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

*«Технические средства и методы защиты информации»*

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

*«Технические средства и методы защиты информации»*

для подготовки дипломированных специалистов по специальности 090301.65 *«Компьютерная безопасность»*

Учебный план № 836

Факультет компьютерных технологий и информатики

Кафедра автоматизированных систем обработки информации и управления

Курс – 4

Семестр – 8

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Лекции | 36 ч. |  | Экзамен | Семестр 8 |
| Лабораторные занятия | 36 ч. |  |  |  |
| Практические занятия | 18 ч. |  |  |  |

|  |  |  |
| --- | --- | --- |
| Аудиторные занятия | 90 ч. |  |
| Самостоятельные занятия | 80 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 «Технические средства и методы защиты информации» преподается на основе ранее изученных дисциплин:

1) Физика

2) Теоретические основы информатики

3) Теоретические основы электротехники

4) Основы информационной безопасности

и является фундаментом для изучения последующих дисциплин:

1) Защита компьютерных сетей и телекоммуникаций

2) Организационно-правовое обеспечение информационной безопасности

3) Инженерно-техническая защита объектов информатизации

Рабочая программа одобрена методической комиссией факультета компьютерных технологий и информатики “\_\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_2011 г.

**АННОТАЦИЯ ДИСЦИПЛИНЫ**

Курс **«**Технические средства и методы защиты информации» предназначен для подготовки дипломированных специалистов по специальности 090102.65 – «Компьютерная безопасность». Программа курса рассчитана на выполнение в течении 1 семестра (8 семестр обучения) и включает в себя лекционный курс и лабораторный практикум. Оценкой освоения студентами программы лабораторного практикума является зачет, а всего курса – экзамен.

Курс рассчитан на студентов, имеющих базовые знания в области физики, теории информации, электроники и схемотехники и основ информационной безопасности. Программа курса включает в себя изучение задач защиты информации от утечки по техническим каналам. Лекционный курс содержит как материалы прикладного характера по противодействию технической разведке, так и материалы теории защиты. Рассматриваются вопросы характеристики технических каналов утечки информации и классификации технической разведки, возможности ее видов. Уделяется внимание вопросам скрытия речевой информации в каналах связи, подавления опасных сигналов. Лекционные материалы курса по каждому разделу подкрепляются примерами обнаружения и локализации закладных устройств.

Успешное усвоение материалов курс является основой для последующего изучения дисциплин по проектированию систем технической защиты различного назначения.

**Цели и задачи дисциплины**

1. Изучение основ защиты информации от утечки по техническим каналам.
2. Формирование навыков расчета и инструментального контроля показателей защиты информации.

**Требования к уровню освоения дисциплины**

Изучение дисциплины направлено на формирование вклада в следующие компетенции:

*ПК-1* – способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и применять соответствующий физико-математический аппарат для их формализации, анализа и выработки решения;

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

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

*ПК-24* – способность участвовать в разработке систем защиты информации предприятия (организации) и подсистемы информационной безопасности компьютерных систем;

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

*ПК-26* – способность участвовать в проведении экспериментально-исследовательских работ при аттестации СЗИ с учетом требований к уровню защищенности компьютерных систем;

*ПК-27* – способность к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей;

*ПК-28* – способность обосновывать правильность выбранной модели решения проф.задачи, сопоставлять экспериментальные данные и теоретические решения;

*ПК-29* – способность оценивать эффективности систем защиты информации в компьютерных системах;

*ПК-36* – способность производить проверку технического состояния и профилактические осмотры оборудования по защите информации;

*ПК-37* – способность выполнять работы по приему, настройке, регулировке, освоению и восстановлению работоспособности оборудования по защите информации;

*ПК-38* – способность разрабатывать и составлять инструкции и руководства пользователей по эксплуатации средств обеспечения информационной безопасности компьютерных систем и аппаратно-программных средств защиты информации.

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

*ПСК-8.2* – способность на основании моделей угроз моделей нарушителя информационной безопасности формировать требования к обеспечению информационной безопасности объектов информатизации на базе компьютерных систем 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;

*ПСК-8.7* – способность разрабатывать проекты нормативных и правовых актов предприятия, учреждения, организации, регламентирующих деятельность по обеспечению ИБ ОИ на базе КС в защ.исполнении.

В результате изучения дисциплины студенты должны:

1. Знать классификацию и основные характеристики технических каналов утечки информации. Знать классификацию и возможности видов технической разведки.
2. Уметь проводить декомпозицию задачи защиты информации на объекте от утечки по техническим каналам, организовывать мероприятия по защите информации и по контролю эффективности защиты информации. Уметь обосновать состав комплекса инженерно-технических средств охраны объекта. Владеть навыками разработки модели угроз, расчета основных показателей защиты информации и инструментального контроля показателей защиты информации.
3. Иметь представление об обнаружении и локализации специальных электронных устройств перехвата информации Понимать физические основы утечки информации по побочным электромагнитным излучениям технического средства обработки информации. Иметь представление об экранировании электромагнитных полей, специальном исследовании технических средств обработки информации на наличие каналов утечки информации.

#### Содержание рабочей программы

**Тема 1. Техническая разведка.**

Виды, источники и носители защищаемой информации. Безопасность информации. Демаскирующие признаки объектов наблюдения и сигналов. Технические средства разведки и их возможности. Направления защиты информации от технической разведки.

**Тема 2. Технические каналы утечки информации.**

Обобщенная модель канала утечки информации. Опасный сигнал, среда распространения, техническое средство разведки. Классификация технических каналов утечки информации. Побочные электромагнитные излучения и наводки. Ближняя, промежуточная и дальняя зоны электромагнитных излучений технических средств обработки информации.

**Тема 3. Защита информации от утечки по побочным электромагнитным излучениям технических средств обработки информации.**

Физические основы утечки информации по побочным электромагнитным излучениям технического средства обработки информации. Показатели защищенности информации от разведки и методика их оценки. Специальное исследование технических средств обработки информации на наличие каналов утечки информации за счет побочных электромагнитных излучений. Защита от утечки информации: экранирование, система пространственного зашумления.

**Тема 4. Экранирование электромагнитных полей.**

Поверхностный эффект. Распространение электромагнитных волн в проводах, потери отражений. Особенности конструирования экранов. Многослойное экранирование. Оценка эффективности применения экранов.

**Тема 5. Защита информации от утечки по цепям заземления и электропитания.**

Физические основы утечки информации по цепям заземления и электропитания. Показатели защищенности информации и методика их оценки. Специальное исследование технических средств обработки информации на наличие канала утечки информации. Подавление опасных сигналов (защита информации) в цепях заземления и электропитания.

**Тема 6. Защита информации от утечки за счет опасных сигналов, возникающих в акустоэлектрических преобразователях.**

Физические основы утечки информации при акустоэлектрических преобразованиях в технических средствах обработки информации. Показатели защищенности информации и методика их оценки. Специальное исследование технических средств обработки информации на наличие канала утечки информации при акустоэлектрическом преобразовании. Подавление опасных сигналов, возникающих в акустоэлектрическом преобразователе.

**Тема 7. Защита информации от утечки из-за взаимного влияния цепей и наводок.**

Физические основы утечки информации. Показатели защищенности и методика их оценки. Методика измерения сигналов, наведенных в проводах и кабелях, выходящих за пределы контролируемой зоны. Мероприятия по защите информации.

**Тема 8. Защита информации от утечки за счет «паразитной» модуляции высокочастотных генераторов и усилителей.**

Паразитная модуляция высокочастотных колебаний генераторов, входящих в состав технических средств обработки информации. Устойчивость усиления. Самовозбуждение усилителей. Показатели защищенности и методика оценки возможности утечки информации при модуляции речевым сигналом колебаний высокочастотных генераторов. Проверка устойчивости усилителей звукового диапазона частот к самовозбуждению. Мероприятия по защите информации.

**Тема 9. Защита информации от утечки по акустическим полям.**

Физические основы утечки информации по акустическим полям. Показатели защищенности. Звукоизоляция выделенных помещений. Методика определения эффективности звукоизоляции.

**Тема 10. Обнаружение и локализация специальных электронных устройств перехвата информации.**

Специальные устройства перехвата информации. Способы и средства перехвата речевой информации на объектах технических средств обработки информации и выделенных помещений. Радиозакладки. Телефонные закладки. Специальная проверка объектов и помещений. Средства обнаружения закладок.

**Тема 11. Методы и средства инженерной защиты и технической охраны объекта.**

Состав комплекса инженерно-технических средств охраны объекта. Принципы построения и классификация средств обнаружения. Ультразвуковые, инфракрасные, радиотехнические, емкостные средства обнаружения нарушителя. Охрана периметров объектов. Блокирование помещений, сейфов, шкафов.

**Перечень лабораторных работ**

| № | Наименование работы | Номер темы | Трудоемкость |
| --- | --- | --- | --- |
| 1 | Побочные электромагнитные излучения при работе технических средств обработки информации – утечка информации за счет побочных электромагнитных излучений усилителя звуковой частоты | 3 | 3 |
| 2 | Наводки (вторичные сигналы, образующиеся в проводниках, расположенных в зоне действия побочного электромагнитного излучения) – утечка информации по цепям заземления усилителя звуковой частоты | 7 | 3 |
| 3 | Неравномерность потребления тока в сети электропитания (амплитудная модуляция тока в сети электропитания информативным сигналом) – утечка информации по цепи электропитания усилителя звуковой частоты | 5 | 3 |
| 4 | Паразитная генерация элементов технических средств – утечка информации при самовозбуждении усилителя звуковой частоты | 5 | 3 |
| 5 | Модуляция информативным сигналом излучений генераторов, входящих в состав технических средств – утечка информации за счет побочного электромагнитного излучения телефонного аппарата с кнопочным номеронабирателем | 8 | 3 |
| 6 | ВЧ-навязывание (получение информации путем перехвата электромагнитных излучений, возникающих при подаче высокочастотного сигнала в нелинейные цепи технических средств обработки информации) – перехват информации из выделенного помещения способом ВЧ-навязывания | 2 | 3 |
| 7 | Электроакустические преобразования – утечка информации по радиотрансляционной сети | 6 | 3 |
| 8 | Электроакустические преобразования – утечка информации за счет электроакустического преобразования в телефонных аппаратах с электромеханическим звонком | 6 | 3 |
| 9 | Акустические колебания, распространяемые в среде, разделяющей источник излучения и средство технической разведки – утечка информации по виброакустическому каналу | 9 | 3 |
| 10 | Технические каналы утечки информации, образованные проводными линиями связи – перехват речевой информации из телефонной линии | 10 | 3 |
| 11 | Технические каналы утечки информации, образованные проводными линиями связи – перехват речевой информации из телефонного кабеля | 10 | 3 |
| 12 | Утечка информации за счет побочных электромагнитных излучений персональной ЭВМ | 3 | 3 |

**Перечень практических занятий**

| № | Наименование занятия | Номер темы | Трудоемкость |
| --- | --- | --- | --- |
| 1 | Побочные электромагнитные излучения при работе технических средств обработки информации – утечка информации за счет побочных электромагнитных излучений усилителя звуковой частоты | 3 | 3 |
| 2 | Наводки (вторичные сигналы, образующиеся в проводниках, расположенных в зоне действия побочного электромагнитного излучения) – утечка информации по цепям заземления усилителя звуковой частоты | 7 | 3 |
| 3 | Неравномерность потребления тока в сети электропитания (амплитудная модуляция тока в сети электропитания информативным сигналом) – утечка информации по цепи электропитания усилителя звуковой частоты | 5 | 3 |
| 4 | Паразитная генерация элементов технических средств – утечка информации при самовозбуждении усилителя звуковой частоты | 5 | 3 |
| 5 | Модуляция информативным сигналом излучений генераторов, входящих в состав технических средств – утечка информации за счет побочного электромагнитного излучения телефонного аппарата с кнопочным номеронабирателем | 8 | 3 |
| 6 | ВЧ-навязывание (получение информации путем перехвата электромагнитных излучений, возникающих при подаче высокочастотного сигнала в нелинейные цепи технических средств обработки информации) – перехват информации из выделенного помещения способом ВЧ-навязывания | 2 | 3 |

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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| №  темы | Название разделов, тем рабочей программы и видов самостоятельной работы | Количество учебных часов | | | | | | | Сем. | Литература по темам |
| Лекции | Лаб.  работы | Практ.  занятия. | Ауд. занятия | | Самост.  работа | Всего |
| Всего | В интерактивн. форме\* |
| 1 | Техническая разведка | 6 |  |  | 6 |  |  | 6 | 8 | Л1, Л2, Д1-Д5 |
| 2 | Технические каналы утечки информации | 4 | 3 | 3 | 10 | 3 | 6 | 16 | 8 | Л1, Л2, Д1-Д5 |
| 3 | Защита информации от утечки по побочным электромагнитным излучениям технических средств обработки информации | 4 | 6 | 3 | 13 | 3 | 6 | 19 | 8 | Л1, Л2, Д1-Д5 |
| 4 | Экранирование электромагнитных полей | 2 |  |  | 2 |  |  | 2 | 8 | Л1, Л2, Д1-Д5 |
| 5 | Защита информации от утечки по цепям заземления и электропитания | 3 | 6 | 6 | 15 | 6 | 6 | 21 | 8 | Л1, Л2, Д1-Д5 |
| 6 | Защита информации от утечки за счет опасных сигналов, возникающих в акустоэлектрических преобразователях | 3 | 6 |  | 9 |  | 5 | 14 | 8 | Л1, Л2, Д1-Д5 |
| 7 | Защита информации от утечки из-за взаимного влияния цепей и наводок | 4 | 3 | 3 | 10 | 3 | 6 | 16 | 8 | Л1, Л2, Д1-Д5 |
| 8 | Защита информации от утечки за счет "паразитной" модуляции высокочастотных генераторов и усилителей | 4 | 3 | 3 | 10 | 3 | 5 | 15 | 8 | Л1, Л2, Д1-Д5 |
| 9 | Защита информации от утечки по акустическим полям | 2 | 3 |  | 5 |  | 5 | 10 | 8 | Л1, Л2, Д1-Д5 |
| 10 | Обнаружение и локализация специальных электронных устройств перехвата информации | 2 | 6 |  | 8 |  | 5 | 13 | 8 | Л1, Л2, Д1-Д5 |
| 11 | Методы и средства инженерной защиты и технической охраны объекта | 2 |  |  | 2 |  |  | 2 | 8 | Л1, Л2, Д1-Д5 |
| Подготовка к экзамену | |  |  |  |  |  | 36 | 36 | 8 | Л1, Л2, Д1-Д5 |
| ИТОГО: | | 36 | 36 | 18 | 90 | 18 | 80 | 170 |  |  |

# **Учебно-методическое обеспечение дисциплины**

# **Основная литература**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Название, библиографическое описание | Л | Лр | Пз (С) | Кп (р) | Инд.  зад. | К-во экз. в библ. (на каф.) | Гриф |
| **Л1** | Белов Е.Б., Лось В.П., Мещеряков Р.В. Основы информационной безопасности. М.: «Горячая линия – Телеком, 2006 | 8 | 8 | 8 |  |  | Ф(2)ЧЗ1(2) |  |
| **Л2** | Данжани Н., Кларк Д. Средства сетевой безоавсности. М. Кудиц – Пресс, 2007 | 8 | 8 | 8 |  |  | Ф(2)ЧЗ1(2) |  |

##### **Дополнительная литература**

|  |  |  |
| --- | --- | --- |
| № | Название, библиографическое описание | К-во экз. в библ. (на каф.) |
| **Д1** | Вим ван Эйк. Электромагнитное излучение видеодисплейных модулей: риск перехвата информации. // Защита информации. Конфидент № 1, 2001. – С. 90–93; № 2, 2001. – С. 84–93. | нет |
| **Д2** | Железняк В. К., Комарович В. Ф. Общие вопросы защиты информации от утечки по техническим каналам // Защита информации. Конфидент № 1 (43), 2002. – С. 80. | нет |
| **Д3** | Андриенко А. А., Петров В. В. и др. Определение границ ближней и дальней зоны при измерениях ПЭМИ // Защита информации. Конфидент № 4–5 (46–4), 2002. – С. 36. | нет |
| **Д4** | Хорев А. А. Методы и средства поиска электронных устройств перехвата информации. – М.: МО РФ, 1998. – 224 с. | нет |
| **Д5** | Энциклопедия промышленного шпионажа/ Под ред. Е.В.Куренкова. - СПб.: ООО «Издательство Полигон». - 1999. | нет |

|  |  |
| --- | --- |
| Зав. отделом учебной литературы | Киселева Т.В |
|  |  |
|  |  |

|  |  |
| --- | --- |
| Авторы: д.т.н., доцент | Максимов Р.В |
|  |  |
| Рецензент: к.т.н., доцент | Анисимов А.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. |
|  |  |