Учебный курс «Стандартные криптоалгоритмы» в системе подготовки и переподготовки специалистов по компьютерной безопасности

Харин Ю.С., Костевич А.Л.

Белорусский государственный университет,
пр. Ф. Скорины, 4, Минск, 220050, Республика Беларусь

kharin@bsu.by, kostevich@bsu.by

Учебный курс «Стандартные криптоалгоритмы» в системе подготовки и переподготовки специалистов по компьютерной безопасности

Реферат. В докладе описывается программа, программное обеспечение и опыт организации курса «Стандартные криптосистемы» в Белорусском государственном университете для подготовки и переподготовки специалистов в области компьютерной безопасности. Описывается деловая игра, сопровождающая этот курс.

Ключевые слова: стандартные криптоалгоритмы, компьютерная безопасность, обучение, деловая игра

Введение

При подготовке и переподготовке специалистов по защите информации одной из главных задач является их ознакомление с системой национальных стандартных криптографических алгоритмов [1].

В Республике Беларусь, как и во многих других странах, разработан ряд национальных стандартных криптографических алгоритмов, и их применение регламентировано нормативными документами: для защиты информации в государственных органах и банковской сфере должны использоваться только национальные стандартные алгоритмы; реализации криптографических алгоритмов должны проходить экспертизу. При этом в области защиты информации криптографическими методами Республика Беларусь наследовала от СССР только стандарт ГОСТ 28147-89 на блочный криптоалгоритм. Набор национальных стандартов, необходимых для создания полнофункциональных средств криптографической защиты информации и их использования в электронном документообороте, был разработан в Республике Беларусь только за последние 10 лет. В связи с этим остро стоит проблема переподготовки специалистов в области защиты информации. Поэтому чтобы сформировать у студентов (в том числе слушателей курсов повышения квалификации и переподготовки) целостный взгляд на систему национальных стандартов и предотвратить их стремление использовать реализации криптографических алгоритмов пусть эффективных, но не утвержденных в качестве стандартных, в программу подготовки и переподготовки специалистов по компьютерной безопасности в Белорусском государственном университете с 1997 г. был включен курс «Стандартные криптоалгоритмы».

Структура курса

Применительно к проводимой в Белорусском государственном университете подготовке и переподготовке специалистов по компьютерной безопасности, курс «Стандартные криптоалгоритмы» проводится в следующих формах:

- общий курс — для студентов по специальности «Компьютерная безопасность» со специализацией по радиофизическому направлению;
- специальный семинар, поддерживающий общий курс «Криптографические методы» — для студентов по специальности «Компьютерная безопасность» со специализацией по математическим методам;
- специальный семинар, поддерживающий специальный курс «Математическая теория информации и введение в криптологию» и специальный семинар «Математические методы криптоанализа» — для студентов по специальности «Прикладная математика» со специализацией в области компьютерной безопасности;
- курс лекций — для специалистов, проходящих курсы повышения квалификации и переподготовку в области защиты информации.

Целью курса «Стандартные криптоалгоритмы» является ознакомление студентов с национальными стандартными криптографическими алгоритмами и с оценками

их стойкости. Курс «Стандартные криптоалгоритмы» призван дать студентам сведения необходимые для разработки, анализа и эксплуатации средств криптографической защиты информации.

Курс состоит из следующих блоков:

1. *Стандартизация в области криптографической защиты информации*: вводная лекция, знакомящая слушателей с основными нормативными документами, регламентирующими применение криптографических методов защиты информации в Республике Беларусь.
2. *Блочные криптоалгоритмы*: блок занятий, на которых рассматриваются стандарт ГОСТ 28147-89 на блочный криптоалгоритм и стандарты FIPS 46 и FIPS 197 на алгоритмы DES и AES.
3. *Функции хэширования*: блок занятий, на которых рассматриваются национальный стандарт СТБ 1176.1-99 на функцию хэширования и стандарт FIPS 180–2 на алгоритм SHA.
4. *Алгоритмы электронной цифровой подписи*: блок занятий, на которых рассматриваются национальный стандарт СТБ 1176.2-99 на процедуры выработки и проверки ЭЦП, стандарт FIPS 186 на алгоритм DSA, основы технологии PKI (NIST SP 800-15, 800-32).
5. *Криптографические протоколы*: блок занятий, на которых рассматриваются:
   – стандарты на протоколы генерации ключей (национальный стандарт РД РБ 070040.1202-2003 на процедуру выработки псевдослучайных данных с использованием секретного параметра и стандарт ANSI X9.17);
   – стандарты на протоколы распространения ключей (проект национального стандарта РД РБ «Протоколы формирования общего ключа»);
   – основные понятия жизненного цикла ключей.
6. *Деловая игра*, в рамках которой студенты разрабатывают проект подсистемы криптографической защиты информации для организации электронного документооборота с использованием только национальных криптографических алгоритмов.

Отметим, что в программу курса включены блоки только по тем типам криптографических алгоритмов, по которым в Республике Беларусь действуют национальные стандарты. Каждый блок включает рассмотрение следующих сведений:

– основные понятия и определения;
– типовые конструкции криптографических алгоритмов;
– национальный стандартный криптографический алгоритм и, чтобы дать слушателям возможность сравнивать, один из наиболее широко распространенных стандартных алгоритмов других стран;
– известные в литературе атаки и оценки стойкости.

В зависимости от формы проведения курса, его содержание может меняться: больше теоретических сведений по свойствам алгоритмов для общего курса или больше практических сведений только по национальным алгоритмам для курсов повышения квалификации.

Для проведения курса «Стандартные криптоалгоритмы» используются стандарты и руководящие документы Республики Беларусь на криптографические алгоритмы, а также учебные пособия [3,4]. Курс поддерживается компьютерным практикумом на основе пакета прикладных программ «Криптолаборатория» [2], разработанном в Белорусском государственном университете.

Деловая игра

Для контроля знаний студентов проводится деловая игра: группа студентов делится на две подгруппы, каждая подгруппа разрабатывает проект подсистемы криптографической защиты информации для организации электронного документооборота некоторой типовой организации с использованием только национальных криптографических алгоритмов. Студентам сообщаются типы документов и структура компьютерной сети организации. Студенты каждой подгруппы должны:

– выделить задачи, которые должны решаться криптографическими методами для каждого из типов документов (конфиденциальность, целостность, невозможность отречения от авторства, аутентификация данных);
– выбрать набор криптографических алгоритмов, необходимых для создания подсистемы криптографической защиты информации;
– построить систему управления ключами (способы генерации ключей (в том числе на основе паролей), хранение, распространение, обеспечение целостности открытых ключей и т.д.).
– предложить проект подсистемы криптографической защиты информации, сформулировав предположения, необходимые для ее безопасной эксплуатации.

Первая подгруппа представляет проект своей подсистемы, и студенты второй подгруппы пытаются обнаружить «бреши» в ее безопасности, оценивают удобство ее эксплуатации, затем подгруппы меняются ролями.

Данная деловая игра стимулирует студентов к тщательному самостоятельному изучению программы курса, а также дает практические навыки по разработке, анализу и эксплуатации средств криптографической защиты информации.

Литература

1. Государственный образовательный стандарт высшего профессионального образования. Специальность 075200 — Компьютерная безопасность. Квалификация: математик. 2000.
2. Харин Ю.С., Агиевич С.В. Компьютерный практикум по математическим методам защиты информации. — Минск: БГУ, 2001. — 190 с.
3. Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии. — Минск: Новое знание, 2003. —320 с.
4. Menezes A.J., van Oorschot P. C., Vanstone S.A. Handbook of Applied Cryptography. — CRC Press, 1996. — 816 p.