

Документ подписан простой электронной подписью
Информация о владельце:

ФИО: Худин Александр Николаевич

Должность: Ректор

Дата подписания: 26.01.2021 12:23:21

Уникальный программный ключ:

08303ad8de1c60b987361de7085acb509ac3da145741b561af0ee9e73a17

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

Теоретические основы компьютерной безопасности

Направление подготовки: 10.03.01 Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Квалификация: бакалавр

Факультет физики, математики, информатики

Форма обучения: очная

Общая трудоемкость 3 ЗЕТ

Виды контроля в семестрах:

зачет(ы) с оценкой 7

Распределение часов дисциплины по семестрам

| Семестр (<Курс>.<Семестр на курсе>) | 7 (4.1) | | Итого | |
|---|---------|-----|-------|-----|
| | Неделя | | | |
| Вид занятий | уп | рп | уп | рп |
| Лекции | 18 | 18 | 18 | 18 |
| Лабораторные | 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 |
| Итого | 108 | 108 | 108 | 108 |

Рабочая программа дисциплины Теоретические основы компьютерной безопасности / сост. доцент, Гордиенко В.В.; доцент, Крыжевич Л.С.; 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 "Теоретические основы компьютерной безопасности" предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность профиль Безопасность компьютерных систем

Составитель(и):

доцент, Гордиенко В.В.; доцент, Крыжевич Л.С.

© Курский государственный университет, 2017

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

| | |
|-----|---|
| 1.1 | Целью освоения учебной дисциплины «Теоретические основы компьютерной безопасности» является формирование у студентов знаний и умений по защите компьютерной информации с применением современных программно-аппаратных средств. |
| 1.2 | Задачи дисциплины – дать знания: |
| 1.3 | • о методах и средствах защиты информации в компьютерных системах; |
| 1.4 | • о защитных механизмах, реализованных в средствах защиты компьютерных систем от несанкционированного доступа (НСД); |
| 1.5 | • о современных программно-аппаратных комплексах защиты информации; |
| 1.6 | • о применении средств криптографической защиты информации и средств защиты от НСД для решения задач обеспечения информационной безопасности. |
| 1.7 | Приобретенные знания и навыки позволят студентам работать в должностях администраторов компьютерных сетей и администраторов безопасности. Содержание дисциплины охватывает круг вопросов, связанных с обеспечением информационной безопасности кибернетических систем. Особое внимание уделяется обеспечению безопасности автоматизированных систем управления технологическими процессами. |

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:

основы компьютерной обработки данных, принципы структурной организации вычислительных систем и компьютерных сетей;

Основные угрозы и характеристику технических каналов утечки информации

основные руководящие и нормативные документы по инженерно-технической защите информации

Уметь:

выявлять угрозы и технические каналы утечки информации

применять наиболее эффективные методы и средства инженерно-технической защиты информации

моделировать объекты защиты и угрозы безопасности информации

Владеть:

практическими навыками в использовании основных методов и средств технической защиты информации

навыками применения руководящих и нормативных документов по инженерно-технической защите информации

навыками программирования прикладных задач

ПСК-1.1: Способностью участвовать в разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах

Знать:

методы защиты компьютерной информации

классификацию и общую характеристику программно-аппаратных средств защиты информации

основные принципы администрирования защищенных компьютерных систем

Уметь:

выполнять защиту рабочих мест с использованием программно-аппаратных средств защиты информации

выполнять функции администратора безопасности защищенных компьютерных систем

выполнять настройку защитных механизмов программно-аппаратных средств

Владеть:

средствами администрирования программно-аппаратных комплексов защиты информации от несанкционированного доступа

средствами администрирования комплексов криптографической защиты информации

средствами администрирования средств организации виртуальных частных сетей

ПСК-1.2: Способностью использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований

Знать:

| |
|--|
| основные математические методы обработки |
| основные математические методы анализа и синтеза результатов |
| основные проблемы в применении математических методов |
| Уметь: |
| применять методы математической обработки |
| применять методы математического анализа и синтеза результатов |
| применять математические методы при исследовании и проектировании систем |
| Владеть: |
| методами математической обработки |
| методами математического анализа и синтеза результатов |
| методами математических методов при исследовании и проектировании систем |

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

| Код занятия | Наименование разделов и тем | Вид занятий | Семестр / Курс | Часов | Интеракт. |
|-------------|---|-------------|----------------|-------|-----------|
| | Раздел 1. Раздел 1. Компьютерная безопасность и защита информации как учебная дисциплина. Основные термины и определения | Раздел | | | |
| 1.1 | Тема 1. Понятия компьютерной безопасности | Лек | 7 | 2 | 2 |
| 1.2 | Тема 1. Понятия компьютерной безопасности | Лаб | 7 | 4 | 0 |
| 1.3 | Тема 1. Понятия компьютерной безопасности | Ср | 7 | 6 | 0 |
| 1.4 | Тема 2. Виды угроз информационной безопасности и характеристика информационных атак | Лек | 7 | 2 | 2 |
| 1.5 | Тема 2. Виды угроз информационной безопасности и характеристика информационных атак | Лаб | 7 | 4 | 0 |
| 1.6 | Тема 2. Виды угроз информационной безопасности и характеристика информационных атак | Ср | 7 | 4 | 0 |
| 1.7 | Тема 3. Понятия информационных угроз и информационной безопасности. Базовые признаки классификации информационных угроз. | Лек | 7 | 2 | 2 |
| 1.8 | Тема 3. Понятия информационных угроз и информационной безопасности. Базовые признаки классификации информационных угроз. | Лаб | 7 | 4 | 0 |
| 1.9 | Тема 3. Понятия информационных угроз и информационной безопасности. Базовые признаки классификации информационных угроз. | Ср | 7 | 6 | 0 |
| 1.10 | Рубежный контроль | Лаб | 7 | 2 | 0 |
| | Раздел 2. Раздел 2: Утечка информации по техническим каналам | Раздел | | | |
| 2.1 | Тема 1: . Основные типы моделей управления доступом. Принципы системности, комплексности, непрерывности защиты, разумной достаточности, гибкости управления, открытости алгоритмов. | Лек | 7 | 2 | 2 |

| | | | | | |
|------|---|--------|---|---|---|
| 2.2 | Тема 1: . Основные типы моделей управления доступом. Принципы системности, комплексности, непрерывности защиты, разумной достаточности, гибкости управления, открытости алгоритмов. | Лаб | 7 | 4 | 0 |
| 2.3 | Тема 1: . Основные типы моделей управления доступом. Принципы системности, комплексности, непрерывности защиты, разумной достаточности, гибкости управления, открытости алгоритмов. | Ср | 7 | 6 | 0 |
| 2.4 | Тема 2:Криптографические методы защиты .Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Электронная цифровая подпись | Лек | 7 | 2 | 0 |
| 2.5 | Тема 2:Криптографические методы защиты .Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Электронная цифровая подпись | Лаб | 7 | 4 | 0 |
| 2.6 | Тема 2:Криптографические методы защиты .Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Электронная цифровая подпись | Ср | 7 | 6 | 0 |
| 2.7 | Тема 3: Аутентификация, авторизация и администрирование. Методы аутентификации, использующие пароли. Строгая аутентификация. Биометрическая аутентификация пользователей. | Лек | 7 | 2 | 0 |
| 2.8 | Тема 3: Аутентификация, авторизация и администрирование. Методы аутентификации, использующие пароли. Строгая аутентификация. Биометрическая аутентификация пользователей. | Лаб | 7 | 2 | 0 |
| 2.9 | Тема 3: Аутентификация, авторизация и администрирование. Методы аутентификации, использующие пароли. Строгая аутентификация. Биометрическая аутентификация пользователей. | Ср | 7 | 6 | 0 |
| 2.10 | Рубежный контроль | Лаб | 7 | 2 | 0 |
| | Раздел 3. Раздел 3 Технологии применяемые для защиты электронных и компьютерных сетей и баз данных | Раздел | | | |
| 3.1 | Тема 1:Методы управления средствами сетевой безопасности. Задачи управления информационной безопасностью. Архитектура управления информационной безопасностью. | Лек | 7 | 2 | 0 |

| | | | | | |
|------|---|----------|---|---|---|
| 3.2 | Тема 1:Методы управления средствами сетевой безопасности. Задачи управления информационной безопасностью. Архитектура управления информационной безопасностью. | Лаб | 7 | 2 | 0 |
| 3.3 | Тема 1:Методы управления средствами сетевой безопасности. Задачи управления информационной безопасностью. Архитектура управления информационной безопасностью. | Ср | 7 | 6 | 0 |
| 3.4 | Тема 2:Технологии межсетевых экранов. Функции межсетевых экранов. Особенности функционирования межсетевых экранов. Схемы сетевой защиты на базе межсетевых экранов. | Лек | 7 | 2 | 0 |
| 3.5 | Тема 2:Технологии межсетевых экранов. Функции межсетевых экранов. Особенности функционирования межсетевых экранов. Схемы сетевой защиты на базе межсетевых экранов. | Лаб | 7 | 2 | 0 |
| 3.6 | Тема 2:Технологии межсетевых экранов. Функции межсетевых экранов. Особенности функционирования межсетевых экранов. Схемы сетевой защиты на базе межсетевых экранов. | Ср | 7 | 6 | 0 |
| 3.7 | Тема 3: Сбор информации системами обнаружения атак. Методы обнаружения информационных атак. Противодействие информационным атакам. | Лек | 7 | 2 | 0 |
| 3.8 | Тема 3: Сбор информации системами обнаружения атак. Методы обнаружения информационных атак. Противодействие информационным атакам. | Лаб | 7 | 4 | 0 |
| 3.9 | Тема 3: Сбор информации системами обнаружения атак. Методы обнаружения информационных атак. Противодействие информационным атакам. | Ср | 7 | 6 | 0 |
| 3.10 | Рубежный контроль | Лаб | 7 | 2 | 0 |
| 3.11 | Итоговое занятие | ЗачётСОц | 7 | 2 | 0 |

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания для текущей аттестации

Оценочные материалы для проведения текущего контроля по дисциплине "Теоретические основы компьютерной безопасности" рассмотрены и одобрены на заседании кафедры от «30» марта 2017 г. протокол №8, является приложением к рабочей программе.

5.2. Фонд оценочных средств для промежуточной аттестации

Оценочные материалы для проведения промежуточного контроля по дисциплине "Теоретические основы компьютерной безопасности" рассмотрены и одобрены на заседании кафедры 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- |
|--|----------|-----------|------|
|--|----------|-----------|------|

| | Заглавие | Эл. адрес | Кол- |
|--|---|---|------|
| Л1.1 | Галатенко В. А. - Основы информационной безопасности: учебное пособие - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. | http://www.iprbookshop.ru/22424 | 1 |
| 6.1.2. Дополнительная литература | | | |
| | Заглавие | Эл. адрес | Кол- |
| Л2.1 | Фаронов А. Е. - Основы информационной безопасности при работе на компьютере: учебное пособие - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. | http://www.iprbookshop.ru/16711 | 1 |
| 6.3.1 Перечень программного обеспечения | | | |
| 7.3.1.1 | 198: | | |
| 7.3.1.2 | MacOS 10.11(Документы о приобретении iMac 21.5") | | |
| 7.3.1.3 | OracleVMVirtualBox (Свободная лицензия 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 | Adobe Acrobat Reader DC (Бесплатное программное обеспечение) | | |
| 7.3.1.7 | 7-Zip (Свободная лицензия GNU GPL) | | |
| 7.3.1.8 | GoogleChrome (Свободная лицензия BSD) | | |
| 7.3.1.9 | FlatAssembler (Свободное программное обеспечение лицензия BSD с возможно анти-GPL) | | |
| 7.3.1.10 | VisualStudioCommunity (Проприетарная академическая лицензия) | | |
| 7.3.1.11 | Code::Blocks (Свободная лицензия GNU GPLv3) | | |
| 7.3.1.12 | EclipseNeon (Открытое программное обеспечение EclipsePublicLicense) | | |
| 7.3.1.13 | | | |
| 7.3.1.14 | 146: | | |
| 7.3.1.15 | Microsoft Windows 7 (OpenLicense: 47818817) | | |
| 7.3.1.16 | Ms OfficeProfessional 2007 (OpenLicense: 47818817) | | |
| 7.3.1.17 | Google Chrome (Свободная лицензия BSD) | | |
| 7.3.1.18 | 7-Zip (Свободная лицензия GNU LGPL) | | |
| 7.3.1.19 | Adobe Acrobat Reader DC (Бесплатное программное обеспечение) | | |
| 6.3.2 Перечень информационных справочных систем | | | |
| 7.3.2.1 | | | |
| 7.3.2.2 | Каталог библиотеки КГУ. - Режим доступа: http://195.93.165.10:2280 | | |
| 7.3.2.3 | Электронная библиотека. - Режим доступа: http://elibrary.ru | | |
| 7.3.2.4 | Университетская информационная система «Россия» – http://uisrussia.msu.ru | | |
| 7.3.2.5 | Электронная библиотечная система «КнигаФонд» – http://www.knigafund.ru/ | | |
| 7.3.2.6 | Электронная библиотечная система издательства «Лань» – http://e.lanbook.com/ | | |
| 7.3.2.7 | Электронная библиотечная система «IPRbooks» – http://www.iprbookshop.ru/ | | |

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

| | |
|-----|---|
| 7.1 | Компьютерная аудитория : учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы, |
| 7.2 | 305000, Курская область, г. Курск, ул. Радищева, д. № 33, 198. |
| 7.3 | Интерактивная доска – 1 шт. |
| 7.4 | Доска Классная – 1 шт. |
| 7.5 | Apple iMac 21.5 – 15 шт. |
| 7.6 | Коммутатор 24порт. – 1 шт. |

| | |
|------|--|
| 7.7 | |
| 7.8 | Помещение для самостоятельной работы обучающихся – аудитория, оснащенная компьютерной техникой с возможностью подключения к сети "Интернет" и с обеспечением доступа в электронную информационно-образовательную среду университета. |
| 7.9 | 305000, Курская область, г. Курск, ул. Радищева, д. № 33, 146. |
| 7.10 | Столов – 61 |
| 7.11 | Посадочных мест – 162 |
| 7.12 | Компьютеров: |
| 7.13 | Для пользователей – 40 |
| 7.14 | Для библиотекаря – 2 |
| 7.15 | Моноблоков MSI (27) - модель MS-A912, 2Гб оперативной памяти, Athlon CPU D525 1.80GHz |
| 7.16 | 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, имеющимися 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 занятиям семинарского типа

Практические занятия имеют следующую структуру:

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

«Методические указания по подготовке к практическим занятиям по дисциплине "Теоретические основы компьютерной безопасности" 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 "Теоретические основы компьютерной безопасности"» 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.