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

*«Защита компьютерных сетей и телекоммуникаций»*

Для подготовки дипломированных специалистов по специальности 090102.65

*«Компьютерная безопасность»*

Санкт-Петербург

2011

# Санкт-Петербургский государственный электротехнический

университет “ЛЭТИ”

### “УТВЕРЖДАЮ”

Проректор по учебной работе

Лысенко Н.В.

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

РАБОЧАЯ ПРОГРАММА

дисциплины

*«Защита компьютерных сетей и телекоммуникаций»*

Для подготовки дипломированных специалистов по специальности 090102.65

*«Компьютерная безопасность»*

Уч.план. № 339

Факультет компьютерных технологий и информатики

Кафедра автоматизированных систем обработки информации и управления

Курс – 5

Семестр – 10

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Лекции | 34 ч. |  | Экзамен | Семестр 10 |
|  |  |  |  |  |
| Лабораторные занятия | 17 ч. |  | Зачет | Семестр 10 |
| Курсовая работа | 17 ч. |  | Курсовая работа | Семестр 10 |

|  |  |  |
| --- | --- | --- |
| Аудиторные занятия | 68 ч. |  |
| Самостоятельные занятия | 52 ч. |  | |
| Всего часов | 120 ч. |  |

|  |
| --- |
|  |

2011

Рабочая программа обсуждена на заседании кафедры автоматизированных систем обработки информации и управления“\_\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2011г., протокол №\_\_\_\_\_\_.

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

090102.65 – «Компьютерная безопасность»

Дисциплина «Защита КС и ТК» преподается на основе ранее изученных дисциплин:

1) Операционные системы

2) Организация ЭВМ и систем

3) Сети ЭВМ и ТК

4) Архитектура современных ЭВМ

5) Криптографические методы защиты информации

и обеспечивает выполнение ВКР.

Рабочая программа одобрена методической комиссией факультета компьютерных технологий и информатики «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2011 г.

**АННОТАЦИЯ ДИСЦИПЛИНЫ**

Дисциплина «Защита компьютерных сетей и телекоммуникаций» посвящена изучению принципов организации защиты информации в программных и аппаратных средствах на основе криптографических алгоритмов и протоколов. В рамках данной дисциплины рассматриваются базовые принципы обеспечения защиты информации. Отдельные разделы дисциплины посвящены изучению: криптографических алгоритмов, характеристик уязвимостей СУБД, методов защиты СУБД, принципов работы и архитектуре частных виртуальных сетей.

**Цели и задачи дисциплины**

Приобретение знаний в области современных методов защиты информации. Формирование навыков обоснованно выбирать готовые средства защиты, комплексно оценивать угрозы и обеспечивать необходимый уровень защиты информации при проектировании автоматизированных систем обработки информации и управления.

**Требования к уровню освоения дисциплины**

В результате изучения дисциплины студенты должны:

Знать:

* основные принципы и методы защиты информации в компьютерных сетях и телекоммуникациях;
* основные режимы работы криптографического алгоритма по ГОСТ 28147-89;
* основные требования к генерации случайных и псевдослучайных последовательностях;
* основные принципы построения и функционирования межсетевых экранов и частных виртуальных сетей;

Уметь:

* оптимально выбирать алгоритмы, протоколы и средства защиты для обеспечения безопасности компьютерных сетей и телекоммуникаций;

Владеть:

* навыками в области выбора, проектирования и разработки проектных решений для обеспечения безопасности компьютерных сетей и телекоммуникаций.

**Содержание рабочей программы**

**Введение**

Угрозы безопасности информации в компьютерных сетях и телекоммуникациях.

Обзор основных криптографических алгоритмов.

Основы проектирования криптографических средств защиты информации.

**Тема 1. Криптографический алгоритм по ГОСТ 28147-89**

Обзор и основные параметры, характеристики и область применения криптографического алгоритма по ГОСТ 28147-89.

Схема построения и основные режимы работы криптографического алгоритма по ГОСТ 28147-89.

**Тема 2. Защита СУБД**

Основы защиты СУБД. Атаки на СУБД. Атаки сетевого уровня.

Атаки прикладного уровня. Особенности выполнения команд операционной системы Microsoft SQL, Oracle и DB2. Защита от атак на уровне SQL.

Криптографическая защита СУБД.

**Тема 3. VPN**

Введение в технологию Виртуальных частных сетей (VPN).

Преимущества и недостатки VPN.

Преимущества глобального доступа.

Архитектура VPN.

Топологии VPN.

Безопасность VPN.

**Тема 4. Случайные и псевдослучайные последовательности**

Основные требования к генерации случайных и псевдослучайных последовательностей.

Схема генерации случайного ключа по стандарту ANSI X9.17. Требования к датчикам случайных чисел.

**Тема 5. Межсетевой экран**

Методы и средства защиты от удаленных атак через сеть Internet.

Особенности функционирования межсетевых экранов (МЭ).

Основные компоненты МЭ.

Основные схемы сетевой защиты на базе МЭ.

**Тема 6. Несанкционированный доступ к информации**

Основные требования к средствам защиты информации от несанкционированного доступа (СЗИ НСД) к информации.

**Перечень лабораторных работ**

|  |  |  |
| --- | --- | --- |
| № п.п. | Наименование лабораторных работ | Номер темы |
| 1 | Моделирование и ознакомление с работой режима гаммирования ГОСТ 28147-89 | 1 |
| 2 | Моделирование и ознакомление с работой режима гаммирования с обратной связью ГОСТ 28147-89 | 1 |
| 3 | Моделирование и ознакомление с работой режима выработки лимитов ставки  ГОСТ 28147-89 | 1 |
| 4 | Практическая работа и ознакомление с работой VPN | 3 |
| 5 | Практическая работа и ознакомление с работой MЭ на примере FW-Windows XP | 5 |
| 6 | Изучение принципов работы СЗИ НСД «ЩИТ РЖД» | 6 |
| 7 | Изучение принципов работы криптографической подсистемы СЗИ НСД «ЩИТ РЖД» | 6 |

**Цели и содержание курсовой работы**

Целью предлагаемой курсовой работы является разработка документации на средства защиты информации.

В качестве основных тем предлагаются следующие:

1. Разработка и описание работы криптографического средства защиты файлов на основе ГОСТ 28147-89 в режиме гаммирования.
2. Разработка и описание работы криптографического средства защиты файлов на основе ГОСТ 28147-89 в режиме гаммирования с обратной связью.
3. Разработка проекта технического задания на создание VPN.
4. Разработка технического задания на создание межсетевого экрана.
5. Разработка технического задания на создание криптографического иммобилайзера.
6. Разработка технического задания на создание СЗИ НСД.

Ориентировочная трудооемкость — 35 часов.

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

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| №  темы | Название разделов и тем | Объем учебных часов | | | | | | Семестр | **Литература по темам** |
| Лекции | Лабор.  занят. | К/р | Аудит.  занят. | Самост.  работа | **Всего** |
| 1 | Криптографический алгоритм по ГОСТ 28147-89 | 5 | 4 | 3 | 12 | 9 | 21 | 10 | **Л1, Д1, Д2, Д3, Д4** |
| 2 | Защита СУБД | 6 |  | 3 | 9 | 9 | 18 | 10 | **Л1, Д1, Д2, Д3, Д4** |
| 3 | VPN | 6 | 4 | 2 | 12 | 7 | 19 | 10 | **Л1, Д1, Д2, Д3, Д4** |
| 4 | Случайные и псевдослучайные последовательности | 6 |  | 3 | 9 | 9 | 18 | 10 | **Л1, Д1, Д2, Д3, Д4** |
| 5 | Межсетевой экран | 6 | 5 | 3 | 14 | 9 | 23 | 10 | **Л1, Д1, Д2, Д3, Д4** |
| 6 | Несанкционированный доступ к информации | 5 | 4 | 3 | 12 | 9 | 21 | 10 | **Л1, Д1, Д2, Д3, Д4** |
| **ИТОГО:** | | 34 | 17 | 17 | 68 | 52 | 120 |  |

# **Учебно-методическое обеспечение дисциплины**

# **Основная литература**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Название, библиографическое описание | Л | Лр | Пз (С) | Кп | Кр | К-во экз. в библ. (на каф.) | Гриф |
| **Л1** | Брюс Шнайер. Прикладная криптография. | 10 | 10 |  |  | 10 | Ф(2) |  |

##### Дополнительная литература

|  |  |  |
| --- | --- | --- |
| № | Название, библиографическое описание | К-во экз. в библ. (на каф.) |
| **Д1** | Браун С. Виртуальные частные сети.-М.- Лори, 2001.- 491с. | нет |
| **Д2** | Баричев С., Серов Р. Основы современной криптографии. - М. - Горячая линия — Телеком, 2001. - 122с. | Ф(2)  ЧЗ1(1) |
| **Д3** | ГОСТ 28147-89, Криптографический алгоритм.-1989. - 34с. | нет |
| **Д4** | Козиол Дж., Личфилд Д., Эйтел Д., Энли К., Эрен С., Мехта Н., Хассель Р. Искусство взлома и защиты систем.-СПб.-Питер,2006.- 416с.:ил. | нет |

|  |  |
| --- | --- |
| Зав. отделом учебной литературы *(для технических дисциплин)* | Киселева Т.В |
|  |  |
|  |  |

|  |  |
| --- | --- |
| Авторы:. к.т.н., доцент | Молдовяну П.А. |
|  |  |
| Рецензент: д.т.н., профессор | Воробьев В.И. |
|  |  |
| 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. |