Министерство образования и науки РФ

Государственное образовательное учреждение высшего профессионального образования

**«Санкт-Петербургский государственный электротехнический университет “ЛЭТИ” им. В.И. Ульянова (Ленина)» (СПбГЭТУ)**

РАБОЧАЯ ПРОГРАММА

дисциплины

*«Методы нарушения безопасности и вирусология»*

Для подготовки дипломированных специалистов по специальности 090301.65

*«Компьютерная безопасность»*

# Санкт-Петербург

2011

# Санкт-Петербургский государственный электротехнический

университет “ЛЭТИ”

### “УТВЕРЖДАЮ”

Проректор по учебной работе

Лысенко Н.В.

“\_\_\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2011 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

*«Методы нарушения безопасности и вирусология»*

Для подготовки дипломированных специалистов по специальности 090301.65

*«Компьютерная безопасность»*

Факультет компьютерных технологий и информатики

Кафедра автоматизированных систем обработки информации и управления

Курс – 5

Семестр – 9

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Лекции | 54 ч. |  | Экзамен | Семестр 9 |
| Лабораторные занятия | 36 ч. |  | Зачет | Семестр 9 |
| Практические занятия | 18 ч. |  |  |  |

|  |  |  |
| --- | --- | --- |
| Аудиторные занятия | 108 ч. |  |
| Самостоятельные занятия | 62 ч. |  |
| Всего часов | 170 ч. |  |

|  |  |
| --- | --- |
|  |  |

2011

Рабочая программа обсуждена на заседании кафедры автоматизированных систем обработки информации и управления“\_\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2011 г., протокол №\_\_\_\_\_\_.

Рабочая программа составлена в соответствии с государственным образовательным стандартом для дипломированных специалистов по специальности

090301.65 – «Компьютерная безопасность»

Дисциплина «МНБ и вирусология» преподается на основе ранее изученных дисциплин:

1) Программирование

2) Организация ЭВМ и систем

3) Инфокоммуникационные системыисети

4) Криптографические методы защиты информации

и обеспечивает изучение следующи дисциплин:

1. Защита КС и ТК
2. Защита ОС и СУБД
3. Технология разработки ИС в ЗИ

Рабочая программа одобрена методической комиссией факультета компьютерных технологий и информатики “\_\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_2011г.

**АННОТАЦИЯ ДИСЦИПЛИНЫ**

Дисциплина «*Методы нарушения безопасности и вирусология*» направлена на развитие системного мышления студентов, приобретение ими знаний по основным направлениям защиты информации, и навыков, которые будут необходимы при изучении других специальных дисциплин в области защиты информации и в практической деятельности выпускников.

**Цели и задачи дисциплины**

**Целью дисциплины** является формирование знаний о моделях безопасности информационных систем, приемах проведения атак, признаках их обнаружениях, источниках информации о существующих атаках и уязвимостях вычислительных систем; формирование практических навыков по обнаружению атак и методам организации защиты информации в вычислительных системах.

**Основными задачами** дисциплины являются:

1. дать представление об основных задачах, решаемых компьютерной вирусологией, дать представление об алгоритмических аспектах проблемы обнаружения вредоносного программного обеспечения;
2. дать основы по существующим шаблонам, способам и средствам проведения атак;
3. дать основы по общим принципам функционирования вредоносных программ, их классификации
4. дать основы о существующих уязвимостях ПО, методах и средствах обнаружения и устранения
5. дать навыки по формированию критериев к выбору, настройке и эксплуатации систем обнаружения атак;
6. развить умение самостоятельно изучать новые результаты и разработки в области компьютерной вирусологии и систем обнаружения атак и антивирусного обеспечения

**Требования к уровню освоения дисциплины**

Изучение дисциплины направлено на формирование вклада в следующие компетенции:

*ПК-10 –* способность формулировать результат проведенных исследований в виде конкретных рекомендаций, выраженных в терминах предметной области изучавшегося явления;

*ПК-11 –* способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в КС;

*ПК-13* – способность организовывать антивирусную защиту информации при работе с КС;

*ПК-15* – способность применять современные методы и средства исследования для обеспечения ИБ КС;

*ПК-16* – способность проводить анализ безопасности КС с использованием отечественных и зарубежных стандартов в области КБ;

*ПК-17* – способность готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ;

*ПК-19* – способность проводить обоснование и выбор рационального решения по уровню защищенности КС с учетом заданных требований;

*ПК-20* – способность проводить анализ и формализацию поставленных задач в области КБ;

*ПК-21* – способность проводить сбор и анализ исходных данных для проектирования систем защиты информации;

*ПК-22* – способность участвовать в разработке проектной документации;

*ПК-23* – способность проводить анализ проектных решений по обеспечению защищенности КС;

*ПК-24* – способность участвовать в разработке СЗИ предприятия (организации) и подсистемы ИБ КС;

*ПК-25* – способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи;

*ПК-31* – способность разрабатывать оперативные планы работы первичных подразделений;

*ПК-32* – способность разрабатывать предложения по совершенствованию системы управления ИБ КС;

*ПСК-8.1* – способность разрабатывать модели угроз и модели нарушителя информационной безопасности конкретных объектов информатизации на базе КС в защищенном исполнении;

*ПСК-8.2* – способность на основании моделей угроз моделей нарушителя информационной безопасности формировать требования к обеспечению ИБ объектов информатизации на базе КС в защищенном исполнении;

*ПСК-8.3* – способность на основании требованию к обеспечению ИБ формировать перечень функций безопасности объекта информатизации на базе КС в защищенном исполнении и выбирать рациональные способы и средства их реализации;

*ПСК-8.4* – способность разрабатывать проектные решения по системам обеспечения ИБ ОИ на базе КС в защищенном исполнении;

*ПСК-8.5* – способность проводить анализ систем обеспечения ИБ ОИ на базе КС в защ.исполнении на предмет их соответствия требованиям по обеспечению ИБ;

*ПСК-8.6* – способность обеспечить ИБ процессов проектирования, создания, модернизации ОИ на базе КС в защ.исполнении;

В результате изучения дисциплины студенты должны:

1. *знать* виды информационных угроз, шаблоны проведения атак и средства для их реализации, основные принципы функционирования вредоносного программного обеспечения, основные типы и виды уязвимостей программного обеспечения, методы и средства по их устранению,
2. *уметь* выбрать и построить инфраструктуру обнаружения атак в зависимости от целей и задач политики безопасности,
3. *иметь* *представление* об основных направлениях развития теории компьютерной вирусологии, об открытых современных проблемах в этой области.

#### Содержание рабочей программы

**Тема 1. Информационная безопасность и основные понятия**

Информационная безопасность (ИБ), основные составляющие ИБ. Понятие угрозы ИБ, несанкционированного доступа, классификация атак. Модели безопасности информационных систем. Законодательные акты в области компьютерных преступлений.

**Тема 2. Теоретические основы компьютерной вирусологии**

Машина Тьюринга и рекурсивные функция (понятия и определения, примеры). Формальная модель компьютерного вируса Ф. Коэна, модели безопасности Ф.Коэна. Концепция вредоносного программного обеспечения Л. Адельмана. Проблема обнаружения компьютерных вирусов (теория Д. Чесса, С. Уайта). Вычислительная сложность обнаружения компьютерных вирусов.

**Тема 3. Терминология вредоносного программного обеспечения (ПО)**

Терминология и основные виды вредоносного ПО. Проблематика унификации наименования вредоносного ПО. Причины успешного распространения вредоносных программ и MMPC. Архитектурно – платформенная зависимость вредоносных программ.

**Тема 4. Существующие классификации вредоносного ПО**

Классификация по стратегиям заражения. Классификация по стратегиям расположения в памяти. Классификация по вредоносной нагрузке.

**Тема 5. Базовые методы самозащиты вредоносного ПО от обнаружения антивирусным ПО**

Тунеллирующие вирусы: задачи и способы реализации. Бронированные вирусы. Агрессивные ретровирусы.

**Тема 6. Усовершенствованные методы самозащиты вредоносного ПО от обнаружения антивирусным ПО**

Самошифрующиеся вирусы. Полиморфные вирусы, уровни полиморфизма. Метаморфные вирусы. Вирусные генераторы.

**Тема 7. Компьютерные черви**

Структура и основные компоненты компьютерных червей. Стратегии поиска цели и распространения. Компьютерная эпидемиология: основные понятия и базовые модели.

**Тема 8. Уязвимости ПО**

Понятие уязвимости. Основные ошибки программирования (с примерами). Пример использования уязвимости Apache 1.3. (переполнение буфера) на основе атаки червя Linux/Slapper.

**Тема 9. Сканеры антивирусного программного обеспечения**

Определение антивирусных программ, функциональная структура. Сканеры 1,2,3-го поколения. Эвристический анализ для обнаружения win32 вирусов

**Тема 10. Современные системы обнаружения вредоносного ПО**

Системы контроля целостности. Поведенческие блокираторы. Антивирусные песочницы.

**Тема 11. Сетевые методы обнаружения атак**

Системы обнаружения вторжений: классификация, принципы. Сканеры безопасности. Обманные системы.

**Перечень лабораторных работ**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Наименование работы | Номер темы | Трудоемкость |
| 1 | Изучение самовоспроизводящихся клеточных автоматов | **2** | **4** |
| 2 | Изучение структуры исполняемого файла формата PE | **3,5,6,7** | **13** |
| 3 | Разработка самовоспроизводящейся программы | **3,4,5,6** | **13** |
| 4 | Обнаружение вредоносного ПО стандартными средствами ОС Windows | **8,9,10** | **6** |

**Перечень практических занятий**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Наименование работы | Номер темы | Трудоемкость |
| 1 | Самовоспроизводящиеся клеточные автоматы | **2** | **3** |
| 2 | Структура исполняемого файла формата PE | **3,5,6,7** | **6** |
| 3 | Самовоспроизводящиеся программы | **3,4,5,6** | **6** |
| 4 | Обнаружение вредоносного ПО | **8,9,10** | **3** |

**Распределение учебных часов по темам и видам занятий**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| №  темы | Название разделов и тем | Объем учебных часов | | | | | | | Семестр | Литература по темам |
| Лекции | Лаб.  занят. | Пр.занят. | Аудит.  занят. | | Сам.  работа | Всего |
| Всего | в т.ч. инт.формы |
| 1 | Информационная безопасность и основные понятия | 4 |  |  | 4 |  |  | 4 | 9 | Л1, Л3, Д2, Э5 |
| 2 | Теоретические основы компьютерной вирусологии | 8 | 4 | 3 | 15 | 3 | 6 | 21 | 9 | Л1,Д2, Э5, Д5 |
| 3 | Терминология вредоносного программного обеспечения (ПО) | 4 | 5 | 2 | 11 | 2 | 8 | 19 | 9 | Л2, Д1, Д3, Э2, Э5 |
| 4 | Существующие классификации вредоносного ПО | 6 | 5 | 2 | 13 | 2 | 8 | 21 | 9 | Л1, Л3, Д3, Э5, Д5 |
| 5 | Базовые методы самозащиты вредоносного ПО от обнаружения антивирусным ПО | 4 | 6 | 3 | 13 | 3 | 8 | 11 | 9 | Л2, Л3, Д1, Д3, Э4, Э5 |
| 6 | Усовершенствованные методы самозащиты вредоносного ПО от обнаружения антивирусным ПО | 4 | 5 | 3 | 12 | 3 | 8 | 20 | 9 | Л2, Л3, Д1, Д3, Э4, Э5 |
| 7 | Компьютерные черви | 4 | 5 | 2 | 11 | 2 | 8 | 19 | 9 | Л1, Л2, Э5 |
| 8 | Уязвимости ПО | 8 | 2 | 1 | 11 | 1 | 6 | 17 | 9 | Л2, Д1, Э1, Э2, Э3 |
| 9 | Сканеры антивирусного программного обеспечения | 4 | 2 | 1 | 7 | 1 | 6 | 13 | 9 | Л2, Л3, Д1, Д3, Э4, Э5 |
| 10 | Современные системы обнаружения вредоносного ПО | 4 | 2 | 1 | 7 | 1 | 4 | 11 | 9 | Л2, Л3, Д1, Д3, Э4, Э5 |
| 11 | Сетевые методы обнаружения атак | 4 |  |  | 4 |  |  | 4 | 9 | Л1, Л3, Д4, Э5 |
| ИТОГО: | | 54 | 36 | 18 | 108 | 18 | 62 | 170 |  |

.

# **Учебно-методическое обеспечение дисциплины**

# **Основная литература**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Название,библиографическое описание | Л | Лр | Пз(С) | Кп (р) | Инд.  зад. | К-воэкз.в библ.(на каф.) | Гриф |
| **Л1** | Олифер В.Г., Олифер Н.А.  Компьютерные сети: Принципы протоколы, технологии, 4- изд СПб БХВ-Питер 2010. | 9 | 9 | 9 |  |  | Ф(2)  ЧЗ1(2) | Мино  бразо  вания РФ |
| **Л2** | Белов Е.Б Основы информационной безопасности: Учебное пособие для вузов М. Горячая линия –Телеком 2006 | 9 | 9 | 9 |  |  | Ф(2)ЧЗ1(2) | Миноразования РФ |
| **Л3** | Данжани Н. Кларк Дж.Средства сетевой безопасности. М. Кудиц-Пресс 2007 | 9 | 9 | 9 |  |  | Ф(2)ЧЗ1(2) |  |

##### **Дополнительная литература**

|  |  |  |
| --- | --- | --- |
| № | Название, библиографическое описание | К-во экз.в библ.(на каф.) |
| **Д1** | Касперски К. Рокко Е. Искусство дизассемблирования. СПб.: «БХВ-Петербург» 2008 г. | нет |
| **Д2** | Роджерс Х. Теория рекурсивных функций и эффективная вычислимость. М.Мир 1972г | нет |
| **Д3** | Гошко С. В. Технологии борьбы с компьютерными вирусами М.: Солон-Пресс 2009 г. | нет |
| **Д4** | Лукацкий А.В. Обнаружение атак. СПб.: «БХВ-Петербург» 2003 г. | У(7) |
| **Д5** | Касперски К. Компьютерные вирусы изнутри и снаружи СПб.:Питер 2006 г. | нет |

|  |  |
| --- | --- |
|  |  |

**Электронные информационные ресурсы**

|  |  |
| --- | --- |
| № | Название (адрес в Интернет) |
| **Э1** | www.sans.org |
| **Э2** | [www.mitre.org](http://www.mitre.org/) |
| **Э3** | [www.owasp.org](http://www.owasp.org/) |
| **Э4** | [www.uinc.ru/articles/](http://www.uinc.ru/articles/) |
| **Э5** | www.vxheavens.com |

|  |  |
| --- | --- |
|  |  |
| Авторы:  к.т.н., ассистент | Новикова Е.С. |
|  |  |
| Рецензент:  к.т.н., доцент | Власенко С.В. |
|  |  |
| Зав. кафедрой АСОИУ,  д.т.н., профессор | Советов Б.Я. |
|  |  |
| Декан факультета КТИ,  д.т.н., профессор | Куприянов М.С. |
|  |  |
| Программа согласована: |  |
| Председатель методической комиссии факультета компьютерных технологий и информатики, к.т.н., доцент | Михалков В.А. |
|  |  |
| Руководитель методического отдела |  |
| к.т.н., доцент | Марасина Л.А. |