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
Защита в операционных системах

Направление подготовки: 10.03.01 Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Квалификация: бакалавр

Факультет физики, математики, информатики

Форма обучения: очная

Общая трудоемкость 2 ЗЕТ

Виды контроля в семестрах:

зачет(ы) 4

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**4 (2.2)**		Итого	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Практические	18	18	18	18
В том числе инт.	8	8	8	8
Итого ауд.	36	36	36	36
Контактная работа	36	36	36	36
Сам. работа	36	36	36	36
Итого	72	72	72	72

Курск 2017

Рабочая программа дисциплины Защита в операционных системах / сост. к.т.н., доцент, Бабкин Геннадий Викторович;Кониченко Александр Васильевич; 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 "Защита в операционных системах" предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность профиль Безопасность компьютерных систем

Составитель(и):

к.т.н., доцент, Бабкин Геннадий Викторович;Кониченко Александр Васильевич

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Целью дисциплины является освоение обучающимися принципов построения защиты информации в операционных системах и анализа надежности их защиты; формирование систематизированных знаний о комплексе организационно-правовых мер по защите отдельных видов информации, изучение нормативных правовых актов, регламентирующих правовой режим государственной тайны и иной конфиденциальной информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.ДВ.4

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 нормативные и правовые документы в области информационной и компьютерной безопасности
Уметь:
находить, обобщать полученную научную, справочную, статистическую и иную информацию
Владеть:
навыками оценки угроз безопасности компьютерным системам

ПК-3: Способностью администрировать подсистемы информационной безопасности объекта защиты
Знать:
основные определения и понятия; основы предметной области
Уметь:
выявлять и оценивать проблемы в своей профессиональной деятельности
Владеть:
навыками применения средств защиты в соответствии с заданными требованиями

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем	Вид занятий	Семестр / Курс	Часов	Интеракт.
	Раздел 1.	Раздел			
1.1	Требования к защите ОС. Понятие защищенной ОС. Подходы к организации защиты ОС и их недостатки	Лек	4	1	0
1.2	Исследование методов разграничения доступа в ОС Windows. Этапы построения защиты. Административные меры защиты. Управление загрузкой и восстановление данных в Windows.	Пр	4	1	0
1.3	Стандарты безопасности ОС	Ср	4	2	0

1.4	Анализ защищенности современных операционных систем. Встроенные средства защиты Windows, Unix	Лек	4	1	1
1.5	Аудит системных процессов и событий в Windows. Анализ выполнения современными ОС формализованных требований к защите информации от НСД.	Пр	4	1	0
1.6	Обзор и статистика методов, лежащих в основе атак на современные ОС	Лек	4	1	1
1.7	Архивации и восстановления данных в Windows. Классификация атак на ОС и их сравнительная статистика. Шифрование данных в Windows с помощью EFS.	Пр	4	2	0
1.8	Анализ атаки и методов, позволяющих несанкционированно вмешаться в работу ОС	Ср	4	4	0
	Раздел 2.	Раздел			
2.1	Разграничение доступа в ОС. Субъекты, объекты, методы и права доступа. Привилегии субъектов доступа	Лек	4	2	0
2.2	Избирательное и полномочное разграничение доступа, изолированная программная среда	Пр	4	1	0
2.3	Примеры реализации разграничения доступа в современных ОС	Ср	4	4	0
2.4	Идентификация и аутентификация пользователей ОС	Лек	4	1	1
2.5	Аутентификация на основе паролей, методы подбора паролей, средства и методы повышения защищенности ОС от подбора паролей. Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя	Пр	4	1	0
2.6	Примеры реализации идентификации и аутентификации в современных ОС	Ср	4	4	0
	Раздел 3.	Раздел			
3.1	Разграничение доступа к ресурсам в ОС Windows, Unix. Организация разграничения доступа к объектам	Лек	4	2	0
3.2	Анализ защищенности операционных систем семейства Windows и Unix. Разделяемые сетевые ресурсы, NTFS и права доступа. Распределенная файловая система и права доступа.	Пр	4	2	0
3.3	Назначение прав доступа к объектам: файлам и папкам NTFS, сетевым ресурсам, объектам Active Directory	Ср	4	2	0
3.4	Аудит в ОС. Необходимость аудита	Лек	4	2	1
3.5	Требования к подсистеме аудита	Пр	4	1	0
3.6	Примеры реализации аудита в современных ОС	Ср	4	2	0
3.7	Защита сетевого взаимодействия Windows, Unix. Методика проникновения. Сбор информации о системе	Лек	4	1	1
3.8	Защита каналов средствами файервола. Виртуальные частные сети, протоколы	Пр	4	1	0
3.9	Обзор защиты беспроводных сетей	Ср	4	2	0
	Раздел 4.	Раздел			

4.1	Повышение уровня защищенности рабочей среды пользователей на базе Windows, Unix. Безопасность рабочей среды и приложений пользователя	Лек	4	2	1
4.2	Изучение средств защиты сетевого взаимодействия. Настройки зон безопасности. Безопасность приложений с поддержкой сценариев Централизованная настройка приложений через групповые политики. Конфигурирование средств защиты каналов.	Пр	4	2	0
4.3	Защита от неправомерных изменений конфигурации рабочих станций и серверов, от использования неучтенных программ	Ср	4	4	0
4.4	Безопасность систем под управлением Windows, Unix	Лек	4	2	0
4.5	Применение шаблонов безопасности для защиты рабочих станций пользователей. Защита серверов.	Пр	4	2	0
4.6	Анализ параметров безопасности систем под управлением Windows, Unix	Ср	4	4	0
4.7	Повышение защищенности служб на базе Windows, Unix	Лек	4	1	1
4.8	Защита Active Directory. Защита DNS, FTP, DHCP.	Пр	4	2	0
4.9	Защита терминального сервера с использованием RDP	Ср	4	4	0
	Раздел 5.	Раздел			
5.1	Системы защиты программного обеспечения	Лек	4	2	1
5.2	Анализ средств защиты от копирования и взлома программных средств	Пр	4	2	0
5.3	Уязвимости современных методов защиты ПО	Ср	4	4	0

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания для текущей аттестации

Оценочные материалы для проведения текущего контроля по дисциплине "Защита в операционных системах" рассмотрены и одобрены на заседании кафедры от «30» марта 2017 г. протоколом № 8

5.2. Фонд оценочных средств для промежуточной аттестации

Оценочные материалы для проведения промежуточного контроля по дисциплине "Защита в операционных системах" рассмотрены и одобрены на заседании кафедры от «30» марта 2017 г. протоколом № 8

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

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Заглавие	Эл. адрес	Кол-
Л1.1	Назаров С. В., Широков А. И. - Современные операционные системы: учебное пособие - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.	http://www.iprbookshop.ru/15837	1
Л1.2	Назаров С.В., Широков А.И. - Современные операционные системы: учебное пособие - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.	http://www.iprbookshop.ru/52176.html	1

6.3.1 Перечень программного обеспечения

7.3.1.1	210:
7.3.1.2	MacOS 10.11(Документы о приобре-тении iMac 21.5")

7.3.1.3	Oracle VM VirtualBox (Свободная ли-цензия GNU GPL 2)
7.3.1.4	Microsoft Windows 7 (Open License: 47818817)
7.3.1.5	MsOffice Professional 2007 (Open License: 43219389)
7.3.1.6	AdobeAcrobatReader DC (Бесплатное программное обеспечение)
7.3.1.7	7-Zip (Свободная лицензия GNU LGPL)
7.3.1.8	GoogleChrome (Свободная лицензия BSD)
7.3.1.9	Linux Ubuntu 16 (Свободно распро-страняемое программное обеспече-ние)
7.3.1.10	Microsoft Windows XP (Open License: 47818817)
7.3.1.11	Code::Blocks
7.3.1.12	(Бесплатное программное обеспече-ние)
7.3.1.13	Microsoft SQL Server 2016 Express (Проприетарная академическая ли-цензия)
7.3.1.14	MySQLCommunityEdition (Свободное программное обеспечение GNU GPL)
7.3.1.15	MySQLWorkbench (Свободная лицен-зия GNU GPL)
7.3.1.16	CASE-средство ALL Fusion
7.3.1.17	FlatAssembler (Свободное программ-ное обеспечение лицензия BSD с воз-можно анти-GPL)
7.3.1.18	Visual Studio Community (Проприе-тарная академическая лицензия)
7.3.1.19	
7.3.1.20	146:
7.3.1.21	Microsoft Windows 7 (OpenLi-cense: 47818817)
7.3.1.22	Ms OfficeProfessional 2007 (OpenLicense: 47818817
7.3.1.23	Google Chrome (Свободная ли-цензия BSD)
7.3.1.24	7-Zip (Свободная лицензия GNU LGPL)
7.3.1.25	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, 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	Компьютерная аудитория: учеб-ная аудитория для проведения за-нятий лекционного типа, занятий семинарского типа, курсового проектирования, групповых и ин-дивидуальных консультаций, те-кущего контроля и промежуточ -ной аттестации,
7.2	305000, Курская область, г. Курск, ул. Радищева, д. № 33, 210.
7.3	Комплекты компьютерных столов и стульев (14 шт)
7.4	ppeleiMac 21.5 – 15шт.
7.5	МоноблокSamsung – 1 шт.
7.6	Мультимедиа-проектор – 1 шт.
7.7	Доска интерактивная HitachiStarboard – 1 шт.

7.8	Доска классная – 1 шт.
7.9	Монитор ЖК-панель17Асер – 1 шт.
7.10	Системный блок Gateway E2530S – 1 шт.
7.11	Концентратор Compex – 1 шт.
7.12	
7.13	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.
7.14	305000, Курская область, г. Курск, ул. Радищева, д. № 33, 146.
7.15	Столов – 61
7.16	Посадочных мест – 162
7.17	Компьютеров:
7.18	Для пользователей – 40
7.19	Для библиотекаря – 2
7.20	Моноблоков MSI (27) - модель MS-A912, 2гб оперативной памя-ти, Athlon CPU D525 1.80GHz
7.21	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 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 «Защита в операционных системах» утверждены на заседании кафедры от «30» марта 2017 г. протоколом № 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 «Защита в операционных системах», утвержденных на заседании кафедры от «30» марта 2017 г. протоколом № 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.