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 операционных систем и систем управления базами данных»*

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 операционных систем и систем управления базами данных»*

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. |  | Текущий контроль | 10 семестр |
| Лабораторные работы | 17 ч. |  | Зачет | 10 семестр |
| Курсовая работа | 17 ч. |  | Курсовая работа | 10 семестр |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |
| --- | --- |
| Аудиторные занятия | 68 ч. |
| Самостоятельные занятия | 62 ч. |
| Всего часов | 130 ч. |

2011 г.

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

090102.65 — «Компьютерная безопасность»

Дисциплина «Защита операционных систем и систем управления базами данных» преподается на основе изученных ранее дисциплин:

* Основы информационной безопасности;
* Технические средства и методы защиты информации;
* МНБ и вирусология;
* Криптографические протоколы

и обеспечивает подготовку ВКР.

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

Аннотация дисциплины

Учебная дисциплина «Защита операционных систем и систем управления базами данных» является важной составляющей общей профессиональной подготовки специалистов в области обеспечения информационной безопасности. Она призвана обеспечить освоение слушателями практических навыков обеспечения информационной безопасности средствами ОС и СУБД.

**Цели и задачи дисциплины**

Целью дисциплины является формирование у обучаемых знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

**Требования к уровню освоения дисциплины**

В результате изучения дисциплины студент должен:

**знать:** основные методы защиты информационно-программного обеспечения;

**уметь:**

* проводить анализ степени защищенности информации и повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных систем;
* проводить обобщение и анализ реальных эксплуатационных характеристик и разработка рекомендаций по совершенствованию систем и средств защиты информации;

**владеть навыками:**

* проведения мероприятий для обеспечения на предприятии (в организации) деятельности в области защиты информации;
* организации и выполнения мероприятий для обеспечения безопасной обработки информации на средствах вычислительной техники;
* подготовки типовых средств защиты информационно-программного обеспечения к применению по назначению;
* эксплуатации систем и средств защиты информационно-программного обеспечения;
* принятия решения по действиям в нештатных ситуациях, возникающих при функционировании программных средств;
* самостоятельного изучения и освоения новых методов и средств защиты информационно-программного обеспечения.

Содержание рабочей программы

**Тема 1. Введение в информационную безопасность**

Понятие национальной безопасности: виды безопасности: государственная, экономическая, общественная, военная, экологическая, информационная; роль и место системы обеспечения информационной безопасности (ИБ) в системе национальной безопасности РФ; доктрина ИБ, история проблемы ИБ, угрозы ИБ; методы и средства обеспечения ИБ; методологические и технологические основы комплексного обеспечения ИБ; модели, стратегии и системы обеспечения ИБ; методы управления, организации и обеспечения работ по обеспечению ИБ; обеспечение ИБ в нормальных и чрезвычайных ситуациях; проблемы информационной войны; правовые и нормативные акты в области ИБ.

**Тема 2. Правовое обеспечение информационной безопасности**

Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации; конституционные гарантии прав граждан на информацию и механизм их реализации; понятие и виды защищаемой информации по законодательству РФ; защита интеллектуальной собственности средствами патентного и авторского права; правовая регламентация охранной деятельности; международное законодательство в области защиты информации.

**Тема 3. Организационное обеспечение информационной безопасности**

Анализ и оценка угроз информационной безопасности объекта; оценка ущерба вследствие противоправного раскрытия информации ограниченного доступа и меры по его локализации; средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа; служба безопасности объекта; подбор, расстановка и работа с кадрами; организация и обеспечение режима секретности; организация пропускного и внутриобъектового режима; организация режима и охраны объектов в процессе транспортировки; защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения; технологические меры поддержания информационной безопасности объектов; обеспечение информационной безопасности объекта (учреждения, банка, промышленного предприятия) при осуществлении международного научно-технического и экономического сотрудничества.

**Тема 4. Технические средства обеспечения информационной безопасности**

Общие вопросы организации противодействия технической разведке; основные организационные и технические мероприятия, используемые для противодействия технической разведке; методы и средства защиты режимных объектов от утечки конфиденциальной информации по техническим каналам; физические основы образования побочных электромагнитных излучений от технических средств; каналы утечки информации: электромагнитные, электрические (проводные), виброакустические; защита технических средств от утечки информации по этим каналам; нормы эффективности защиты; роль и место технического контроля эффективности защиты информации; нормы, руководящие документы по организации и ведению контроля; организационный и технический контроль; методы контроля; особенности контроля объектов в различных сферах; аппаратура контроля; взаимодействие контрольных органов с подразделениями контроля на местах; методологические основы автоматизации технического контроля; основные задачи технического контроля, требующие автоматизированного решения.

**Тема 5. Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах**

Структура и принципы функционирования современных вычислительных систем. Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах. Базовые этапы построения системы комплексной защиты вычислительных систем. Анализ моделей нарушителя. Угрозы информационно-программному обеспечению вычислительных систем и их классификация. Функции системы защиты по предупреждению угроз и устранению последствий их реализации. Классификация способов и средств комплексной защиты информации. Классификация методов защиты информации с использованием программно-аппаратных средств вычислительной системы. Организационная структура системы комплексной защиты информационно-программного обеспечения. Управление системой защиты. Функции ядра системы комплексной защиты. Многоуровневая структура системы защиты на основе программно-аппаратных средств вычислительной системы. Стандарты по оценке безопасности вычислительных систем. Требования руководящих документов Гостехкомиссии.

**Тема 6. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств**

Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Основные этапы допуска к ресурсам вычислительной системы. Использование простого пароля. Использование динамически изменяющегося пароля. Взаимная проверка подлинности и другие случаи опознания. Способы разграничения доступа к компьютерным ресурсам. Разграничение доступа по спискам. Использование матрицы установления полномочий. Произвольное и принудительное управление доступом. Разграничение доступа по уровням секретности и категориям. Понятие меток безопасности. Управление метками безопасности. Парольное разграничение доступа и комбинированные методы. Особенности программной реализации контроля установленных полномочий. Защита программных средств от несанкционированного копирования, исследования и модификации. Привязка программ к среде функционирования. Защита программ от несанкционированного запуска.

**Тема 7. Защита от компьютерных вирусов**

История появления компьютерных вирусов и факторы, влияющие на их распространение. Понятие компьютерного вируса. Основные этапы жизненного цикла вирусов. Объекты внедрения, режимы функционирования и специальные функции вирусов. Схемы заражения файлов. Схемы заражения загрузчиков. Способы маскировки, используемые вирусами. Классификация компьютерных вирусов. Общая организация защиты от компьютерных вирусов. Транзитный и динамический режимы антивирусной защиты. Поиск вирусов по сигнатурам и обезвреживание обнаруженных вирусов. Углубленный анализ на наличие вирусов путем контроля эталонного состояния компьютерной системы. Защита от деструктивных действий и размножения вирусов. Использование средств аппаратного и программного контроля. Стратегия заблаговременной подготовки к эффективной ликвидации последствий вирусной эпидемии. Технология гарантированного восстановление вычислительной системы после заражения компьютерными вирусами.

**Тема 8. Криптографическое закрытие информации**

Введение в криптографию. Представление защищаемой информации; угрозы безопасности информации; ценность информации; основные термины и понятия криптографии; открытые сообщения и их характеристики; модели открытых сообщений; исторический очерк развития криптографии; Типы криптографических систем. Простые методы шифрования: шифры подстановки и перестановки. Подстановки с переменным коэффициентом сдвига. Многослойные шифры. Использование псевдослучайных чисел для генерации ключей. Выбор порождающего числа и максимизация длины последовательности чисел ключа. Режимы шифрования. Особенности шифрования данных в режиме реального времени. Шифрование ключа при необходимости его хранения с зашифрованными данными. Скоростные и недетерминированные программные шифры. Основы скоростного шифрования. Внесение неопределенностей в процесс криптографических преобразований. Стандарты шифрования. Протоколы распределения ключей; протоколы установления подлинности; электронная цифровая подпись; Общая организация криптографической защиты информации. Использование общесистемных и специализированных программных средств для шифрования файлов и работы с секретными внешними носителями информации.

**Тема 9. Уничтожение остаточных данных**

Введение в проблему. Виды остаточных данных. Способы защиты от несанкционированного использования остаточной информации. Использование специализированных программ по уничтожению остаточных данных. Специальные режимы и особенности шифрования данных в режиме реального времени с возможность мгновенного уничтожения данных. Использование общесистемных и специализированных программных средств для мгновенного уничтожения данных.

**Тема 10. Защита от потери информации и отказов программно-аппаратных средств**

Основные способы защиты от потери информации и нарушений работоспособности вычислительных средств. Внесение функциональной и информационной избыточности. Способы резервировании информации. Правила обновления резервных данных. Методы сжатия информации. Архивация файловых данных. Особенности архивации на магнитные диски и магнитную ленту. Резервирование системных данных. Подготовка программных средств восстановления. Безопасная инсталляция программных средств. Общие сведения о нарушении доступа к дисковой и оперативной памяти. Технология восстановления дисковой и оперативной памяти. Диагностирование и устранение логических и физических дефектов магнитных дисков. Восстановление разметки дискеты и корневого каталога. Отмена результатов форматирования и восстановление поврежденных файлов данных. Защита файлов от удаления и восстановление удаленных файлов. Безопасное кэширование и дефрагментация дисковой памяти. Восстановление и оптимизация оперативной памяти компьютера. Ручное восстановление данных. Безопасное окончание работы на компьютере.

**Тема 11. Защита информационно-программного обеспечения на уровне операционных систем**

Общие сведения о реализации защиты информационно-программного обеспечения в операционных системах. Классификация функций защиты по уровням безопасности, поддерживаемых операционной системой (ОС). Ядро безопасности ОС. Аппаратная основа реализации защиты на уровне ОС. Стандарты по оценке уровня безопасности ОС. Внесение функциональной и информационной избыточности ресурсов на уровне ОС. Основы надежного администрирования ОС. Используемые способы разграничения доступа к компьютерным ресурсам, а также службы регистрации и сигнализации. Средства ОС по диагностированию и локализации несанкционированного доступа к ресурсам ВС. Безопасные файловые системы современных ОС (HPFS, NTFS). Подсистемы безопасности современных ОС, их недостатки и основные направления совершенствования.

**Тема 12. Защита информации на уровне систем управления базами данных**

Концептуальные вопросы построения уровней защиты систем управления базами данных (СУБД). Основные требования к подсистеме безопасности СУБД. Общие сведения о разграничении доступа к базам данных. Обязанности администратора по защите баз данных от несанкционированного доступа. Определение полномочий пользователей по доступу к базе данных. Использование матрицы полномочий для разграничения доступа к элементам баз данных. Мандатная система разграничения доступа. Защита данных при статистической обработке. Общее понятие о целостности базы данных. Типы ошибок, ведущих к нарушению целостности. Задание ограничений целостности. Транзакция и ее свойства. Восстановление базы данных. Особенности восстановления распределенной базы данных. Проблема непротиворечивости при параллельной обработке данных. Использование блокирования для управления параллельной обработкой. Метод независимого выполнения транзакций. Управление параллельными транзакциями на основе временных и версионных отметок. Метод обнаружения противоречивых записей журнала регистрации. Метод использования теста правильности. Разрешение тупиковых ситуаций. Инструментальные средства СУБД по обеспечению целостности баз данных.

**Тема 13. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях**

Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности. Угрозы информационно-программному обеспечению, характерные только для распределенной вычислительной среды. Использование криптографических систем для защиты данных, циркулирующих в вычислительной сети. Особенности применения симметрических и асимметрических систем шифрования. Распределение ключей между узлами вычислительной сети. Выработка секретных ключей по Диффи-Хеллману. Распределение ключей с помощью асимметрических систем шифрования. Взаимное подтверждение подлинности при обмене сообщениями в сети. Поддержание целостности циркулирующих в сети сообщений. Формирование и проверка цифровой подписи. Защита от отрицания фактов отправки и приема сообщений. Защита от наблюдения за потоком сообщений (трафиком) в сети. Защита в Internet и Intranet. Использование межсетевых экранов (брандмауэров) для защиты информации в локальных вычислительных сетях. Типы межсетевых экранов, их достоинства и недостатки. Ограничение доступа из локальной сети в Internet с помощью proxy-серверов. Безопасность JAVA-приложений.

**Тема 14. Современные средства защиты информации от НСД**

Методы и средства ограничения доступа к компонентам ЭВМ, надежность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации, типовые решения в организации ключевых систем; защита программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий (РПВ), понятие изолированной программной среды, защита программ от изменения и контроль целостности; системные вопросы защиты программ и данных, основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, вычислительных сетях.

#### **Перечень лабораторных работ**

|  |  |  |
| --- | --- | --- |
| № | Наименование темы занятия | Номер темы программы |
| 1 | Предотвращение несанкционированного доступа к компьютерным ресурсам на основе использования общесистемных и специализированных программных средств | 6 |
| 2 | Резервирование информации, подготовка программных средств восстановления, безопасная инсталляция программных средств и восстановление компьютерной системы после возникновения отказов | 10 |
| 3 | Работа с подсистемой безопасности Windows | 11 |
| 4 | Использование средств СУБД по разграничению доступа к информации и шифрованию данных | 12 |
| 5 | Использование специализированных систем по формированию и проверке цифровой подписи, а также шифрованию передаваемых по сети сообщений | 13 |

**Цели и содержание курсовой работы**

Задачей курсовой работы является обзор и сравнительный анализ стандартных и дополнительных средств обеспечения безопасности, которые предоставляют различные операционные системы (Windows, UNIX, Solaris) для безопасного функционирования, безопасной работы пользователей, а также сохранности конфиденциальной информации. Также должны быть рассмотрены вопросы сетевой безопасности.

1. Локальная и сетевая безопасность системы.
2. Обзор стандартных средств обеспечения безопасности.
3. Обзор дополнительных средств обеспечения безопасности, а также техника безопасной работы в ОС.

В качестве дополнения можно рассмотреть политики безопасности и профили защиты в различных ОС.

Ориентировочная трудоемкость — 27 часов.

**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. | К/р. | Аудит. занят. | Самост. Работа | **Всего** |
| 1 | Введение в информационную безопасность | 1 |  |  | 1 | 2 | 3 | 10 | Л1, Д1-Д13 |
|
| 2 | Правовое обеспечение информационной безопасности | 1 |  |  | 1 | 2 | 3 | 10 | Л1, Д1-Д13 |
|
| 3 | Организационное обеспечение информационной безопасности | 1 |  |  | 1 | 2 | 3 | 10 | Л1, Д1-Д13 |
|
| 4 | Технические средства обеспечения информационной безопасности | 1 |  |  | 1 | 3 | 4 | 10 | Л1, Д1-Д13 |
|
|
| 5 | Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах | 2 |  | 1 | 3 | 3 | 6 | 10 | Л1, Д1-Д13 |
| 6 | Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств | 2 | 3 | 2 | 7 | 3 | 10 | 10 | Л1, Д1-Д13 |
| 7 | Защита от компьютерных вирусов | 2 |  | 1 | 3 | 3 | 6 | 10 | Л1, Д1-Д13 |
| 8 | Криптографическое закрытие информации | 2 |  | 1 | 3 | 3 | 6 | 10 | Л1, Д1-Д13 |
| 9 | Уничтожение остаточных данных | 2 |  | 1 | 3 | 5 | 8 | 10 | Л1, Д1-Д13 |
| 10 | Защита от потери информации и отказов программно-аппаратных средств | 2 | 3 | 2 | 7 | 6 | 13 | 10 | Л1, Д1-Д13 |
| 11 | Защита информационно-программного обеспечения на уровне операционных систем | 7 | 4 | 2 | 13 | 11 | 24 | 10 | Л1, Д1-Д13 |
| 12 | Защита информации на уровне СУБД | 7 | 4 |  | 11 | 11 | 22 | 10 | Л1, Д1-Д13 |
| 13 | Специфические особенности защиты информации в локальных и глобальных компьютерных сетях | 2 | 3 | 2 | 7 | 4 | 11 | 10 | Л1, Д1-Д13 |
| 14 | Современные средства защиты информации от НСД | 2 |  |  | 2 | 4 | 6 | 10 | Л1, Д1-Д13 |
| ИТОГО: | | 34 | 17 | 17 | 68 | 62 | 130 | 10 |

**Учебно-методическое обеспечение дисциплины**

# Основная литература

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Название, библиографическое описание | Л | Лр | Пз (С) | Кп | Кр | К-во экз. в библ. (на каф.) | Гриф |
| **Л1** | Вус М.А., Долгирев Д.В., Гусев В.С., Молдовян А.А. Информатика: введение в информационную безопасность. – 2004. | 10 | 10 |  |  | 10 | Каф (5) |  |

##### Дополнительная литература

|  |  |  |
| --- | --- | --- |
| № | Название, библиографическое описание | К-во экз. в библ. (на каф.) |
| **Д1** | Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. – СПб: БХВ-Петербург. – 2001. – 368 с. | У(4) |
| **Д2** | Мафтик С. Механизмы защиты в сетях ЭВМ: Пер. с англ. - М.: Мир. - 1993. | У(1) |
| **Д3** | Феденко Б.А., Макаров И.В. Безопасность сетевых ОС. – М.: ЭКО-ТРЕНДЗ. –1999. | нет |
| **Д4** | Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – В 2-х кн. – М.: Энергоатомиздат. – 1994. | нет |
| **Д5** | Зима В.М., Молдовян А.А. Многоуровневая защита информационно-программного обеспечения вычислительных систем: Учеб. пособие. – СПб: издательско-полиграфический центр ГЭТУ. – 1997. | нет |
| **Д6** | Зима В.М., Молдовян А.А. Многоуровневая защита от компьютерных вирусов: Учеб. пособие. – СПб: издательско-полиграфический центр ГЭТУ. – 1997. | Ф(1) |
| **Д7** | Зима В.М., Молдовян А.А., Молдовян Н.А. Компьютерные сети и защита передаваемой информации. – Спб: издательство СпбГУ. – 1998. | нет |
| **Д8** | Зима В.М., Молдовян А.А., Молдовян Н.А. Защита компьютерных ресурсов от несанкционированных действий пользователей: Учеб. пособие. – Спб: типография Военной Академии Связи. – 1997 | Ф(1) |
| **Д9** | Зима В.М., Молдовян А.А., Молдовян Н.А. Основы резервирования информации и архивация файловых данных в вычислительных системах: Учеб. пособие. – Спб: издательство СпбГУ. – 1998. | Ф(1) |
| **Д10** | Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. СПб.: Лань. – 2001. | У(16) |
| **Д11** | Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999. | нет |
| **Д12** | Мельников В.В. Защита информации в компьютерных системах. - М.: Финансы и статистика; Электронинформ. - 1997. | нет |
| **Д13** | Зима В.М., Молдовян А.А. Технология практического обеспечения информационной безопасности: Учеб. пособие. - Спб: издательско-полиграфический центр ГЭТУ. - 1997. | Ф(1) |

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

|  |  |
| --- | --- |
| Авторы: |  |
| д.т.н., профессор | Молдовян А.А. |
|  |  |
| Рецензент |  |
| д.т.н., профессор | Водяхо А.И. |
|  |  |
| 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. |
|  |  |