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

*«Технология разработки информационных систем в защищенном исполнении»*

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

*«Технология разработки информационных систем в защищенном исполнении»*

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 | 54 ч. |  | Экзамен | Семестр 10 |
| Лабораторные занятия | 18 ч. |  |  |  |
| Практические занятия | 18 ч. |  |  |  |
| Курсовая работа | ч. |  | Курсовая работа | Семестр 10 |

|  |  |  |
| --- | --- | --- |
| Аудиторные занятия | 90 ч. |  |
| Самостоятельные занятия | 114 ч. |  | |
| Всего часов | 204 ч. |  |

|  |
| --- |
|  |

2011

Рабочая программа обсуждена на заседании кафедры автоматизированных систем обработки информации и управления“\_\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2011г., протокол №\_\_\_\_\_\_.

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

090301.65 – «Компьютерная безопасность»

Дисциплина «Технология разработки ИС в ЗИ» преподается на основе ранее изученных дисциплин:

1) Операционные системы

2) Организация ЭВМ и систем

3) Инфокоммуникационные системы и сети

4) Архитектура информационных систем

5) Криптографические протоколы

и обеспечивает выполнение ВКР.

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

**АННОТАЦИЯ ДИСЦИПЛИНЫ**

«Технология разработки информационных систем в защищенном исполнении» является одной из основных дисциплин цикла «Методы и средства обеспечения информационной безопасности» и обеспечивает приобретение знаний, умений и навыков в области криптографической защиты информации в соответствии с государственным образовательным стандартом.

**Цели и задачи дисциплины**

Целью преподавания дисциплины «Технология разработки информационных систем в защищенном исполнении» является освоение основ проектирования автоматизированных систем в защищенном исполнении, а также формирование практических навыков проектирования защищенных автоматизированных информационно-телекоммуникационных систем.

**Требования к уровню освоения дисциплины**

Изучение дисциплины направлено на формирование вклада в следующие компетенции:

*ПК-14* – способность осуществлять подбор, изучение и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности компьютерных систем;

*ПК-15* – способность применять современные методы и средства исследования для обеспечения информационной безопасности компьютерных систем;

*ПК-16* – способность проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности;

*ПК-17* – способность готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ;

*ПК-18* – способность разрабатывать математические модели безопасности защищаемых компьютерных систем;

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

*ПК-20* – способность проводить анализ и формализацию поставленных задач в области компьютерной безопасности;

*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 защищенном исполнении на предмет их соответствия требованиям по обеспечению ИБ;

*ПСК-8.6* – способность обеспечить ИБ процессов проектирования, создания, модернизации ОИ на базе КС в защищенном исполнении;

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

В результате изучения дисциплины студенты должны:

знать:

* основные понятия и термины ИБ;
* модели нарушителей и политик безопасности;
* основные схемы применения механизмов обеспечения ИБ;
* методы идентификации и аутентификации;
* методы обнаружения вторжений в ИС;
* методы безопасного использования коммуникационных сетей общего доступа при построении защищенных ИС;
* основные принципы применения аппаратных и программных средств обеспечения ИБ;
* типовые требования безопасности к защищенным ИС;

уметь:

* решать задачи проектирования защищенных ИС;
* применять современные программные и аппаратные средства защиты информации;

иметь представление:

* об альтернативных вариантах решения частных задач комплексной защиты информации в ИС;
* об основных требованиях к защищенным ИС;
* о современных средствах обеспечения информационной безопасности (ИБ) ИС;
* об основных угрозах информационной безопасности, моделях нарушителей и современных средствах защиты информации от несанкционированного доступа;
* о вариантах реализации криптографических механизмов защиты и аутентификации информации в ИС и протоколах управления ключами.

**Содержание рабочей программы**

**Введение**

Предмет, задачи и содержание дисциплины. Цели и задачи проектирования ИС в защищенном исполнении. Вопросы экономичности и эффективности. Рекомендуемая литература.

**Тема 1. Проблемы защиты информации в информационных системах**

Угрозы информационной безопасности (ИБ): классификация, виды, происхождение и предпосылки появления угроз. Источники угроз. Оценка угроз. Обоснование структуры и содержания системы показателей, необходимых для исследования и практического решения всех задач, связанных с защитой информации. Обоснование структуры и содержания тех параметров, которые оказывают существенное влияние на значения показателей уязвимости информации.

**Тема 2. Защита информации на технологическом уровне**

Задачи и механизмы защиты информации на технологическом уровне. Идентификация, аутентификация и авторизация. Программные средства защиты информации (ЗИ). Технология многоуровневого шифрования для защиты рабочих станций и компьютерных сетей.: требования к криптографическим механизмам по производительности, размеру кода, доступа к зашифрованной информации. Функциональная схема комплексной программной системы компьютерной безопасности. Защита информации на различных уровнях 7-уровневой модели взаимодействия открытых систем ISO. Обеспечение целостности обрабатываемой информации.

**Тема 3. Применение защищенных виртуальных сетей**

Вопросы включения телекоммуникационные системы общего для объединения локальных вычислительных сетей. Виртуальные частные сети VPN (Virtual Private Networks). Применение криптографических механизмов ЗИ, аутентификации информации и контроля целостности информации. Стандарты Internet IPSec (IP Security). Универсальность и гибкость стандартов IPSec. Использование цифровых сертификатов и структуры открытых ключей PKI (Public Key Infrastructure). Использование средств VPN для поддержания защищенных каналов трех основных типов: с удаленными сотрудниками (защищенный удаленный доступ); с сетями филиалов предприятий (защита intranet); с сетями предприятий-партнеров (защита extranet). Клиентские части VPN для основных клиетских операционных систем. Использование гибридных криптосистем.

**Тема 4. Межсетевые экраны**

Применение межсетевых экранов (МЭ) для реализации простых схем доступа. Контроль доступа в одной точке на пути соединений внутренней сети с Internet или другой публичной сетью, являющейся источником потенциальных угроз. Контроль доступа с разделением все субъектов доступа на группы по IP-адресам, явно указанным в пакете. Контроль доступа внешних пользователей к внутренним ресурсам сети при использовании ограниченного числа сервисов Internet и отсечением трафика остальных сервисов. Применение МЭ в случае нескольких точек контроля доступа. Контроль доступа к нескольким внешним сетям (к публичной части Internet и IP-сети провайдера). Использование несколько связей с Internet через разных провайдеров (для повышения надежности). Повышение требований к защите обрабатываемой информации внутри сети и использование межсетевых экранов между внутренними подсетями. Координация работы МЭ на основе единой политики доступа. Обеспечение корректной обработки пакетов при их прохождении через несколько точек доступа. распределенные межсетевые экраны. Агенты выполняющие функции МЭ. Контроль многоагентных МЭ из единого центра безопасности.

**Тема 5. Технология обнаружения вторжений**

Угрозы, атаки и вторжения. Средства обнаружения вторжений (СОВ) как механизм повышения уровня защищенности ИС. Факторы обусловливающие актуальность применения средств обнаружения вторжений и внесения изменений в соответствующие настройки подсистемы информационной безопасности. Средства обнаружения вторжений как механизм дополнения защитных функций межсетевых экранов. Межсетевые экраны – механизм отсечения потенциально опасного трафика. Направленность средств обнаружения вторжений на анализ результирующего трафика. Использование СОВ в незащищенных сегментах ИС. Использование экспертных системы и других элементов искусственного интеллекта в СОВ. Основные задачи и функции СОВ.

**Тема 6. Централизованное управление средствами безопасности**

Наличие средств централизованного управления средствами ИБ как важнейшее требование построения защищенных ИС. Преимущества централизованного управления средствами ИБ. Единство политики безопасности предприятия. Правила функционирования для всех средств защиты информации в защищенной ИС. Согласованное задание правила политик безопасности для различных устройств защиты. Использование администратором общей консоли управления для обеспечения непротиворечивость и эффективности политик безопасности. Взаимодействие индивидуальных устройств защиты, используемых в ИС, с централизованной системой управления. Защищенная передача правил безопасности индивидуальным устройствам. Протоколы распределения правил безопасности по устройствам защиты.

**Тема 7. Управление доступом на уровне пользователей**

Категории пользователей, отличающиеся правами доступа. Принцип дифференцированного распознавания. Сотрудники предприятия, работающие во внутренней сети. Удаленные и мобильные сотрудники предприятия. Сотрудники предприятий-партнеров по бизнесу. Клиенты предприятия, получающие услуги по Internet. Проблемы классифицирования по IP-адресам пользователей. Контроль доступа на уровне пользователей с использованием в межсетевых экранах собственных средств работы с учетной информацией пользователей и средств аутентификации. Интеграция средств контроля доступа с применяемыми в ИС механизмами администрирования и аутентификации пользователей. Управление доступом на уровне пользователей как способ повышения эффективности аудита событий, связанных с безопасностью. Гарантированная аутентификация пользователей. Обеспечение единого логического входа пользователя в сеть. Использование электронных токенов (смарт-карт, устройств touch-memory, ключей для USB-портов) в качестве идентификаторов. Механизмы аутентификации при осуществлении подключений (протоколы PPP PAP, PPP CHAP, PPP EAP, RADIUS, EAP-TLS, TFPOL , стандарт IEEE 802.1x, )

**Тема 8. Защита от вирусов**

Типы вредоносных программ. Компьютерные вирусы - серьезная угроза ИБ. Типы вредоносных воздействий вирусов на ИС. Жизненный цикл вирусов. Антивирусная защита как один из важнейших компонентов комплексной системы ИБ. Используется комплексов антивирусной защиты. Современные антивирусные программы. Принципы распознавания вирусов. Сигнатуры и эвристический анализ. Динамический и статический режимы антивирусной защиты. Влияние выбора операционной системы на устойчивость и подверженность к вирусным атакам.

**Тема 9. Политики безопасности и профили защиты**

Понятие политики безопасности. Подходы к организации защиты информации и формирование политики безопасности. Достоинства и недостатки “фрагментарного” подхода к управлению безопасностью. Комплексный подход как создание защищенной среды обработки информации в ИС. Политика безопасности и архитектура системы защиты. Реализация комплексного применения административно-организационных мер, физических мер и программно-аппаратных средств. Влияние на политику безопасности способа управления доступом, определяющего порядок доступа к объектам ИС. Основные виды политик безопасности: избирательная и полномочная. Избирательная политика безопасности как способ избирательного управления доступом. Избирательное (или дискреционное) управление доступом как задание администратором множеством разрешенных отношений доступа. Математическая модель правил доступа в виде матрицы доступа. Полномочная политика безопасности. Полномочное (мандатное) управление доступом как совокупность правил предоставления доступа, базирующихся на множестве атрибутов безопасности объектов и субъектов. Метки конфиденциальности информации и уровня допуска пользователя. Принцип рационального сочетании избирательного и полномочного управления доступом.

**Тема 10. Анализ безопасности функционирования ИС**

Экспертный анализ. Анализ стойкости криптографических протоколов. Безопасность криптографических механизмов. Экспертный анализ. Проверка соответствия нормативным требованиям безопасности к ИС в защищенном исполнении. Экспертный и формальный анализ защищенности. Средства автоматизированного анализа уязвимостей. Сканеры уязвимости. Анализ недекларированных возможностей системных и прикладных программ. Экспертные и интеллектуальные средства анализа безопасности. Многоагентные сканеры безопасности. Роль элементной базы в построении защищенных ИС. Катастрофоустойчивость транспортных и технологических объектов и информационная безопасность.

**Заключение**

Перспективы расширения областей применения защищенных информационных систем. Системы тайного голосования через интернет. Задача обеспечения анонимности. Роль стандартизации в области ИБ. Роль криптографии в обеспечении ИБ в современных защищенных ИС.

**Перечень лабораторных работ**

|  |  |  |  |
| --- | --- | --- | --- |
| № п.п. | Наименование лабораторных работ | Номер темы | Трудоемкость |
| 1 | Задание правил доступа в системе компьютерной безопасности «Аура» | 6,7 | 4 |
| 2 | Гарантированное затирание информации на магнитных носителях с использование средства защиты информации от несанкционированного доступа (СЗИ НСД) «Аура» | 2,5 | 4 |
| 3 | Гарантированное затирание информации на магнитных носителях с использованием программного средства СГУ. | 2,5 | 3 |
| 4 | Изучение механизмов файлового шифрования СЗИ НСД «Аура» | 3 | 4 |
| 5 | Изучение механизмов дискового шифрования СЗИ НСД «Аура» | 3 | 3 |

**Перечень практических занятий**

|  |  |  |  |
| --- | --- | --- | --- |
| № п.п. | Наименование занятия | Номер темы | Трудоемкость |
| 1 | Доступ в СУБД Oracle с аутентификацией на основе цифровых сертификатов. | 7,9 | 6 |
| 2 | Доступ в СУБД Oracle с аутентификацией по имени пользователя и паролю. | 7,9 | 6 |
| 3 | Использование eToken для безопасного доступа к информационным ресурсам, для шифрования и для ЭЦП. | 7,9 | 6 |

**Цели и содержание курсовой работы**

Целью курсовой работы является закрепление знаний и получение навыков использования программного обеспечения технологии VPN и обеспечение безопасного подключения из недоверенных сред передачи данных.

Содержанием курсовой работы является изучение и настройка режимов работы протокола IPSec на модуле NME-RVPN при использовании программного обеспечения CSP VPN gate для аутентификации и защиты данных.

Альтернативным заданием по курсовой работе является настройка программного обеспечения Secure Gateway для безопасного подключения к опубликованным приложениям из недоверенных сред передачи данных.

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** | **Лабор.**  **занят.** | **Практ.занят.** | **Аудит.**  **занят.** | | **Сам.**  **работа** | **Всего** |
| **Всего** | **в т.ч. инт.формы** |
|  | Введение | 1 |  |  | 1 |  |  | 1 |  |  |
| 1 | Проблемы защиты информации в информационных системах | 4 |  |  | 4 |  | 3 | 7 | 10 | **Л1, Л2, Д1, Д2, Д3** |
| 2 | Защита информации на технологическом уровне | 5 | 2 |  | 7 | 2 | 5 | 12 | 10 | **Л1, Л2, Д1, Д2, Д3** |
| 3 | Применение защищенных виртуальных сетей | 5 | 3 |  | 8 | 3 | 5 | 13 | 10 | **Л1, Л2, Д1, Д2, Д3** |
| 4 | Межсетевые экраны | 5 |  |  | 5 |  | 3 | 8 | 10 | **Л1, Л2, Д1, Д2, Д3** |
| 5 | Технология обнаружения вторжений | 5 | 3 |  | 8 | 3 | 5 | 13 | 10 | **Л1, Л2, Д1, Д2, Д3** |
| 6 | Централизованное управление средствами безопасности | 6 | 5 |  | 11 | 5 | 5 | 16 | 10 | **Л1, Л2, Д1, Д2, Д3** |
| 7 | Управление доступом на уровне пользователей | 6 | 5 | 9 | 20 | 14 | 5 | 25 | 10 |  |
| 8 | Защита от вирусов | 5 |  |  | 5 |  | 3 | 8 | 10 |  |
| 9 | Политики безопасности и профили защиты | 6 |  | 9 | 15 | 9 | 5 | 20 | 10 |  |
| 10 | Анализ безопасности функционирования ИС | 5 |  |  | 5 |  | 3 | 8 | 10 |  |
|  | Заключение | 1 |  |  | 1 |  |  | 1 | 10 |  |
| Курсовая работа | |  |  |  |  |  | 36 | 36 | 10 |
| Подготовка к экзамену | |  |  |  |  |  | 36 | 36 | 10 |
| ИТОГО: | | 54 | 18 | 18 | 90 | 36 | 114 | 204 |  |

# **Учебно-методическое обеспечение дисциплины**

# **Основная литература**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Название, библиографическое описание | Л | Лр | Пз (С) | Кп | Кр | К-во экз. в библ. (на каф.) | Гриф |
| **Л1** | Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. Основы информационной безопасности. М., Горячая линия – Телеком. 2006.- 544 с. | 10 | 10 | 10 |  | 10 | Ф(2)  ЧЗ1(2) |  |
| **Л2** | Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам /под ред. А.А.Шелупанова, С.Л. Груздева / М. горячая линия – Телеком, 2009.- 549 с. | 10 | 10 | 10 |  | 10 | нет |  |
| **Л3** | Соколов А. В., Шаньгин В. Ф. Защита информации в распределенных корпоративных сетях и системах – М.: ДМК, 2002. – 328 с. | 10 | 10 | 10 |  | 10 | нет |  |

##### **Дополнительная литература**

|  |  |  |
| --- | --- | --- |
| № | Название, библиографическое описание | К-во экз. в библ. (на каф.) |
| **Д1** | Столлингс В. Криптография и защита сетей: принципы и практика., 2-е изд. : Пер. с англ. – Изд. Дом «Вильямс», 2001. – 672с. | ЧЗ1(2)  Ф(2)  У(38) |
| **Д2** | Зима В.М., Молдовян А.А. ., Молдовян Н.А. Безопасность глобальных сетевых технологий. . –СПб.: БХВ-Петербург, 2001. – 318 с. | Ф(3)  ЧЗ1(3)  У(6) |
| **Д3** | Шнайер Б. Прикладная криптогргафия. Протоколы, алгоритмы, исходные тексты на языке СИ. – М.: Триумф, 2002, -816с. | Ф(2) |
| **Д4** | Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В. Криптография. Скоростные шифры. – СПб.: БХВ – Петербург, 2002. – 496 с. | нет |

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

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