Информационная безопасность - Москва: ГРОТЕК, 2014.	http://biblioclub.ru/index.php?page=book&id=230502	1

6.3.1 Перечень программного обеспечения

7.3.1.1	199:
7.3.1.2	Microsoft Windows 7 (Open License: 47818817)
7.3.1.3	Microsoft Office 2007 (OpenLicense: 43136274)
7.3.1.4	Adobe Acrobat Reader DC (Бес-платное программное обеспечение)
7.3.1.5	GoogleChrome (Свободная лицензия BSD)
7.3.1.6	7-Zip (Свободная лицензия GNU LGPL),
7.3.1.7	Visual Studio Community (Проприе-тарная академическая лицензия)
7.3.1.8	СКЗИ "КриптоПроCSP" версии 4.0
7.3.1.9	СС КонсультантПлюс (Договор № 7/3Ц от 14.02.2017),
7.3.1.10	СКМ-21 ПО (Компакт-диск со специ-альным программным обеспечением)
7.3.1.11	Смарт-ПО (Компакт-диск с про-граммным обеспечением)
7.3.1.12	Code::Blocks (Свободная лицензия GNU GPLv3)
7.3.1.13	EclipseNeon (Открытое программное обеспечение EclipsePublicLicense)
7.3.1.14	
7.3.1.15	146:
7.3.1.16	Microsoft Windows 7 (OpenLi-cense: 47818817)
7.3.1.17	Ms OfficeProfessional 2007 (OpenLicense: 47818817
7.3.1.18	Google Chrome (Свободная ли-цензия BSD)
7.3.1.19	7-Zip (Свободная лицензия GNU LGPL)
7.3.1.20	Adobe Acrobat Reader DC (Бес-платное программное обеспе-чение)

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. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Лаборатория программно-аппаратных средств обеспечения информационной безопас-ности;
7.2	Лаборатория технических средств защиты информации;
7.3	для проведения занятий лекци-онного типа, занятий семинаркого типа, курсового проекти-рования (выполнения курсовых работ), групповых и индивиду-альных консультаций, текуще-го контроля и промежуточной аттестации, самостоятельной работы,
7.4	305000, Курская область, г. Курск, ул. Радищева, д. № 33, 199.
7.5	МоноблокLenovoC560 – 9 шт.
7.6	Стенд информационный 1,4м*0,9м – 9 шт.
7.7	Малогабаритный камуфлирован-ный блокиратор работы сотовых телефонов и закладных устройств – 1 шт.
7.8	Селективный обнаружитель циф-ровых радиоустройств ST062 – 1 шт.
7.9	Устройство защиты объектов ин-форматизации от утечки инфор-мации за счет ПЭМИН «Блокада» – 1 шт.
7.10	Нелинейный локатор «Буклет-2» – 1 шт.
7.11	Устройство МП—1А – 1 шт.
7.12	Электронно-оптическое устройст-во для обнаружения любых типов оптических устройств «Гранат» – 1 шт.
7.13	Программно-аппаратный ком-плекс «Соболь» – 1 шт.
7.14	ИМФ-3 имитатор многофункцио-нальный – 1 шт.
7.15	МониторЖК-панель 17 Асер – 1 шт.
7.16	Жалюзи вертикальные тканевые – 1 шт.
7.17	Концентратор 24порт – 1 шт.
7.18	Лабораторный комплекс «Беспро-водные сети ЭВМ»
7.19	Система активной защиты рече-вой акустической информации SEL-157 "Шагрень",
7.20	Устройство «Смарт (Комплекс оценки эффективности защиты речевой информации от утечки по акустическому, виброакустиче-скому и акустоэлектрическому каналам),
7.21	Программно-аппаратные средства защиты информации от НСД .
7.22	
7.23	Помещение для самостоятельной работы обучающихся – аудитория, оснащенная компьютерной техни-кой с возможностью подключения к сети "Интернет" и с обеспечением доступа в электронную информационно-образовательную среду университета.
7.24	305000, Курская область, г. Курск, ул. Радищева, д. № 33, 146.
7.25	Столов – 61
7.26	Посадочных мест – 162
7.27	Компьютеров:
7.28	Для пользователей – 40
7.29	Для библиотекаря – 2
7.30	Моноблоков MSI (27) - модель MS-A912, 2гб оперативной памяти, Athlon CPU D525 1.80GHz
7.31	Моноблоков Asus (13) - модель ET2220I, 4гб оперативной памяти, Intel Core i3-3220 CPU 3.30 GHz
7.32	
7.33	

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

Приступая к изучению курса, студентам рекомендуется ознакомиться с содержанием рабочей программы, с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, методическими разработками, имеющимся на кафедре программного обеспечения и администрирования информационных систем.
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.
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.
В начале изучения курса, в учебнике или учебном пособии, рекомендуемом в качестве основной или дополнительной литературы для освоения дисциплины, студенту рекомендуется проанализировать оглавление, научно-справочный аппарат, аннотацию и предисловие.
Студенту рекомендуется использовать следующие виды записей при работе с литературой:
Конспект - краткая схематическая запись основного содержания научной работы, целью которой является не переписывание материала, а выявление его логики, системы доказательств, основных выводов. Тезисы - концентрированное изложение основных положений прочитанного материала.
Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:
Для изучения конспекта лекции в тот же день, после лекции студенту рекомендуется 10-15 минут.
Изучение конспекта лекции по предыдущей теме за день перед лекцией по следующей темой - 10-15 минут.
Изучение теоретического материала по учебнику и конспекту - 1 час в неделю.
Подготовка к практическому занятию - 30 мин.
Всего в неделю - 2 часа 55 минут.
При изучении дисциплины рекомендуется самостоятельно изучать материал, который еще не прочитан на лекции. В этом случае, понимание лекционного материала осуществляется студентом более эффективно.
Для понимания материала и качественного его усвоения рекомендуется следующая последовательность действий:
После работы на лекции, или на практической работе, и после окончания учебных занятий, студенту рекомендуется самостоятельно проанализировать лекционный материал, или материал практической работы (10-15 минут).
При подготовке к лекции, или практической работе по следующей теме, студенту рекомендуется проанализировать лекционной материал, или материал практической работы по предыдущей теме (10-15 минут).
При подготовке к практическому занятиям рекомендуется также изучить соответствующий теоретический материал по дисциплине, предусмотренный темой практической работы.
В течение учебной недели студенту рекомендуется изучать материал по дисциплине, изложенный в рекомендуемой литературе в течение 1 часа.