

ЗАЩИТА ЦИФРОВЫХ СТРУКТУР ОТ НЕСАНКЦИОНИРОВАННОГО ВНЕДРЕНИЯ

Л.А. Золоторевич, А.В. Павлова

В связи с высокими темпами роста объемов производства цифровых устройств в настоящее время особую остроту приобретает проблема нарушения авторских прав [1, 2]. Ущерб от пиратства и других угроз в области производства аппаратного обеспечения составляет около 4 млрд. долларов в год, что примерно в 10 раз превышает ущерб от пиратства в области программного обеспечения [2]. Кроме пиратства появляются новые виды угроз, такие как внедрение в проект дополнительных вредоносных несанкционированных операций, изменяющих функциональное наполнение системы, внедрение механизмов деградации схемных решений с целью нарушения системы синхронизации, приводящих к нарушению временной согласованности путей распространения сигналов, и, в конечном итоге, к сбою системы, включение средств для получения конфиденциальной информации (к примеру, получение криптографических ключей) через порты контроля и к подрыву безопасности и др. [3, 4].

Очевидно, что после изготовления интегральной схемы проверить ее на наличие внесенных искажений, дополненной функциональности можно путем перепроектирования «по прототипу», восстанавливая поэтапно логику устройства и сравнивая с правильным образцом. При этом восстанавливается проект, реализованный в схеме, и сравнивается с моделью исходного проекта. Этот метод обеспечивает высокую вероятность обнаружения искажений, но время и стоимость, необходимые для выполнения перепроектирования, непомерно высоки.

Одной из известных методик защиты исходных кодов программ от обратного проектирования является обфускация, основной задачей которой является затруднение понимания функционирования программы. К сожалению, применение методов обфускации теряет свою актуальность в случае языка VHDL, так как результаты их применения не приводят к изменению конечного результата синтеза, и структурные реализации устройств до и после обфускации выглядят одинаково [2].

В докладе для блокирования преднамеренных искажений структурных реализаций цифровых устройств применяются известные методы и средства технического диагностирования. Предлагаемый метод заключается в изменении логической структуры путем включения дополнительных элементов и внедрении во входную последовательность встроенных ключей, уникальных для данной схемы.

Литература

1. Security analysis of integrated circuit camouflaging / J. Rajendran [et al.]. // ACM SIGSAC conference on Computer & communications security. Germany, Berlin. 04–08 November, 2013. P. 709–720.
2. Сергейчик В.В., Иванюк А.А. Методы лексической обфускации VHDL-описаний // Information Technologies and Systems 2013 (ITS 2013): Proceeding of The International Conference. Minsk, 24th October 2013. P. 198–199.
3. Benchmarking of hardware Trojans and maliciously affected circuits / B. Shakya [et al.] // Hardw. Syst. Secur. (HaSS). 2017. № 1(1). P. 85–102.
4. Hardware Trojans: Lessons learned after one decade of research / K. Xiao [et al.] // ACM transactions on design automation of electronic system. 2016. Vol. 22, No.1. Article 6.

ПРИМЕНЕНИЕ КРЕАТИВНЫХ МЕТОДОВ В ОБУЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д.В. Зубик, Н.Л. Черкас

Современные образовательные технологии вуза должны опираться на следующие принципы: приоритет мышления над запоминанием, активная познавательная деятельность, партнерские отношения преподавателя со студентом, интерактивные формы организации учебного процесса, сотрудничество. Это вызвано радикальным изменением спроса на рынке труда, критичного к компетенциям выпускника вуза, его способности действовать в условиях высокой неопределенности и быстрой динамики. В новых условиях необходимо делать ставку на когнитивные технологии обучения, позволяющие обеспечить эффективное понимание обучающимися реального мира, успешную адаптацию к жизни в информационно

перенасыщенной среде и интеллектуальное развитие. Рост хакерских атак и киберпреступлений, необходимость надежной защиты информационного актива компаний делает профессию специалиста по информационной безопасности одной из самых востребованных на рынке труда. Традиционная форма преподавания дисциплин, в которых делается упор на организационные и правовые методы, обычно не вызывает энтузиазма у студентов. На помощь приходят творческие технологии, прежде всего тризовские.

Так, метод «маленьких человечков» применим для моделирования злоумышленных атак на информационные ресурсы компании и планирования адекватных контрмер. Метод РВС развивает творческое мышление при построении надежной системы информационной безопасности предприятия. Системный оператор используется при анализе эволюции средств промышленного шпионажа для прогнозирования каналов утечки ближайшего и отдаленного будущего. Таблица основных приемов разрешения противоречий помогает при проектировании системы защиты компьютерных сетей. Опыт показывает, что студенты позитивно воспринимают деловые игры на базе творческих технологий. Внедрение тризовских методов обучения в учебный процесс позволяет выработать у студента умение ориентироваться в меняющихся условиях, навыки анализа нестандартных проблемы, самостоятельной разработки и реализации управленческих решений, что в конечном итоге позволяет существенно повысить уровень и качество профессиональной подготовки в целом.

Литература

1. Экономическая безопасность предприятия (фирмы) / В.Б. Зубик [и др.]. Минск: Вышэйшая школа, 1998. 391 с.
2. Nesbor K. Arbeit in Gruppen.Projektarbeit. – Kompetenzzentrum «Hochschuldidaktik für Niedersachsen» an der TU Braunschweig, 2010.

РЕАЛИЗАЦИЯ ШИФРОВАНИЯ С ЭЛЕМЕНТАМИ ПОДПИСИ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Н.С. Иванин

Схема шифрования с элементами подписи (шифрование с ЭП) была предложена в [1] для одновременного решения задач конфиденциальности и аутентификации. Эта схема как правило является частью систем, использующих инфраструктуру с публичным ключом. В таких системах пользователи регистрируют свои публичные ключи вместе с удостоверяющим центром, которые являются независимыми между собой в отличии от разделяемых ключей в системах с симметричным шифрованием (в таких системах у пользователей хранится одинаковый ключ). При шифровании с ЭП для защиты коммуникации пользователю необходимо получить публичный ключ второго пользователя из удостоверяющего центра и зашифровать сообщение.

В качестве схемы была использована схема шифрования с ЭП без использования сертификата, основанная на использовании эллиптических кривых без вычисления функции пересчета пар. Эта схема основана на схеме Барбосы-Фашима, описанной в [2]. Такой подход позволяет шифровать сообщения любой длины и использовать одноразовый ключ симметричного шифрования. Используемая в схеме хэш-функция является устойчивой к коллизиям.

Полученная система состоит из 3 частей: сервера генерации ключей(СГК), отправителя и получателя. Сначала СГК вычисляет параметры, которые будут затем использованы в схеме шифрования. После чего пользователь на своей стороне вычисляет свой публичный ключ. На третьем этапе происходит извлечение частичного приватного ключа. Эта операция выполняется на сервере генерации ключей на основе идентификатора пользователя. Затем полученный приватный ключ и публичный ключ присваиваются пользователю также на основе его идентификатора. С помощью публичного и частичного приватного ключей пользователь зашифровывает сообщение и отправляет его в канал связи. Получатель с помощью своего публичного и полного приватного ключей расшифровывает и верифицирует полученное сообщение.