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 и средства защиты информации»*

Для подготовки дипломированных специалистов по специальности

230102.65 *«Автоматизированные системы обработки информации и управления»*

и специальности 230101.65 *«Вычислительные машины, комплексы, системы и сети»*

на открытом факультете

Санкт-Петербург

2011

Санкт-Петербургский государственный электротехнический

университет “ЛЭТИ”

"УТВЕРЖДАЮ"

проректор по учебной работе

проф.\_\_\_\_\_\_\_\_\_ Лысенко Н.В.

"\_\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_\_2011 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

*«Методы и средства защиты информации»*

Для подготовки дипломированных специалистов по специальности

230102.65 *«Автоматизированные системы обработки информации и управления»*

и специальности 230101.65 *«Вычислительные машины, комплексы, системы и сети»*

на открытом факультете

Уч. план №636, №637

Открытый факультет

Кафедра автоматизированных систем обработки информации и управления

Кафедра вычислительной техники

Курс – 5

Семестр – 9

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Лекции | 34 ч. |  | Экзамен | 9 сем. |
|  |  |  |  |  |
| Лабораторные работы | 17 ч. |  | Зачет | 9 сем. |
|  |  |  |  |  |

|  |  |
| --- | --- |
| Аудиторные занятия | 51 ч. |
| Самостоятельные занятия | 61 ч. |
| Всего часов | 112 ч. |

2011 г.

Рабочая программа обсуждена на заседании кафедры автоматизированных систем обработки информации и управления и кафедры вычислительной техники «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2011 г., протокол № \_\_\_\_.

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

230102.65 — «Автоматизированные системы обработки информации и управления»

230101.65 — «Вычислительные машины, комплексы, системы и сети»

Дисциплина «Методы и средства защиты информации» преподается на основе ранее изученных дисциплин:

1. Дискретная математика;
2. Теория вероятностей и математическая статистика;
3. Языки программирования и информационные технологии;
4. Инфокоммуникационные системы и сети;
5. Операционные системы

и может служить фундаментом для изучения следующихдисциплин:

1. Проектирование корпоративныхинформационныхуправляющих систем;
2. Распределенные автоматизированные системы обработки информации и управления.

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

**Аннотация дисциплины**

В дисциплине излагаются вопросы по методам и средствам защиты информации в проектировании и эксплуатации автоматизированных систем обработки информации и управления, включая законодательную базу.

В настоящей дисциплине рассмотрены как устоявшиеся теоретические вопросы, так и новые аспекты, которые мало или несистемно рассмотрены в отечественной и переводной литературе. Это относится как к локальным сетям, так и к распределенным информационным системам и прикладным программным средствам. Подробно рассмотрены способы защиты в операционных системах.

Работа отличается системным рассмотрением прежде всего теоретических вопросов, которые сопровождаются компьютерной реализацией. Это позволяет лучше понять процедуры построения, работы и использования баз данных.

Для успешного усвоения материалов курса необходимо изучения дисциплин: компьютерные сети; проектирования информационных систем; ИТ- технологии.

**Цели и задачи дисциплины**

Получение студентами теоретических основ анализа неавторизованного доступа к информации, нарушения конфиденциальности, целостности доступности информации, неавторизованного доступа к сетям и другим сервисам, современных методах защиты информации, криптографическим методам защиты информации и практическим навыкам по защите информации от несанкционированного доступа, принципов построения защищенной вычислительной сети и баз данных.

В результате изучения курса студент овладевает методами и средствами защиты информации, которые необходимы при создании, использовании, совершенствовании и ликвидации сложных комплексов информационного профиля.

Требования к результатам освоения дисциплины

В результате изучения дисциплины студенты должны:

1. Знать идеологию построения открытых систем, эталонную модель взаимодействия открытых систем; методы проектирования средств защиты информационных систем; методы определения и анализа угроз безопасности информационных систем; криптографические системы и цифровую подписи;

2. Уметь проектировать средства защиты информационных систем в соответствии с ГОСТом; применять распространенные криптографических систем и цифровой подписи; анализа угроз безопасности информационных систем; применять распространенные криптографических систем и цифровой подписи.

3. Владеть представлением об идеологии построения глубоко эшелонированной системы комплексной информационной безопасности IT-среды, методами и средства обеспечения информационной безопасности периметра инфраструктуры ЛВС; методами и средствами обеспечения информационной безопасности систем и информационных сервисов (HTTP, FTP, SMTP,POP3), размещаемых в специализированных демилитаризованных зонах.

Содержание рабочей программы

**Тема 1. Понятие об информационной безопасности**

Введение. Актуальность Введение. Понятие об информационной безопасности. Основные виды угроз. Классификация угроз. Естественные и искусственные угрозы.

**Тема 2. Сетевая безопасность**

Эталонная модель взаимодействия открытых систем OSI. Средства и методы передачи данных (коммутаторы, маршрутизаторы). Стек протоколов Internet. Основы протокола передачи информации TCP/IP. Безопасность протокола TCP/IP. Классификация сетевых атак и способы их реализации. Методы борьбы с атаками. Защита FTP, WWW-сервера, электронной почты. Организация защиты с помощью маршрутизаторов, межсетевых экранов, прокси-серверов. Построение VPN.

**Тема 3. Криптографическая защита информации**

Классификация криптоалгоритмов. Симметричные криптоалгоритмы. Блочные шифры. Алгоритм DES, ГОСТ. Ассиметричные криптосистемы. Алгоритм RSA. Методы хеширования. Технологии цифровых подписей. Алгоритм RSA, Эль-Гамаля, ГОСТ. Механизм распространения открытых ключей. Обмен ключами по алгоритму Диффи-Хеллмана. Методы стеганографии.

**Тема 4. Защита от вирусов**

Классификация вирусов. Этапы жизненного цикла вируса. Методы обнаружения. Обзор антивирусных программ Недостатки реляционных баз данных.

**Тема 5. Безопасность операционных систем**

Безопасность операционных систем: Методы идентификации и аутентификации пользователей. Аутентификация на основе одноразовых паролей, многоразовых паролей, биометрических данных, технических средств. Авторизация. Классификация методов авторизации. Управление доступом. Матричный, дискреционный, полномочный доступ. Классы защиты. Математические методы анализа политики безопасности. Модель Кларка-Вильсона. Модель "TAKE-GRANT" . Модель БЕЛЛА-ЛАПАДУЛА (Б-Л). Модель LOW-WATER-MARK (LWM). Модель выявления нарушения безопасности. Комплексный поиск возможных методов доступа. Ролевое управление. Обеспечение безопасность ОС WINDOWS, UNIX, NETWARE.

**Тема 6. Технологии производства защищенных программных средств**

Технологии производства защищенных программных средств. Основные категории ошибок в разработке программного обеспечения. Принципы разработки алгоритмов программного обеспечения. Гарантии на правильную работу системы Этапы жизненного цикла программного обеспечения.

**Тема 7. Методы защиты СУБД**

Методы обеспечения безотказности. Безотказность сервисов и служб хранения данных, внесения избыточности на различных уровнях.

**Тема 8. Законодательная база**

Механизмы безопасности "Оранжевая книга". Руководящие документы Гостехкомиссии. ГОСТ 14508.

**Тема 9. Управление рисками и построение систем безопасности**

Основные понятия и определения. Технология анализа и управления рисками. Средства автоматизации оценки информационных рисков.

**Тема 10. Инженерно-технические средства защиты информации**

Схема возможных каналов утечки и несанкционированного доступа к информации. Обнаружение каналов утечки, пассивные и активные методы защиты информации.

**Перечень лабораторных работ**

|  |  |  |
| --- | --- | --- |
| **№**  **л/р** | **Тема лабораторной работы** | **Номер темы программы** |
| 1 | Управление рисками и построение систем безопасности. | 2,3,4,5,6,7,8,9,10 |
| 2 | Криптографические методы защиты информации. Шифр подстановки, шифр перестановки. Алгоритм RSA, Эль-Гамаля | 3,5,6,8 |
| 3 | Изучение способов применения защиты информации и разграничения доступа в операционных системах | 3,4,5, 6,8, 10 |

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

**и видам самостоятельной работы**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| №  темы | Название разделов, тем  и видов самостоятельной  работы | Объем учебных часов | | | | | | Семестр | Литература по темам |
| Лекции | Лаб.  Раб. | Пр.  зан. | Ауд.  Зан. | Сам.  раб. | Всего |
| 1 | Понятие об информационной безопасности | 2 |  |  | 2 | 2 | 4 | 9 | **Л1, Л2, Д1, Д2** |
| 2 | Сетевая безопасность | 4 | 2 |  | 6 | 4 | 10 | 9 | **Л1, Л2, Д1, Д2** |
| 3 | Криптографическая защита информации | 4 | 2 |  | 6 | 8 | 14 | 9 | **Л1, Л2, Д1, Д2** |
| 4 | Защита от вирусов | 4 | 2 |  | 6 | 8 | 14 | 9 | **Л1, Л2, Д1, Д2** |
| 5 | Безопасность операционных систем | 6 | 2 |  | 8 | 8 | 16 | 9 | **Л1, Л2, Д1, Д2** |
| 6 | Технологии производства защищенных программных средств | 2 | 1 |  | 3 | 8 | 11 | 9 | **Л1, Л2, Д1, Д2** |
| 7 | Методы защиты СУБД | 4 | 2 |  | 6 | 8 | 14 | 9 | **Л1, Л2, Д1, Д2** |
| 8 | Законодательная база | 2 | 2 |  | 4 | 5 | 9 | 9 | **Л1, Л2, Д1, Д2** |
| 9 | Управление рисками и построение систем безопасности | 4 | 2 |  | 6 | 6 | 12 | 9 | **Л1, Л2, Д1, Д2** |
| 10 | Инженерно-технические средства защиты информации | 2 | 2 |  | 4 | 4 | 8 | 9 | **Л1, Л2, Д1, Д2** |
| ИТОГО: | | 34 | 17 |  | 51 | 61 | 112 | 9 |

**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** | Олифер Г.В., Олифер Н.А. Компьютерные сети. Учебник. С.-Петербург: Питер. 2007 -672 с. | 9 | 9 |  |  |  | 129 | Минобразования РФ |
| **Л2** | Роберта Брэг Безопасность сетей. Москва, из-во Эком Бином, 2006-912с. | 9 | 9 |  |  |  | нет | Минобразования РФ |

Дополнительная литература

|  |  |  |
| --- | --- | --- |
| № | Название, библиографическое описание | К-во экз. в библ. (на каф.) |
| Д1 | Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009. — 352 с. | 1 |
| Д2 | Галатенко В. А. Стандарты информационной безопасности. — М.: Интернет-университет информационных технологий, 2006. — 264 с. | 1 |

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

Электронные информационные ресурсы

|  |  |
| --- | --- |
| № | Название (адрес в Интернет) |
| Э1 | WWW.OSMAG.RU |

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

|  |  |
| --- | --- |
| Автор: |  |
| д.т.н., профессор | Воробьев В.И. |
| к.т.н., доцент | Фаткиева Р.Р. |
| к.т.н., доцент | Шишкин В.М. |
| Рецензент |  |
| д.т.н., профессор | Водяхо А.И. |
|  |  |
| Зав. кафедрой автоматизированных систем обработки  информации и управления |  |
| д.т.н., профессор | Советов Б.Я. |
| Зав. кафедрой вычислительной техники |  |
| д.т.н., профессор | Пузанков Д.В. |
| Декан открытого факультета |  |
| к.т.н., доцент | Мовнин С.М. |

|  |  |
| --- | --- |
| Программа согласована: |  |
|  |  |
| Руководитель методического отдела |  |
| к.т.н., доцент | Марасина Л.А. |