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

*«Основы информационной безопасности»*

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

*«Основы информационной безопасности»*

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 – 7

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Лекции | 54 ч. |  | Экзамен | 7 семестр |
|  |  |  |  |  |
| Практические занятия | 18 ч. |  |  |  |
|  |  |  |  |  |
| Лабораторные занятия | 18 ч. |  | Зачет | 7 семестр |
|  |  |  |  |  |
| Курсовая работа | ч. |  | Курсовая работа | 7 семестр |

|  |  |  |
| --- | --- | --- |
| 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 специалистов по специальности

090301. 65 – «Компьютерная безопасность»

Дисциплина «Основы информационной безопасности» преподается на основе ранее изученных дисциплин:

1. Программирование
2. Алгоритмы и структуры данных
3. Организация ЭВМ и систем
4. Операционные система
5. Архитектура информационных систем
6. Управление данными

и является фундаментом для изучения последующих дисциплин:

1. Технические средства и методы защиты информации
2. Организационно-правовое обеспечение информационной безопасности.

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

**АННОТАЦИЯ ДИСЦИПЛИНЫ**

Дисциплину «Основы информационной безопасности» следует рассматривать одновременно как общеинженерную, так и специальную. В ней рассматриваются основные понятия, которые необходимы для формирования современного специалиста в области обеспечения ИБ, независимо от предметной области будущей деятельности специалиста.

Соответственно, содержание учебного материала должно отражать различные аспекты и уровни общности представления проблем информационной безопасности, от «Доктрины информационной безопасности РФ» до технических понятий и классификаций факторов безопасности. Необходимыми также являются материалы, представляющие системное видение указанных проблем в устойчивых категориях, освоение которых позволит специалистам адаптироваться к быстро меняющейся конкретике в данной области.

Учебный материал должен быть организован таким образом, чтобы в результате возникал многоуровневый многоаспектный, но в то же время целостный и динамичный образ проблем информационной безопасности и подходов к их решению.

**Цели и задачи дисциплины**

**Цели дисциплины**

1. Формирование системного представления о современном состоянии проблем информационной безопасности;
2. Активизация и систематизация знаний, полученных в процессе общеинженерной и специальной подготовки, в аспекте информационной безопасности;
3. Приобретение практических навыков конкретного анализа безопасности информационных систем и синтеза СЗИ.

**Задачи дисциплины**

1. Сформировать методологическую и понятийную базу для дальнейшей специальной подготовки.

2. Ознакомить с ретроспективой и современными проблемами в области информационной безопасности.

3. Дать представление о существующих методах и средствах нарушения информационной безопасности и подходах к решению вопросов защиты информации.

4. Ознакомить с понятийным аппаратом теории и практики обеспечения информационной безопасности.

5. Сформировать систему представлений о месте и роли вопросов информационной безопасности в контексте расширяющегося использования информационных технологий в технических, социальных и экономических системах.

6. Развить навыки комплексного анализа безопасности информационных систем.

7. Закрепить в процессе выполнения практических работ совокупность умений и навыков в оперировании с теоретическими представлениями дисциплины.

**Требования к уровню освоения дисциплины**

Изучение дисциплины направлено на формирование вклада в следующие компетенции:

*ОК-5* – способность понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению проф.деятельности в области обеспечения ИБ и защиты интересов личности, общества и государства, готовность и способность к активной состязательной деятельности в условиях информационного противоборства;

*ПК-3* – способность понимать сущность и значение информации в развитии современного общества, применять достижения современных ИТ для поиска и обработки больших объемов информации по профилю деятельности в глобальных КС, сетях, в библиотечных фондах и в иных источниках информации;

*ПК-14* – способность осуществлять подбор, изучение и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения ИБ 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-31* – способность разрабатывать оперативные планы работы первичных подразделений;

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

*ПК-33* – способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению ИБ КС, а также положений, инструкций и других организационно-распорядительных документов в сфере проф. деятельности;

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

В результате изучения дисциплины студенты должны:

1. Знать и иметь представление об основных понятиях и современных проблемах информационной безопасности, моделях, методах и средства анализа и управления безопасностью, программных методах и аппаратных средствах обеспечения и нарушения информационной безопасности.

2. Уметь проводить системный анализ безопасности информационных объектов различного масштаба, выявлять факторы риска, оценивать эффективность средств защиты информации.

3. Получить навыки проведения комплексного анализа и оценивания безопасности реальных информационных объектов.

#### Содержание рабочей программы

**Тема 1. Основные понятия и современные проблемы информационной безопасности**

Понятие информационной безопасности (ИБ), смежные понятия,

ретроспектива вопроса, многообразие представлений.

Понятие и проблемы информационной войны, информационного террора.

Проблемы региональной информационной безопасности.

Корпоративная безопасность, противоречия.

Современное состояние проблем безопасности и защиты информации (технические и гуманитарные аспекты).

**Тема 2. Информационная безопасность в системе национальной безопасности Российской Федерации.**

Доктрина информационной безопасности РФ

Понятие национальной безопасности.

ИБ в системе национальной безопасности РФ. структура, объект защиты, составляющие.

Основные источники угроз, основные угрозы ИБ РФ.

Основные задачи по обеспечению ИБ РФ.

Информационный аспект в других составляющих национальной безопасности.

Государственная информационная политика.

**Тема 3. Модели, методы и средства анализа и управления безопасностью информационных систем.**

Общеметодологические принципы теории ИБ.

Принцип целенаправленности в анализе безопасности и построения СЗИ.

Метамодель «объект-среда-защита», основные представления, элементы и структура, факторы риска.

Методика анализа и количественной оценки защищенности информационных объектов.

Оценивание средств защиты (показатели применения, критерии выбора), связь показателей результативности СЗИ и надежности.

Технология анализа защищенности объектов и синтеза СЗИ.

Мониторинг и аудит безопасности, экспертные системы.

**Тема 4. Несанкционированный доступ (НСД) к информации, смежные понятия.**

НСД к информации, его место в проблеме информационной безопасности.

Субъекты и объекты доступа к ресурсам, модели доступа.

Правила разграничения доступа.

Понятие об идентификации и аутентификации субъектов доступа.

Классификация основных угроз НСД к информации.

Основные программные и аппаратные методы и средства НСД к информации.

**Тема 5. Программные и аппаратные методы и средства обеспечения и нарушения ИБ.**

Классификация каналов утечки и искажения информации

Основные программные методы информационного нападения.

Аппаратные средства нарушения безопасности информации.

Базовые признаки классификации угроз ИБ.

Классификация источников угроз ИБ.

Понятие уязвимости, атаки, принципы классификации атак.

Мониторинг сетевой безопасности.

**Перечень лабораторных работ**

|  |  |  |
| --- | --- | --- |
| № | Наименование работы | Номер темы |
| 1 | Спецификация объекта защиты и структуры факторов риска | 3, 4 |
| 2 | Количественная оценка структуры факторов риска | 3, 4, |
| 3 | Определение профиля риска и синтез вариантов СЗИ | 3, 4, 5, |
| 4 | Оценка результативности и эффективности СЗИ | 3, 4, 5, |

**Перечень практических занятий**

|  |  |  |
| --- | --- | --- |
| № | Наименование работы | Номер темы |
| 1 | Объект защиты и факторы риска | 3, 4 |
| 2 | Количественная оценка структуры факторов риска | 3, 4, |
| 3 | Профиль риска, варианты СЗИ | 3, 4, 5, |
| 4 | Результативность и эффективность СЗИ | 3, 4, 5, |

**Цели и содержание курсовой работы**

Курсовая работа предназначена для актуализации имеющихся у студентов знаний по разделам программной и аппаратной защиты информации. Целью курсовой работы является реализация конкретной задачи аудита защиты информации.

Темы курсовых работ:

1. Тестовые испытания программных средств защиты.
2. Защита от утечек по каналу ПЭМИН, по акустическому и виброакустическому каналам.
3. Анализ сетевой топологии и установленных сервисов.
4. Сетевое сканирование.
5. Анализ трафика и сбор критичной информации программами пассивного анализа.
6. Обнаружение уязвимостей по сигнатурам.

Структура раскрытия темы курсовой работы:

1. Возможная уязвимость и выгода нарушителя.
2. Атака на уязвимость (проверка наличия защиты).
3. Оценка результата атаки (проверки). Критерии её успешности.
4. Рекомендации владельцу информации в случае:

* атака отражена
* атака прошла успешно.

Ориентировочная трудоемкость – 36 часов.

**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 | Основные понятия и современные проблемы информационной безопасности | 12 |  |  | 12 |  | 2 | 14 | 7 | Л1, Л2, Д1, Д2, Э1 |
| 2 | Информационная безопасность в системе национальной безопасности Российской Федерации | 10 |  |  | 10 |  | 4 | 14 | 7 | Л1, Л2, Д1, Д2, Д3, Д5, Д6, Э1 |
| 3 | Модели, методы и средства анализа и управления безопасностью информационных систем | 14 | 7 | 7 | 28 | 7 | 10 | 38 | 7 | Л1, Л2, Д2, Д4, Д7, Э1, Э2 |
| 4 | Несанкционированный доступ (НСД) к информации, смежные понятия | 10 | 7 | 7 | 24 | 7 | 16 | 40 | 7 | Л1, Д1, Д2, Д7, Э1, Э2 |
| 5 | Программные и аппаратные методы и средства обеспечения и нарушения ИБ | 8 | 4 | 4 | 16 | 4 | 12 | 28 | 7 | Л1, Л3, Д1, Д2, Д7, Э1, Э2 |
| Курсовая работа | |  |  |  |  |  | 36 | 36 | 7 |
| ИТОГО: | | 54 | 18 | 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 | Галатенко В.А. Основы информационной безопасности: курс лекций: учебное пособие / под ред. ак. РАН В.Б.Бетелина. М.: ИНТУИТ.РУ, 2006. | 7 |  | 7 | 7 |  | нет | Минобразования РФ |
| Л2 | Расторгуев С.П. Основы информационной безопасности: учеб. пособие для студ. вузов. М.: Академия, 2007. | 7 |  | 7 | 7 |  | нет | Минобразования РФ |
| Л3 | Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. С-Пб., «БХВ-Петербург», 2003 | 7 |  | 7 | 7 |  | У(4) |  |

##### **Дополнительная литература**

|  |  |  |
| --- | --- | --- |
| № | Название, библиографическое описание | К-во экз. в библ. (на каф.) |
| Д1 | Юсупов Р.М. Наука и национальная безопасность. СПб: Наука, 2006 | нет |
| Д2 | Расторгуев С.П. Информационная война. Проблемы и модели. Экзистенциальная математика: учеб. пособие для студ. вузов. М.: Гелиос АРВ, 2006. | нет |
| Д3 | Доктрина информационной безопасности Российской Федерации. 9 сентября 2000 г. № Пр-1895 | нет |
| Д4 | Шишкин, В.М. Метамодель анализа, оценки и управления безопасностью информационных систем // Проблемы управления информационной безопасностью: Сборник трудов Института системного анализа Российской академии наук / под ред. Д.С.Черешкина. – М.: Едиториал УРСС, 2002. С. 92 – 105. | нет |
| Д5 | «Стратегия развития информационного общества в Российской Федерации» от 7 февраля 2008 г. № Пр-212. | нет |
| Д6 | «Стратегия национальной безопасности Российской Федерации до 2020 года» от 12 мая 2009 г. № Пр-537. | нет |
| Д7 | ГОСТ Р ИСО/МЭК 15408 | нет |

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

**Электронные информационные ресурсы**

|  |  |
| --- | --- |
| № | Название (адрес в Интернет) |
| Э1 | http://info-sec.edu.nw.ru |
| Э2 | www.infosec.ru |

|  |  |
| --- | --- |
| Авторы: к.т.н., доцент | Шишкин В.М |
|  |  |
| 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. |
|  |  |