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

*«Криптографические методы защиты информации»*

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

*«Криптографические методы защиты информации»*

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 – 4

Семестр – 8

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Лекции | 36 ч. |  | Экзамен | Семестр 8 |
| Лабораторные занятия | 36 ч. |  | Зачет | Семестр 8 |
| Практические занятия | 18 ч. |  |  |  |
|  |  |  |  |  |

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

090301.65 – «Компьютерная безопасность»

Дисциплина «Криптографические методы защиты информации» преподается на основе ранее изученных дисциплин:

1) Основы информационной безопасности

2) Теоретико-числовые методы в криптографии

и является фундаментом для изучения последующих дисциплин:

1) Криптографические протоколы

2) Защита ОС и СУБД

3) Защита КС и ТК

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

**АННОТАЦИЯ ДИСЦИПЛИНЫ**

Дисциплина “Криптографические методы защиты информации” 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 изучения дисциплины «Криптографические методы защиты информации» является освоение теоретических основ криптографической защиты электронной информации, а также формирование практических навыков использования симметричных и асимметричных криптографических систем для решения задач защиты и аутентификации информации в компьютерных и телекоммуникационных системах.

**Требования к уровню освоения дисциплины**

Изучение дисциплины направлено на формирование вклада в следующие компетенции:

*ПК-2* – способность применять мат.аппарат, в т.ч. с использование вычислительной техники, для решения профессиональных задач;

*ПК-12* – способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах;

*ПК-15* – способность применять современные методы и средства исследования для обеспечения ИБ КС;

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

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

*ПСК-8.4* – способность разрабатывать проектные решения по системам обеспечения ИБ объекта информатизации на базе компьютерных систем в защищенном исполнении;

*ПСК-8.5* – способность проводить анализ систем обеспечения ИБ объекта информатизации на базе компьютерных систем в защищенном исполнении на предмет их соответствия требованиям по обеспечению ИБ.

В результате изучения дисциплины студент должен быть подготовлен к решению

***следующих задач***:

1. выбор из числа существующих средств криптографической защиты информации (СКЗИ) наиболее эффективных для решения проблемы защиты информации, обрабатываемой в автоматизированных системах или передаваемой по телекоммуникационным каналам с учетом особенностей их функционирования, а также возможных попыток несанкционированного доступа к информационным ресурсам конкретной информационной системы;
2. разработка эффективных алгоритмов защиты электронной информации и их использование в сочетании с другими механизмами обеспечения безопасности информации;
3. оценка криптографической стойкости алгоритмов шифрования с использованием известных специализированных методов криптоанализа, а также на основе исследования алгебраических и вероятностно-статистических свойств шифртекстов.

В результате изучения дисциплины студент должен

***знать и уметь использовать:***

1. основные понятия и термины классической и современной криптографии;
2. математические модели открытых текстов и их основные характеристики;
3. основные статистические тесты для оценки качества шифров, случайных и псевдослучайных последовательностей;
4. основные методы шифрования, их предназначение и основные характеристики;
5. классификация шифров, математические модели шифров;
6. блочные и поточные шифры в системах компьютерной безопасности;
7. системы шифрования с открытым ключом;
8. типовые криптографические протоколы и их криптографические качества;
9. средства контроля целостности информации и защита от навязывания ложных сообщений;
10. методы аутентификации и подтверждения подлинности сообщений и пользователей;
11. основные типы электронной цифровой подписи;
12. способы построения хэш-функций и основные требования к ним;
13. методы и способы криптографической защиты информации с применением симметричных и асимметричных алгоритмов;
14. основные требования к выбору криптографических примитивов и критерии оценки их эффективности;
15. методы повышения помехоустойчивости шифров;
16. основные принципы построения систем реального масштаба времени для защиты электронной информации в автоматизированных системах;
17. основные требования, предъявляемые к системам криптографической защиты информации с учетом возможных угроз;
18. основные принципы, методы и средства предупреждения потенциальных атак на криптосистемы;
19. основные принципы построения аппаратных и программных реализаций криптографических алгоритмов;
20. типовые методы создания сетей засекреченной связи;
21. отечественные стандарты криптографической защиты информации;
22. основные стандарты криптографических методов защиты информации ведущих стран;

***владеть практическими навыками решения следующих задач:***

* защита информации криптографическими методами и средствами.
* аутентификация электронной информации криптографическими методами и средствами.

1. выбор из числа существующих средств криптографической защиты информации (СКЗИ) наиболее эффективных для решения проблемы защиты информации, обрабатываемой в автоматизированных системах или передаваемой по телекоммуникационным каналам с учетом особенностей их функционирования, а также возможных попыток несанкционированного доступа к информационным ресурсам конкретной информационной системы;
2. разработка эффективных алгоритмов защиты электронной информации и их использование в сочетании с другими механизмами обеспечения безопасности информации;
3. оценка криптографической стойкости алгоритмов шифрования с использованием известных специализированных методов криптоанализа, а также на основе исследования алгебраических и вероятностно-статистических свойств шифртекстов.

***иметь представление:***

1. об альтернативных способах защиты информации (физическая защита, стеганография);
2. об основных этапах исторического развития криптографии;
3. о современных тенденциях развития средств и методов криптографической защиты информации;
4. о принципах разработки и применения криптографических алгоритмов для защиты электронной информации;
5. о методах и критериях оценки надежности криптографической защиты информации;
6. об основных методах и средствах криптографического анализа шифрсистем;
7. об основных моделях криптоаналитических нападений на шифрсистему;
8. о требованиях к эксплуатационным качествам шифров;
9. о возможном использовании в криптографическом анализе дополнительной информации, обусловленной наличием конструктивных слабостей криптосистем, ошибками операторов или отказами шифраппаратуры, недостатками в организации сетей засекреченной связи, наличием побочных каналов утечки информации (включая электромагнитное излучение) и т. д.;
10. о протоколах управления ключами (распределении, использовании, хранении и уничтожении ключевой информации);
11. о национальных и международных производителях шифрсредств.

#### Содержание рабочей программы

**Вводная лекция**

Предмет, задачи и содержание дисциплины. История криптографии. Стеганография. Открытый текст и его основные свойства. Простейшие статистические критерии отличия открытых текстов от случайных последовательностей. Цели и задачи криптографической защиты электронной информации. Рекомендуемая литература.

**Тема 1. Основы криптографии как науки о засекречивании информации**

Характер криптографической деятельности. Виды информации, подлежащие закрытию и их свойства. Понятие о ключе и шифре. Криптографическая стойкость шифров. Простейшие шифры и их свойства. Шифр Цезаря. Шифр Вижинера. Шифры простой замены. Шифры с одноалфавитной и полиалфавитной подстановкой. Перестановочные шифры. Шифр гаммирования. Композиционные шифры. Основные требования к шифрам. Принцип Керхкоффа. Теоретико-информационный подход к оценке стойкости шифров. Условная и безусловная стойкость. Теоретическая и практическая стойкость. Проблема распределения секретных ключей. Модели шифров. Формальное представление шифра. Защищенный канал. Теорема К. Шеннона. Условная и безусловная стойкость. Совершенные шифры. Шифр с бесконечной ключевой гаммой.

**Тема 2. Криптографические нападения и понятие о криптоанализе**

Виды атак на шифры: криптографические и некриптографические нападения. Технические варианты атак с использованием аппаратных ошибок, измерения времени вычислений, измерения побочных электромагнитных излучений, измерения потребляемой мощности. Hападения с использованием человеческого фактора. Типы криптографических атак: нападения на основе шифртекста, нападения на основе известного текста, нападения на основе специально подобранных текстов, нападения на основе адаптированных текстов. Частотный криптоанализ одноалфавитных и полиалфавитных шифров. Метод угадывания слов исходного текста. Основы дифференциального и линейного методов криптоанализа блочных шифров.

**Тема 3. Современные шифры с секретным ключом**

Практическая стойкость. Секретность алгоритма шифрования и стойкость (практическая и теоретическая). Вычислительно стойкие шифры. Проблема оценки стойкости условно стойких шифров. Блочные и поточные шифры. Стойкость и длина секретного ключа. Сложность криптоаналитической таки по числу операций и по потребляемой памяти. Аддитивный шифр. Базовые принципы разработки шифров. Рассеивание и перемешивание. Имитостойкость и помехоустойчивость шифров. Последовательность шифрования, кодирования и сжатия информации в системах связи. Сжатие информации как способ повышения стойкости шифрования. Итеративные и композиционные шифры. Блочные шифры в компьютерных системах. Схемы и принципы построения блочных криптографических алгоритмов. Криптосхема Фейстеля как суперпозиция инволюций. Обобщения криптосхемы Фейстеля. Конструирование блочных шифров на основе поточных. Построение поточных шифров на основе блочных. Стандарты шифрования: DES, ГОСТ 28147-89 и AES. Конструктивные критерии. Роль стандартов в повышении эффективности средств защиты информации. Режимы использования блочных шифров.

**Тема 4. Современные поточные шифры**

Основные принципы разработки поточных шифров. Случайные и псевдослучайные последовательности: свойства, принципы и методы их построения. Способы оценки их криптографических свойств. Синхронные и самосинхронизирующиеся поточные шифры. Различие между программными и аппаратными реализациями. Криптографические параметры узлов и блоков шифраторов. Линейные и нелинейные узлы. Криптографические примитивы. Синтез шифров. Формирование алгоритма шифрования по секретному ключу как криптографический примитив. Перспективы программных шифров на основе новых типов управляемых операций. Особенности использования блоков подстановок большого размера. Идеология построения программных шифров. Проблемы использования блоков подстановок большого размера. Hедетерминированные программные шифры.

**Тема 5. Контроль целостности информации**

Вопросы контроля целостности. Коды обнаружения модификаций. Защита от нападений на основе подмены данных. Понятии о хэшировании. Хэш-функции. Стойкость хэш-функций. Схемы построения стойких хэш-функций на основе блочных шифров. Хэш-функция как составной элемент систем электронной цифровой подписи. Обнаружение искажений данных. Коды обнаружения модификаций. Защита от нападений на основе подмены данных. Вычисление кодов по секретному ключу. Вычисление кодов без использования секретных параметров. Хэш-функции. Схемы построения хэш-функций на основе блочных шифров. Hачальный вектор хэширования. Выбор длины хэш-кода и парадокс дней рождения. Основные варианты нападенй на хэш-функции. Хэш-функция - составной элемент систем электронной цифровой подписи.

**Тема 6. Управление ключами**

Составляющие элементы управления ключами в симметричных криптосистемах: генерация, распространение, хранение и уничтожение ключей. Проблема распространения секретных ключей. Проблема аутентификации секретных ключей. Использование двухключевых криптосистем для распределения ключей в симметричных криптосистемах. Гибридные криптосистемы. Проблема аутентификации открытых ключей в двухключевых криптосистемах.

**Тема 7. Открытое распределение ключей и проблема аутентификации**

Понятие односторонней функции. Метод открытого распределения ключей Диффи-Хелмана. Алгоритм быстрого возведения в большую дискретную степень. Идея электронной цифровой подписи. Открытый и закрытый ключ. Проблема дискретного логарифмирования. Проблема аутентификации открытых ключей. Атака типа "нарушитель по середине". Особенности двухключевых шифров. Решение проблемы распределения ключей в секретных системах связи. Система RSA. Секретный и открытый ключ в системе RSA. Сложность проблемы разложения чисел на два простых множителя - основа стойкости системы RSA. Генерация секретного ключа. Генерация простых чисел. Генерация открытого ключа. Расширенный Алгоритм Евклида. Шифрование и формирование цифровой подписи. Особенности системы RSA: мультипликативность и коммутативность.

**Тема 8. Криптографические протоколы**

Понятие криптографического протокола. Требования к протоколам. Анализ протоколов. Слепая подпись. Системы электронной жеребьевки, тайного электронного голосования. Протоколы разделения секрета. Протоколы распределения ключей. Протоколы генерации ключей. Протоколы установления подлинности. Доверительный центр. Цифровые сертификаты. Электронные деньги. Анонимность платежей. Понятие электронной цифровой подписи. Стандарты электронной цифровой подписи ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, . Обновление открытых и секретных ключей. Сложность задачи дискретного логарифмирования - основа стойкости цифровой подписи Эль-Гамаля. Использование случайных чисел. Формирование подписи. Проверка подписи. Открытое шифрование методом Эль-Гамаля.

**Тема 9. Криптографические методы в современных средствах защиты информации в компьютерных системах**

Организация защищенного окружения при использовании криптосистем. Криптографические механизмы в средствах защиты информации в компьютерных системах. Принцип глобального шифрования в масштабе реального времени. Дисковое шифрование с помощью скоростных программных шифров. Файловое шифрование и его особенности. Криптографические загрузчики и использование «минишифров». Скоростные программные хэш-функции. Контроль целостности эталонного состояния рабочей среды. Защита информации на технологическом уровне.

**Заключительная лекция**

Краткий обзор дисциплины. Перспективы развития криптосистем. Рекомендации по самостоятельному углублению знаний в области криптографических методов защиты информации.

**Темы лабораторных работ**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Наименование темы занятия | Номер темы программы | Трудоемкость |
| 1 | Реализация и исследование простейших алгоритмов шифрования в ручном режиме. | 3, 4 | 4 |
| 2 | Исследование и криптоанализ блочных алгоритмов шифрования при небольшом числе итераций. | 3 | 4 |
| 3 | Исследование криптографического алгоритма RSA в режиме шифрования и электронной цифровой подписи. Криптоанализ при неправильном выборе модуля. | 6 | 4 |
| 4 | Реализация и исследование криптосистемы Эль-Гамаля. Элементы дискретного логарифмирования. | 8 | 4 |
| 5 | Исследование систем ЭЦП: DSS и ГОСТ Р 34.10 -94 г. | 8 | 4 |
| 6 | Исследование криптографических свойств подстановочных преобразований. | 6 | 4 |
| 7 | Реализация и исследование схем ЭЦП с сокращенной длиной подписи. | 8 | 4 |
| 8 | Изучение и исследование схем разделения секрета. | 8 | 4 |
| 9 | Изучение и исследование программного средства криптографической защиты PGP v. 7.0. и выше. | 9 | 4 |

**Темы практических занятий**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Наименование темы занятия | Номер темы программы | Трудоемкость |
| 1 | Простейшие алгоритмы шифрования | 3, 4 | 2 |
| 2 | Блочные алгоритмы шифрования | 3 | 2 |
| 3 | Криптографический алгоритм RSA в режиме шифрования и электронной цифровой подписи. | 6 | 2 |
| 4 | Криптосистема Эль-Гамаля. Элементы дискретного логарифмирования. | 8 | 2 |
| 5 | Системы ЭЦП: DSS и ГОСТ Р 34.10 -94 г. | 8 | 2 |
| 6 | Криптографические свойства подстановочных преобразований. | 6 | 2 |
| 7 | Схемы ЭЦП с сокращенной длиной подписи. | 8 | 2 |
| 8 | Схемы разделения секрета. | 8 | 2 |
| 9 | Программное средство криптографической защиты PGP v. 7.0. и выше. | 9 | 2 |

**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** |
|  | Вводная лекция | 1 |  |  | 1 |  | 2 | 3 | 8 | **Л1, Л2, Д1, Д2** |
| 1 | Криптографические нападения и понятие о криптоанализе | 4 |  |  | 4 |  | 6 | 10 | 8 | **Л1, Л2, Д1, Д2** |
| 2 | Основы криптографии как науки о засекречивании  информации | 4 |  |  | 4 |  | 6 | 10 | 8 | **Л1, Л2, Д1, Д2** |
| 3 | Современные шифры с секретным ключом | 3 | 2 | 1 | 6 | 1 | 8 | 14 | 8 | **Л1, Л2, Д1, Д2** |
| 4 | Современные поточные шифры | 3 | 2 | 1 | 6 | 1 | 8 | 14 | 8 | **Л1, Л2, Д1, Д2** |
| 5 | Контроль целостности информации | 4 |  |  | 4 |  | 8 | 12 | 8 | **Л1, Л2, Д1, Д2** |
| 6 | Управление ключами | 4 | 12 | 6 | 22 | 6 | 8 | 30 | 8 | **Л1, Л2, Д1, Д2** |
| 7 | Открытое распределение ключей и проблема аутентификации | 4 |  |  | 4 |  | 10 | 14 | 8 | **Л1, Л2, Д1, Д2** |
| 8 | Криптографические протоколы | 4 | 16 | 8 | 28 | 8 | 12 | 40 | 8 | **Л1, Л2, Д1, Д2** |
| 9 | Криптографические методы в современных средствах  защиты информации в компьютерных системах | 4 | 4 | 2 | 10 | 2 | 10 | 20 | 8 | **Л1, Л2, Д1, Д2** |
|  | Заключительная лекция | 1 |  |  | 1 |  | 2 | 3 | 8 | **Л1, Л2, Д1, Д2** |
| ИТОГО: | | 36 | 36 | 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** | Дернова Е.С., Молдовян Н.А., Молдовяну П.А. Элементы теоретических основ криптографии. - СПб., Изд. СПбГЭТУ, 2009. – 92 с | 8 | 8 |  | 8 |  | У(72) | Минобразования РФ |
| **Л2** | Дернова Е.С., Молдовян Д.Н., Молдовян Н.А. Криптографические протоколы. - СПб., Изд. СПбГЭТУ, 2010. - 100 с. | 8 | 8 |  | 8 |  | У(35) | Минобразования РФ |

##### **Дополнительная литература**

|  |  |  |
| --- | --- | --- |
| № | Название, библиографическое описание | К-во экз. в библ. (на каф.) |
| **Д1** | Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. – СПб.: БХВ – Петербург, 2005. – 286 с. | Ф(2) |
| **Д2** | Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. – СПб.: БХВ – Петербург, 2010. – 304 | У(21) |

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

**Электронные информационные ресурсы**

|  |  |
| --- | --- |
| № | Название (адрес в Интернет) |
| **Э1** | [WWW.OSMAG.RU](http://WWW.OSMAG.RU) |

|  |  |
| --- | --- |
| Авторы:. д.т.н., профессор | 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. |