Министерство образования и науки РФ

Государственное образовательное учреждение высшего профессионального образования

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

РАБОЧАЯ ПРОГРАММА

дисциплины

*«Инженерно-техническая защита объектов информатизации»*

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

*«Инженерно-техническая защита объектов информатизации»*

Для подготовки дипломированных специалистов по специальности 090301.65

*«Компьютерная безопасность»*

Уч. план №836

Факультет компьютерных технологий и информатики

Кафедра автоматизированных систем обработки информации и управления

Курс – 5

Семестр – 10

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Лекции | 36 ч. |  | Дифф.зачет | 8 семестр |
| Лабораторные работы | 18 ч. |  |  |  |
| Практические занятия | 18 ч. |  |  |  |

|  |  |
| --- | --- |
| Аудиторные занятия | 72 ч. |
| Самостоятельные занятия | 64 ч. |
| Всего часов | 136 ч. |

2011г.

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 «Инженерно-техническая защита объектов информатизации» преподается **на основе ранее изученных дисциплин:**

1. Основы информационной безопасности;
2. Технические средства и методы защиты информации;
3. Операционные системы;
4. Безопасность жизнедеятельности

и обеспечивает выполнение ВКР.

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

Аннотация дисциплины

Учебная дисциплина «Инженерно-техническая защита объектов информатизации» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Цели и задачи дисциплины

Основной целью дисциплины «Инженерно-техническая защита объектов информатизации» является ознакомление учащихся с основными методами организации комплексного противодействия техническим средствам негласного съема информации и привитие практических навыков по обеспечению информационной безопасности на объектах защиты.

Задачи дисциплины предусматривают предоставление знаний по вопросам:

* обнаружения и классификации фактов несанкционированного доступа к закрытой информации и непосредственного выявления аппаратуры, обеспечивающей эту возможность;
* выявления угрозы информационной безопасности объекта;
* организации работ по перекрытию основных каналов утечки информации и методов контроля эффективности, проведенных мероприятий;
* основных характеристик технических средств изъятия конфиденциальной информации и аппаратуры зашиты от них;
* приобретение начальных навыков обращения со специальной техникой и организации работы службы безопасности по перекрытию каналов утечки информации через технические средства.

Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование вклада в следующие компетенции:

*ПК-34* – способность производить установку, тестирование ПО и программно-аппаратных средств по обеспечению информационной безопасности компьютерных систем;

*ПК-35* – способность принимать участие в эксплуатации ПО и программно-аппаратных средств обеспечения ИБ КС;

*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 освоения дисциплины студенты должны:

**знать:**

* основы организации защиты информации, ее современные проблемы и терминологию;
* основные руководящие документы по обеспечению информационной безопасности на объекте;
* основные каналы утечки информации через физические поля и технические средства;
* основные приемы и способы негласного изъятия информации из технических средств ее обработки и хранения;
* основные характеристики и особенности применения наиболее распространенных устройств негласного изъятия информации;
* основные организационные и технические методы и средства защиты информации;
* основные способы проверки помещений и технических средств на наличие устройств негласного съема информации;
* технические характеристики и возможности наиболее распространенных средств контроля и поиска устройств съема информации;
* технические характеристики, возможности и особенности применения аппаратуры, обеспечивающей защиту технических средств обработки и хранения информации от несанкционированного доступа;
* методы технического (инструментального) контроля эффективности защиты информации объектов;
* порядок и особенности лицензирования деятельности юридических и физических лиц по организации и осуществлению деятельности, связанной с защитой информации.
* основные документы, регламентирующие организационную безопасность на объекте;

**уметь:**

* оценивать состояние технической защиты информации на объекте;
* определять рациональные меры по обеспечению технической защиты информации на объекте;
* выявлять основные каналы утечки информации через технические средства;
* производить измерения уровня наводок и побочных каналов излучения технических средств хранения и обработки информации;
* проводить основные мероприятия по обеспечению перекрытия каналов утечки информации через технические средства;
* классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
* осуществлять простейший технический (инструментальный) контроль эффективности мероприятий по защите информации.
* организовать работу персонала с секретной (конфиденциальной) информацией;

**владеть:**

* методами выявления угроз информационной безопасности объекта;
* навыками анализа угроз и уязвимостей информационной безопасности;
* методикой поиска основных типов устройств негласного съема конфиденциальной информации с применением специальной аппаратуры;
* навыками анализа достаточности мер по обеспечению информационной безопасности.

Содержание рабочей программы

**Вводная лекция**

Концептуальные основы технического обеспечения информационной безопасности. Угрозы информационной безопасности на объекте защиты. Организация службы технической безопасности. Организация и обеспечение работы с информацией ограниченного доступа. Нормативно-методическое обеспечение организации безопасности информации.

**Тема 1. Угрозы безопасности информации**

Основные направления защиты информации от технических средств несанкционированного съема. Роль технических средств в обеспечении безопасности информации.

**Тема 2. Основные способы ведения промышленного шпионажа**

Каналы утечки информации их характеристика и место в системе технической разведки. Основные физические поля, по которым происходит утечка информации и их характеристики. Классификация технических средств негласного съема информации.

**Тема 3. Естественные каналы утечки информации**

Причины образования технических каналов утечки информации. Перехват информации через естественные каналы утечки и путем несанкционированного доступа.

**Тема 4. Каналы утечки информации в технических средствах ее обработки и хранения**

Каналы утечки информации за счет акустических полей. Каналы утечки информации за счет электромагнитных излучений и наводок. Каналы утечки информации по цепям питания и заземления. Каналы утечки информации за счет рассеянных оптических полей. Каналы утечки информации за счет оптико- , электро- и вибро-акустических преобразований.

**Тема 5. Технические средства несанкционированного доступа**

Основные средства несанкционированного доступа к конфиденциальной информации. Возможности средств акустической разведки и особенности их применения. Возможности средств оптической разведки и особенности их применения. Основные характеристики и методы применения радио-микрофонов и радио-закладок. Устройства подслушивания, использующие проводную связь. Аппаратура лазерной разведки. Устройства съема информации с технических средств ее передачи и хранения.

**Тема 6. Основные понятия информационной безопасности**

Организационные мероприятия по защите информации. Аттестация объектов информации по требованиям безопасности. Общие принципы защиты информации в помещениях и сетях связи.

**Тема 7. Устройства и методы поиска закладных устройств**

Основные методы и средства выявления закладных устройств. Физический поиск. Индикаторы поля. Специальные радиоприемные устройства. Программно-аппаратные комплексы. Нелинейные радиолокаторы. Некоторые рекомендации по поиску устройств негласного съема информации.

**Тема 8. Защита информации в помещениях и сетях связи**

Аппаратура контроля линий связи. Средства защиты линий связи Криптографические методы и средства защиты. Технические средства пространственного и линейного зашумления. Защита от ВЧ навязывания. Защита от несанкционированной аудиозаписи. Основные методы и средства контроля степени защищенности объектов и сетей. Аппаратура измерения уровня сигнала в электрических цепях и сетях связи. Аппаратура измерения уровня побочных излучений. Проверка степени защищенности маскирующими сигналами.

**Тема 9. Основы защиты информации в компьютерных сетях**

Виды потенциально опасных воздействий. Защита от ошибок обслуживающего персонала. Защита от заражений компьютерными вирусами. Программно-аппаратные средства защиты информации от несанкционированного доступа.

#### **Перечень лабораторных занятий**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Наименование темы занятия | Номер темы | Трудоемкость |
| 1 | Исследование эффекта акусто-электрическрго преобразования в РЭА. Исследование наводок, возникающих в электрических сетях. | 4 | 6 |
| 2 | Исследование способов закрытия канала утечки информации через технические средства за счет эффекта акусто-электрического преобразования. Исследование способов обнаружения контактного подключения к линиям связи. | 7 | 6 |
| 3 | Изучение и отработка навыков работы с поисковым прибором «Пиранья». Изучение и отработка навыков работы с нелинейным локатором «Катран». Изучение методики и отработка навыков физического поиска ЗУ в помещении. | 8 | 6 |

#### **Перечень практических занятий**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Наименование темы занятия | Номер темы | Трудоемкость |
| 1 | Расчет размера преобразуемого блока данных по заданному уровню ошибок в отводном канале на границе контролируемой зоны в методе бесключевого шифрования. Сопоставление методов кодового зашумления и бесключевого шифрования. | 4 | 9 |
| 2 | Изучение и отработка навыков работы с поисковым прибором «Пиранья». Изучение и отработка навыков работы с нелинейным локатором «Катран». Изучение методики и отработка навыков физического поиска ЗУ в помещении. | 8 | 9 |

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

**и видам самостоятельной работы**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № темы | Название разделов и тем |  | **Объем учебных часов** | | | | | | Семестр | **Литература по темам** |
| Лекции | Лабор. занят. | Практ. занят. | Аудит. занят. | | Самост. Работа | **Всего** |
| всего | в интер. форме |
|  | Вводная лекция | 1 |  |  | 1 |  |  | 1 | 10 | Л1-Л4, Д1-Д7 |
| 1 | Угрозы безопасности информации | 2 |  |  | 2 |  | 5 | 7 | 10 | Л1-Л4, Д1-Д7 |
| 2 | Основные способы ведения промышленного шпионажа | 2 |  |  | 2 |  | 5 | 7 | 10 | Л1-Л4, Д1-Д7 |
| 3 | Естественные каналы утечки информации | 2 |  |  | 2 |  | 5 | 7 | 10 | Л1-Л4, Д1-Д7 |
| 4 | Каналы утечки информации в технических средствах ее обработки и хранения | 4 | 6 | 9 | 19 | 9 | 15 | 34 | 10 | Л1-Л4, Д1-Д7 |
| 5 | Технические средства несанкционированного доступа | 4 |  |  | 4 |  |  | 4 | 10 | Л1-Л4, Д1-Д7 |
| 6 | Основные понятия информационной безопасности. | 1 |  |  | 1 |  | 10 | 11 | 10 | Л1-Л4, Д1-Д7 |
| 7 | Устройства и методы поиска закладных устройств | 4 | 6 |  | 10 |  | 10 | 20 | 10 | Л1-Л4, Д1-Д7 |
| 8 | Защита информации в помещениях и сетях связи | 4 | 6 | 9 | 19 | 9 | 8 | 27 | 10 | Л1-Л4, Д1-Д7 |
| 9 | Основы защиты информации в компьютерных сетях | 2 |  |  | 2 |  | 6 | 8 | 10 | Л1-Л4, Д1-Д7 |
| **ИТОГО:** | | 36 | 18 | 18 | 72 | 18 | 64 | 136 |  |

# Учебно-методическое обеспечение дисциплины

# Основная литература

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Название, библиографическое описание | Л | Лр | Пз (С) | Кп | Кр | К-во экз. в библ. (на каф.) | Гриф |
| Л1 | Каторин Ю.Ф. и др. Большая энциклопедия промышленного шпионажа. СПб.: «Издательство Полигон», 2000. – 896 с. | 8 | 8 |  |  | 8 | ЧЗ1(2) Ф(2)  Б(1) |  |
| Л1 | Гектор Гарсиа-Молина, Джеффри Ульман, Дженифер Уидом. Системы баз данных. Полный курс. М., С.-Петербург, Киев: Вильямс, 2003. | 8 | 8 |  |  | 8 | У(16) |  |
| Л3 | Мартин Грабер. SQL. Справочное руководство, 2001 | 8 | 8 |  |  | 8 | нет |  |
| Л4 | Вильям Дж. Пейдж (мл.). Использование  Oracle8/8i, 2001 | 8 | 8 |  |  | 8 | нет |  |

**Дополнительная литература**

|  |  |  |
| --- | --- | --- |
| № | Название, библиографическое описание | К-во экз. в библ. (на каф.) |
| Д1 | Вендров А.М. Проектирование программного обеспечения экономических информационных систем. М.: Финансы и статистика, 2000 | нет |
| Д2 | Маклаков С.В. BPwin и Erwin. CASE-средства разработки информационных систем. – М.: ДИАЛОГ-МИФИ, 1999. | нет |
| Д3 | К. Дейт. Введение в системы баз данных. 7-е изд. М.: СПб.: Вильямс, 2001. | Ф(2) ЧЗ1(2) |
| Д4 | Д. Мейер Теория реляционных баз данных. М.: Мир, 1987 | Ф(3) |
| Д5 | Вендров А.М. CASE-технологии. Современные методы и средства проектирования информационных систем. М.: Финансы и статистика, 1998 | нет |
| Д6 | Фаулер М., Скотт К. UML в кратком изложении. Применение стандартного языка объектного моделирования. М.: Мир, 1999 | Ф(1) |
| Д7 | Буч Г., Рамбо Д., Джекобсон А. Язык UML: руководство пользователя. М.: ДМК, 2000 | У(11) |

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

**Электронные информационные ресурсы**

|  |  |
| --- | --- |
| № | Название (адрес в Интернет) |
| Э1 | Кузнецов С.Д. Введение в реляционные базы данных. Интернет-университет информационных технологий - ИНТУИТ.ру, 2005. http://www.intuit.ru/department/database/rdbintro/ |
| Э2 | С. Д. Кузнецов. Проектирование и разработка корпоративных информационных систем. Центр Информационных Технологий, 1998. <http://citforum.ru/cfin/prcorpsys/> |
| Э3 | Кузнецов С.Д. Введение в модель данных SQL - Интернет-университет информационных технологий - ИНТУИТ.ру, 2005. <http://www.intuit.ru/department/database/sqlmdintro/> |
| Э4 | Баженова И. Ю. Основы проектирования приложений баз данных Интернет-университет информационных технологий - ИНТУИТ.ру, 2006. <http://www.intuit.ru/department/database/cdba2/> |
| Э5 | Щавелёв Л.В. Оперативная аналитическая обработка: концепции и технологии. - http://www.olap.ru/basic/olap\_and\_ida.htm |
| Э6 | Хрусталёв Е.М. Агрегация данных в OLAP-кубах. – <http://www.olap.ru/Home/mut.htm> |
| Э7 | Эйриэнн Х. Слотер Архитектуры OLAP. - http://www.olap.ru/Basic/olap\_arch.htm |
| Э8 | Альперович М. Введение в OLAP и многомерные базы данных. - <http://www.olap.ru/Basic/alpero2i.htm> |
| Э9 | What is OLAP? - http://[www.olapreport.com](http://www.olapreport.com)/fasmi.htm |
| Э10 | OLAP Architectures - http://[www.olapreport.com](http://www.olapreport.com)/Architectures.htm |

|  |  |
| --- | --- |
|  |  |
| Авторы: |  |
| (с к.т.н., доцент | Савосин С.В. |
| к.т.н., доцент | Егоров С.С. |
| ассистент | Пономарёв А.В. |
|  |  |
| Рецензент |  |
| к.т.н., доцент | Первицкий А.Ю. |
|  |  |
| Зав. кафедрой автоматизированных систем обработки информации управленияи и управления |  |
| д.т.н., профессор | Советов Б.Я. |
|  |  |
| Декан факультета компьютерных технологий и информатики |  |
| д.т.н., профессор | Куприянов М.С. |
|  |  |
| Программа согласована: |  |
|  |  |
| Председатель методической комиссии факультета компьютерных  технологий и информатики |  |
| к.т.н., доц. | Михалков В.А. |
|  |  |
| Руководитель методического отдела |  |
| к.т.н., доцент | Марасина Л.А. |
|  |  |