УДК 621.3.01+621.38 DOi 10.30837/ bi.2020.1(94).06

П.С. Клімушин[1], Т.П. Колісник[2], О.Ф. Лановий[3], М.О. Можаєв[4]

[1]к.т.н., доцент, кафедра інформаційних технологій та кібербезпеки ХНУВС, м. Харків, Україна, klimushyn@ukr.net, ORCID iD: https://orcid.org/0000-0002-1020-9399;

[2]к.п.н., доцент, кафедра інформаційних технологій та кібербезпеки ХНУВС, м. Харків, Україна, ktp201505@gmail.com, ORCID iD: https://orcid.org/0000-0002-7442-8136;

[3]к.т.н., доцент, кафедра програмної інженерії ХНУРЕ, заступник декана факультету КН, м. Харків, Україна, oleksiy.lanovyy@nure.ua, ORCID iD: https://orcid.org/0000-0002-4504-4301;

[4]к.т.н., доцент, кафедра інформаційних технологій та кібербезпеки ХНУВС, м. Харків, Україна, mikhail.mozhayev@hniise.gov.ua , ORCID iD: https://orcid.org/0000-0003-1566-9260

ДОСЛІДЖЕННЯ СЕРЕДОВИЩ МОДЕЛЮВАННЯ МІКРОПРОЦЕСОРНИХ СИСТЕМ НА МІКРОКОНТРОЛЕРАХ З ДОДАТКОВИМИ МОДУЛЯМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Сфера застосування захищених мікропроцесорних систем складається з забезпечення функцій інформаційної безпеки: автентіфікації суб'єктів і об'єктів інформаційної взаємодії, шифрування інформації, контроля цілісності, управління доступом, управління ключами. Сьогодні актуальним завданням є проектування мікропроцесорних систем з додатковими функціями криптографічного захисту інформації з допомогою використання різних програмних середовищ комп'ютерного моделювання. В роботі проаналізовано найбільш ефективні та доступні програми комп'ютерного моделювання мікропроцесорних систем та надано практичні рекомендації щодо їх використання. Показано,що найбільш потужною системою автоматизованого проектування вважається програмний пакет Proteus, який дозволяє змоделювати роботу різних мікропроцесорних пристроїв з підтримкою декількох сімейств мікроконтролерів від різних виробників. До основних переваг відносяться: виконання всіх етапів розробки в єдиному середовищі; можливість написання, налагодження і тестування мікропрограмного забезпечення, генерування діагностичних повідомлень з пошуку помилки програмування. Використання Multisim в навчальному процесі дає можливість: переглядати і змінювати стан вмісту регістрів, пам'яті програм і даних, осередків стека і біта конфігурації; візуалізувати результат виконання окремої команди або програми в цілому; демонструвати практику спільного застосування мов С і Асемблер в одному проекті з метою оптимізації програми; вивчати основи роботи і особливості функціонування периферійних пристроїв. Проте обмежений набір мікроконтролерів в програмі Multisim накладає суттєві обмеження на можливість її використання при розробці реальних проектів. Програма комп'ютерного моделювання TINA має значно простіший русифікований інтерфейс у порівнянні з Proteus VSM з можливістю укладення всієї інформації про створений проект в одному файлі. У порівнянні з Multisim бібліотека TINA містить значно більше моделей мікроконтролерів, а вбудований програматор дозволяє модифікувати програми та спостерігати результати. Можливість використання безкоштовної версії TINA-TI та наявність онлайн-версії TINACloud з використанням хмарних технологій робить цю програму дуже корисною для освіти. Веб-сервіс пропонує безліч освітніх ресурсів і можливість виконання дослідження з проектування мікропроцесорних систем.

МОДЕЛЮВАННЯ, МІКРОКОНТРОЛЕРИ, МІКРОПРОЦЕСОРНА СИСТЕМА, КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ, PROTEUS, MULTISIM, TINA

Сфера применения защищенных микропроцессорных систем служит для обеспечения функций информационной безопасности: аутентификации субъектов и объектов информационного взаимодействия, шифрование информации, контроля целостности, управления доступом, управления ключами. Сегодня актуальной задачей является определение защищенности микропроцессорных систем с помощью использования различных программных сред компьютерного моделирования. В работе проанализированы наиболее эффективные и доступные программы компьютерного моделирования микропроцессорных систем и даны практические рекомендации по их использованию. Показано, что наиболее мощной системой автоматизированного проектирования является программный пакет Proteus, который позволяет смоделировать работу различных микропроцессорных устройств с поддержкой нескольких семейств микроконтроллеров от разных производителей. К основным преимуществам относятся: выполнение всех этапов разработки в единой среде; возможность написания, отладки и тестирования микропрограммного обеспечения, генерирования диагностических сообщений по поиску ошибки программирования. Использование Multisim в учебном процессе дает возможность: просматривать и изменять состояние содержимого регистров, памяти программ и данных, ячеек стека и бита конфигурации; визуализировать результат выполнения отдельной команды или программы в целом; демонстрировать практику совместного применения языков С и Ассемблер в одном проекте с целью оптимизации программы; изучать основы работы и особенности функционирования периферийных устройств. Однако ограниченный набор микроконтроллеров в программе Multisim накладывает существенные ограничения на возможность ее использования при разработке реальных проектов. Программа компьютерного моделирования TINA имеет простой русифицированный интерфейс по сравнению с Proteus с возможностью

заключения всей информации о созданном проект в одном файле. По сравнению с Multisim библиотека TINA содержит значительно больше моделей микроконтроллеров, а встроенный программатор позволяет модифицировать программы и наблюдать результаты. Возможность использования бесплатной версии TINA-TI и наличие онлайн-версии TINACloud с использованием облачных технологий делает эту программу очень полезной для образования. Веб-сервис предлагает множество образовательных ресурсов и возможность выполнения исследований по проектированию микропроцессорных систем.

МОДЕЛИРОВАНИЕ, МИКРОКОНТРОЛЛЕРЫ, МИКРОПРОЦЕССОРНАЯ СИСТЕМА, КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ, PROTEUS, MULTISIM, TINA

The field of application of the protected microprocessor systems includes information security functions: authentication of subjects and objects of information interaction, information encryption, integrity control, access control, key management. Today, the urgent task is to establish the security of microprocessor-based systems using a variety of computer simulation software environments. The work analyzes the most effective and affordable computer simulation programs for microprocessor systems and gives practical recommendations for their use. It has been shown that the most powerful computer-aided design system is the Proteus software suite which allows simulating the operation of various microprocessor devices with support for several microcontroller families from different manufacturers. The main advantages include: performing all stages of development in a single environment; the ability to write, debug, and test firmware, generate diagnostic messages to find programming errors. Using Multisim in the educational process makes it possible to: review and change the status of the register content, program memory and data, stack cells and bit configuration; visualize the result of the execution of a single command or a program as a whole; demonstrate the practice of joint use of languages C and Assembler in one project in order to optimize the program; to study the basics of operation and features of peripheral devices functioning. However, the limited set of microcontrollers in the Multisim program imposes significant restrictions on the possibility of using it for development of real projects. The computer simulation program TINA has a russified interface that is much easier compared to the Proteus with an ability to enter all the information about the created project into one file. Compared to Multisim, the TINA library contains significantly more microcontroller models, and the built-in programmer allows modifying programs and observing the results. Being able to use the free version of TINA-TI and having an online version of TINACloud using cloud technologies makes this program very useful for education. Web service offers many educational resources and the ability to perform research on the design of microprocessor systems.

MODELING, MICROCONTROLLERS, MICROPROCESSOR SYSTEM, CRYPTOGRAPHIC INFORMATION PROTECTION, PROTEUS, MULTISIM, TINA

Вступ

Сучасну мікроелектроніку важко уявити без такої важливої складової, як мікроконтролери (МК). Мікроконтролерні технології дуже ефективні, так як один і те ж пристрій, який раніше збирався на традиційних елементах, будучи зібраний з застосуванням мікроконтролерів, стає простішим. Крім того, із застосуванням мікроконтролерів з'являються практично безмежні можливості по додаванню нових споживчих функцій, а також забезпечення безпеки їх функціонування. Досить просто поміняти програму або мікропрограму.

Моделювання в електроніці зводиться до вирішення групи задач синтезу і задач аналізу. При цьому під синтезом розуміють створення якогось варіанта схеми, не обов'язково остаточного. До задач аналізу входить вивчення властивостей схеми за заданою в результаті синтезу її структури, характеру вхідних компонентів і їх параметрів. В процесі модулювання синтез як задача може виконуватися багато разів, чергуючись з вирішенням задач аналізу.

Становлення Інтернет речей є однією з основних причин трансформації ринку мікропроцесорних систем в напрямку розробки захищених інтелектуальних систем, об'єднаних в єдину глобальну обчислювальну мережу. Для забезпечення зростаючих потреб ринку актуальним завданням є визначення найбільш ефективних середовищ проектування мікропроцесорних систем на мікроконтролерах з додатковими модулями криптографічного захисту інформації.

Оскільки Інтернет речей привносить мережевий інтелект у фізичні речі навколо нас, особливо гостро постає питання безпеки. Життя сучасної людини залежить від транспортної, промислової, комунальної, цивільної та медичної інфраструктури, незаконне маніпулювання якими може привести до трагічних наслідків. Не менш важливим є захист приватного життя і персональних даних, доступ до яких зловмисники можуть отримати через злам систем промислово-побутової автоматизації, моніторингу, безпеки і контролю доступу, мобільної та домашньої електроніки тощо. Пристрої Інтернет речей можуть бути не лише об'єктом атаки, але і суб'єктом, наприклад, IoT-ботнети використовуються зловмисниками для організації DDoS-атак, поширення вірусів тощо. Проблеми пов'язані з безпекою, що є основними стримуючими факторами впровадження технологій Інтернет речей.

В Інтернеті захист даних від несанкціонованого доступу і збереження інформацією своїх основних властивостей (конфіденційність, автентичність та цілісність) реалізується криптографічними методами, такими як шифрування та хешування. Разом з тим для вироблення ключів та векторів ініціалізації необхідні генератори випадкових чисел.

Під захищеними криптографічними мікроконтролерами розуміються спеціалізовані напівпровідникові

пристрої, що мають на кристалі, крім стандартного процесорного ядра, додаткові апаратні блоки — криптографічні акселератори. Такі апаратні акселератори необхідні для значного прискорення виконання складних криптографічних операцій — генерації випадкових чисел, шифрування і розшифрування, формування і перевірки електронного підпису тощо.

Сфера застосування захищених мікропроцесорних систем складається з забезпечення функцій інформаційної безпеки: автентіфікації суб'єктів і об'єктів інформаційної взаємодії, шифрування інформації, контроля цілісності, управління доступом, управління ключами [1].

Одним з найбільш популярних наборів мікроконтролерів, які застосовуються в системах оброблення даних, контролю і управління та захисту інформації є пристрої, що випускаються фірмою Microchip та відомі під абревіатурою PIC. Наряду з цім, останнім часом корпорація Atmel (США) стала виробляти набір мікросхем на ядрі AVR, яке має більш досконалу архітектуру й забезпечує МК цього набору високу швидкодію та низьке енергоспоживання, що дає їм відчутну перевагу, порівняно з контролерами PIC. До того ж, цінова політика корпорації Atmel є більш привабливою для розробників таких систем. Порівняно з пристроями PIC, МК AVR мають більш розвинену систему команд, що налічує до 133 інструкцій, а flash-пам'ять програм має можливість внутрішньосхемного програмування. Архітектура ядра AVR оптимізована так, що дозволяє використовувати мову високого рівня С.

Для задач, у яких вимоги до захисту інформації особливо високі – смарт-карти, електронна комерція, автентифікація користувачів, шифрування даних, фірма Atmel пропонує спеціалізовані мікроконтролери – зокрема, сім'ї SecureAVR, які поєднують звичайне AVR-ядро з додатковими модулями для підтримки криптографічних операцій та підвищення фізичної захищеності мікросхем до різного роду атак. Отже, застосування мікроконтролерів AVR забезпечує додаткові переваги спеціалістам з інформаційної безпеки.

Застосування комп'ютерного моделювання для проектування мікропроцесорних систем з додатковими функціями криптографічного захисту інформації є непростою задачею, яка вимагає предметного дослідження.

Сьогодні в світової практиці застосовується широкий спектр програмних середовищ комп'ютерного моделювання. До них, перш за все, слід віднести такі програми як Proteus VSM, NI Multisim, TINA.

Приклади використання програм комп'ютерного модулювання електронних схем в своїх наукових працях надають вітчизняні та закордонні автори: Совин Я.Р., Наконечний Ю.М., Опірський І.Р., Стахів М.Ю. [1] — аналізують моделювання можливих загроз інформаційної безпеки в системах з використанням мікроконтролерів; Алехин В.А. [2,3] — визначає розвиток навчальних комплексів з моделювання по електротехніці, електроніці та мікроконтролерам в середовище TINA; Березняков С.В., Греков А.В. [4], Матвеенко І.П. [5] та Филатов М. [6] — надають приклади моделювання мікроконтролерів в системі моделювання Proteus; Макаренко В., Бабко А. [7], Найденко Е.В. [8] та Колесникова Т. [9], Квашнін В.О., Бабаш А.В., Квашнін В.В. [10] — визначають елементи моделювання роботи мікроконтролерів у програмі Multisim; Ляшенко О, Журіло О. [11] та багато інших.

В цілому аналіз цих робіт показує, що проблема використання програмних середовищ моделювання мікропроцесорних систем досконально ще ні досліджена і має мінливий характер в залежності від етапів їх розвитку та кон'юнктури ринку мікроконтролерів.

Обираючи інструментальні засоби моделювання, доцільно брати до уваги: підтримку можливо більшої кількості мікроконтролерів; різноманітність вбудованих інтерфейсів (RS-232, IEEE1284/LPT, USB) та додаткових компонентів, що розширюють функціональні можливості проектування мікропроцесорних систем.

Метою дослідження є визначення найбільш ефективних та доступних програм комп'ютерного моделювання мікропроцесорних систем та надання практичних рекомендацій щодо їх застосування.

1. Дослідження системи проектування Proteus

Аналіз наукових праць свідчить, що найбільш потужною системою автоматизованого проектування вважається програмний пакет Proteus VSM, який дозволяє змоделювати роботу різних мікропроцесорних пристроїв. Програма Proteus VSM є симулятором наскрізного проектування, що має на увазі створення мікропроцесорної системи, починаючи з графічного зображення і закінчуючи виготовленням друкованої плати пристрою.

Proteus VSM складається з двох самостійних програм: ISIS — програма синтезу та моделювання безпосередньо електронних схем і ARES — програма розробки друкованих плат. Крім того, до складу восьмої версії входить інтегроване середовище розробки VSM Studio, що містить у собі текстовий редактор з підсвічуванням синтаксису, компілятор асемблера, симулятор, налагоджувач й інтерфейс із апаратними емуляторами та дозволяє швидко написати програму для мікроконтролера, використовуваного в проекті, і здійснити її компіляцію [4].

При розробці програмного забезпечення мікроконтролерів необхідно звернути увагу на безкоштовні програмні засоби (AVR Studio, WinAVR) підтримки

проектування та налагодження систем на мікроконтролерах AVR, робота з якими економить гроші та забезпечує ліцензовану чистоту кінцевого програмного продукту.

Останнім часом усе популярніше стає використання компіляторів мов високого рівня при написанні програм для МК. Найбільше поширення при цьому одержали компілятори мови С з можливістю оптимізації коду, оскільки в цій мові найбільш просто реалізуються всі необхідні можливості з керування апаратними засобами МК. Крім С при розробці програмного забезпечення для МК застосовуються й інші мови високого рівня. Так, для МК сімейства AVR існують також компілятори мов Basic, Pascal і Forth.

Proteus підтримує наступні етапи розробки: розробка схеми електричної принципової (введення в графічному редакторі); моделювання схеми з використанням різноманітних віртуальних приладів; розробка друкованої плати, включаючи 3D-візуалізацію її збірки.

В Proteus реалізовані таки можливості налагодження мікропрограмного забезпечення: спільне моделювання роботи мікроконтролера, виконуючого задану програму, і оточуючих його аналогової і цифрової схем; широкі налагоджувальні можливості, в т.ч. доступ до вмісту регістрів і пам'яті, завдання точок зупинки програми, покрокове виконання; налагодження на рівні вихідного коду (С, Бейсік, Асемблер, в залежності від типу використовуваного для налагодження файлу з випробовуваним мікропрограмним забезпеченням); підтримка декількох сімейств мікроконтролерів від різних виробників, в т.ч.: PIC12, PIC16, PIC18 і PIC24 (Microchip); 8051/8052, в т.ч. похідні від них, що випускаються Philips і Atmel; AVR, Tiny AVR і Mega AVR (Atmel); ARM7, в т.ч. LPC2000 (NXP); HC11 (Freescale) і мікроконтролерні модулі BASIC Stamp (Parallax); ведеться робота по додаванню підтримки інших МК.

До переваг використання Proteus відносяться: виконання всіх етапів розробки електронного пристрою на основі мікроконтролера в єдиному середовищі; можливість написання, налагодження і тестування мікропрограмного забезпечення, ще до фізичного виготовлення дослідного зразка системи; генерування діагностичних повідомлень (наприклад, при виконанні непередбачуваної інструкції) як з боку процесорного управління, так і з боку моделей пристроїв введення-виведення, що дозволяє виявити складні в пошуку помилки програмування; прискорення процесу розробки електронного пристрою; підтримка спільної роботи з апаратними пристроями, що підключені через порт комп'ютера.

Є демонстраційна версія яку можна використовувати для навчальних закладів з обмеженням (рис. 1): неможливість збереження проекту та його друку; неможливість створення своїх власних схем на основі МК, проте після відкриття існуючих схем є можливість змінити програму, виконувану мікроконтролером, і поспостерігати результат її виконання.

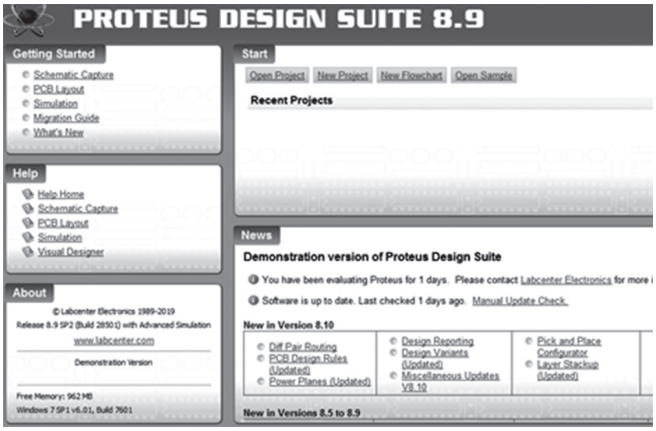

Рис. 1. Стартова сторінка демоверсії Proteus

Таким чином, використовуючи інтегровану середу AVR Studio і демонстраційну версію програми Proteus, з'являється можливість досить легко, з найменшими матеріальними і тимчасовими витратами, спроектувати мікропроцесорну систему, що включає будь-якій мікроконтролер, провести її налагодження і розводку плати і тільки потім створювати реальний пристрій [5, 6].

2. Дослідження середовища моделювання NI Multisim

Традиційно в лабораторних практикумах вузів застосовують програми Electronics Workbench і Multisim компанії National Instruments (NI). Програма NI Multisim має простий наочний інтерфейс, потужні засоби графічного аналізу результатів моделювання, наявність віртуальних вимірювальних приладів, які копіюють реальні аналоги.

Крім того, NI Multisim дозволяє перетворити будь-яку електричну схему в простий процес, з можливістю додати будь-який елемент в схему. Версія NI Multisim Student Edition призначена для навчальних закладів і включає в себе навчальні курси, підготовлені апаратні рішення і робочі підручники (рис. 2). Однак ця версія також вимагає придбання ліцензійного програмного забезпечення.

Програмне середовище NI Multisim 14 містить програмний модуль MCU, що дозволяє моделювати програмовані цифрові пристрої на основі восьмирозрядних мікроконтролерів MCS-51 і PIC-16 фірми Microchip, а також компілятори з мови С і Ассемблер зазначених мікроконтролерів. Ці мікроконтролери мають традиційну архітектуру, загальну систему команд і розширені периферійні функції, що дозволяє широко застосовувати їх в світовому

мікропроцесорному ринку завдяки оптимального поєднання ціни і можливостей.

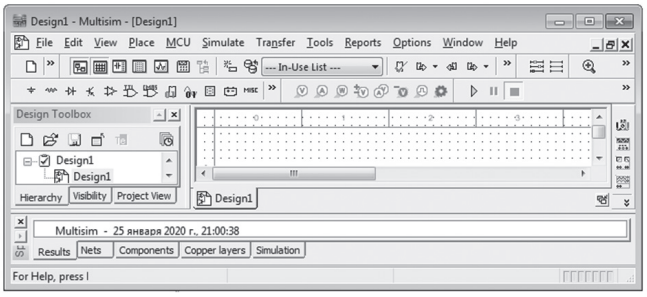

Рис. 2. Стартова сторінка Multisim Student Edition

Використання Multisim в навчальному процесі дає можливість [8]:

– переглядати і змінювати стан вмісту регістрів, пам'яті програм і даних, осередків стека і біта конфігурації, що сприяє розумінню і кращому засвоєнню принципів роботи і архітектури мікроконтролерів;

– візуалізувати результат виконання окремої команди або програми в цілому, підвищуючи наочність викладеного матеріалу;

– наводити приклади практичного застосування, активізуючи інтерес до дисципліни;

– демонструвати практику спільного застосування мов С і Асемблер в одному проекті з метою оптимізації програми;

– вивчати основи роботи і особливості функціонування периферійних пристроїв, використовуючи їх моделі з бази даних Multisim;

– коригувати зміст навчального матеріалу з урахуванням особливостей аудиторії.

Бібліотека Multisim містить групу електромеханічних моделей, що дає можливість вводити в лабораторний практикум міжпредметних компонент і створювати комплексні лабораторні роботи і приклади демонстраційних схем при наскрізному інформаційному навчанні з суміжних дисциплін одночасно, що істотно підвищує ефективність засвоєння матеріалу, що викладається.

З огляду простоти і зручності використання Multisim є найбільш прийнятним засобом для освоєння основних прийомів проектування мікропроцесорних систем. Застосування Multisim в процесі навчання сприяє підвищенню якості освіти та виробленню необхідних професійно-схемотехнічних компетентностій, а також дає можливість рекомендувати його для розробки курсу інтерактивного навчання.

Проте обмежений набір мікроконтролерів в програмі NI Multisim накладає суттєві обмеження на можливість її використання при розробці реальних проектів. З вищевикладеного можна зробити висновок про те, що використовувати програму NI Multisim доцільно на етапі навчання програмування мікроконтролерів на мові С або Асемблер. Всі необхідні для налагодження засоби встановлюються автоматично при інсталяції NI Multisim або є їх дистрибутиви, що знаходяться в папці з встановленою програмою і у користувача немає необхідності пошуку і встановлення додаткового програмного забезпечення. А на сьогоднішній день, мабуть, найкращою програмою для моделювання мікроконтролерів при вивченні їх можливостей і розробки пристроїв з їх застосуванням є Proteus. [7].

3. Дослідження програмного середовища TINA

В останні роки з'явилася нова ефективна програма комп'ютерного моделювання TINA, яка містить інтегровану частину для проектування друкованих плат, має значно простіший інтерфейс у порівнянні з Proteus VSM, який легко освоюється студентами. Крім того, вся інформація про створений проект укладена в одному файлі, який можна переслати і відкрити на іншому комп'ютері для продовження моделювання або перевірки роботи студентів. Наряду з цим, програма має русифікований інтерфейс, що значно підвищує ефективність засвоєння навчального матеріалу (рис. 3).

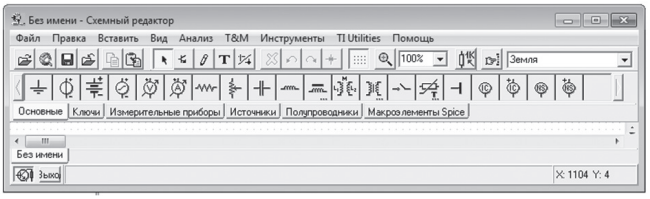

Рис. 3. Стартова сторінка програми TINA

Програма розробляється спільними зусиллями співробітників компаній Texas Instruments і DesignSoft. TINA є потужним інструментом для моделювання електронних схем та мікроконтролерів, дозволяє проводити дослідження схем при зміні параметрів, оптимізації, виконувати частотний і спектральний аналіз, досліджувати перехідні характеристики тощо. У порівнянні з Multisim бібліотека TINA містить значно більше моделей мікроконтролерів — більше 1000, які можна програмувати на Асемблері і на мові С, моделювати, налагоджувати в змішаних схемах. Вбудований програматор дозволяє модифікувати програми та спостерігати результати.

Можливість використання безкоштовної і досить ефективної версії TINA-TI робить цю програму дуже корисною для освіти. Наряду з цим, для мобільного навчання компанія DesignSoft пропонує новий програмний продукт TINACloud [12], який використовує хмарні інтернет-технології і може запускатися через браузер на вашому пристрої. Це багатомовна онлайн-версія популярного програмного забезпечення TINA, на яку можна підписатися за частку ціни TINA (студентська ліцензія на рік 12 євро). Цей сервіс пропонує безліч освітніх ресурсів і можливість виконання

віртуального дослідження і лабораторного практикуму по мікропроцесорної техніки.

Аналіз результатів робіт професора Алехина В. А. показує високу ефективність використання програм TINA та TINACloud в начальному процесі. Ефективність цієї програми підтверджує створений автором навчальний комплекс з електротехніки, електроніки та мікроконтролерів [2, 3].

При застосуванні програми TINA в налагодженні завдань програмування та інтерактивного моделювання пристроїв на мікроконтролерах доцільно вибрати популярні мікроконтролери PIC16F84A і PIC16F877A компанії Microchip Technology Incorporated, так як Microchip надає безкоштовну інтегровану програмну середу розробки мікроконтролерів MPLAB IDE, яка дозволяє писати, налагоджувати, оптимізувати текст програми, включає в себе редактор тексту, симулятор і менеджер проектів, підтримує роботу емуляторів, програматорів і інших налагоджувальних засобів. Щоб полегшити програмування на С поєднання мікроконтролерів з зовнішніми периферійними пристроями, доцільно використовувати середу mikroC PRO for PIC v.6.5.0 компанії MikroElektronika, яка також є безкоштовної при умовах HEX-файлу проекту менш 2кбайт, що є достатнім в навчальних завданнях.

Висновки

На підставі проведеного дослідження можна відзначити чітку тенденцію щодо апаратної підтримки криптографічних операцій та підвищення фізичної захищеності мікросхем до різного роду атак.

Використання захищених криптографічних мікроконтролерів дає змогу підняти швидкодію шифрування AES в 10-20 разів для 8/16-бітових МК та до 150 разів для 32-бітових МК порівняно з програмними реалізаціями алгоритму. Зростання швидкодії обчислення хеш-алгоритмів SHA-1, SHA-256 у 32-бітових МК становить більше ніж в 100 разів, а для криптографічних хеш-алгоритмів HMAC наближається до 500.

У 32-бітових мікроконтролерах спостерігається тренд до впровадження комплексних рішень безпеки, які б не тільки пришвидшували широке коло симетричних і асиметричних алгоритмів і протоколів, але і надавали можливість захищеного зберігання та генерування ключів, безпечного завантаження і оновлення коду, підтримки електронних підписів та сертифікатів [1].

Основними засобами забезпечення безпеки є програмне або апаратне використання симетричних криптоалгоритмів і криптографічних хеш-функцій, застосування електронних підписів, розвивається використання асиметричних криптоалгоритмів.

Складністю для захисту мікроконтролерів є їх обмеженість в ресурсах процесора і доступної пам'яті за сучасними мірками. Підлаштовуючи апаратну частину для максимальної оптимізації обчислювальних витрат, обсягу пам'яті і споживання енергії, на вільних обчислювальних потужностях можливе використання симетричних (AES, 3DES — підтримуються апаратно в Atmel AVR XMEGA) і асиметричних криптоалгоритмів (RSA , DH, ECC), обчислення контрольної суми (CRC підтримується апаратно в мікроконтролерах сімейства Atmel AVR XMEGA), використання криптографічних хеш-функцій, комбінація вищевказаних методів [10].

В дослідженні було визначено, що для моделювання мікропроцесорних систем на мікроконтролерах з додатковими модулями криптографічного захисту інформації доцільно використовувати наступні програми: Proteus VSM, NI Multisim, TINA.

Порівняльний аналіз цих програм комп'ютерного моделювання з точки зору їх доступності, простоти освоєння й ефективності застосування викладачами і студентами в навчальному процесі засвідчив.

Найбільш потужною системою автоматизованого проектування вважається програмний пакет Proteus VSM, який дозволяє змоделювати роботу різних мікропроцесорних пристроїв з підтримкою декількох сімейств мікроконтролерів від різних виробників.

До основних переваг відносяться: виконання всіх етапів розробки в єдиному середовищі; можливість написання, налагодження і тестування мікропрограмного забезпечення, генерування діагностичних повідомлень з пошуку помилки програмування; прискорення процесу розробки мікропроцесорного пристрою; підтримка спільної роботи з апаратними пристроями, що підключені через порт комп'ютера.

Використання Multisim в навчальному процесі дає можливість: переглядати і змінювати стан вмісту регістрів, пам'яті програм і даних, осередків стека і біта конфігурації; візуалізувати результат виконання окремої команди або програми в цілому; демонструвати практику спільного застосування мов С і Асемблер в одному проекті з метою оптимізації програми; вивчати основи роботи і особливості функціонування периферійних пристроїв. Проте обмежений набір мікроконтролерів в програмі Multisim накладає суттєві обмеження на можливість її використання при розробці реальних проектів.

Програма комп'ютерного моделювання TINA має значно простіший русифікований інтерфейс у порівнянні з Proteus VSM з можливістю укладення всієї інформації про створений проект в одному файлі. У порівнянні з Multisim бібліотека TINA містить значно більше моделей мікроконтролерів, а будований програматор дозволяє модифікувати програми та спостерігати результати.

Можливість використання безкоштовної версії TINA-TI та наявність онлайн-версії TINACloud з використанням хмарних технологій робить цю програму дуже корисною для освіти. Веб-сервіс пропонує безліч освітніх ресурсів і надає можливість виконання дослідження з проектування мікропроцесорних систем.

Список літератури:

[1] *Совин Я.Р.,* Наконечний Ю.М., Опірський І.Р., Стахів М.Ю. Аналіз апаратної підтримки криптографії у пристроях Інтернету речей. Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 1, p. 36-48.

[2] *Алехин В.А.* Развитие учебного комплекса по электротехнике, электронике и микроконтроллерам с моделированием в программной среде TINA. Открытое образование. 2017. №6. С. 57–69.

[3] *Алехин В.А.* Электротехника и электроника. Учебные ресурсы для студентов и преподавателей. URL: http://www.toe-mirea.ru/ (дата звернення 02.02.2020).

[4] *Березняков С.В.,* Греков А.В. Моделирование микроконтроллера 80С51 в системе схемотехнического моделирования Proteus VSM. Электротехника, информационные технологии, системы управления. 2016. № 17. С. 104-120.

[5] *Матвеенко И.П.* Компьютерное моделирование электронных схем на базе микроконтроллеров AVR. Науковий вісник Національного університету біоресурсів і природокористування України. Серія : Техніка та енергетика АПК. 2014. Вип. 194(2). С. 39-46.

[6] *Филатов М.* Работа с микроконтроллерами AVR в программной среде Proteus 8.1. Компоненты и технологи. 2015. №12(173). С. 103–112.

[7] *Макаренко В.,* Бабко А. Моделирование работы микроконтроллеров в программе NI Multisim. Электронные компоненты и системы. 2012. №4. С. 38-43.

[8] *Найденко Е. В.* Применение программной среды Ni Multisim при изучении дисциплины «Микропроцессорная техника». Електротехнічні та комп'ютерні системи. 2017. № 25. С. 465–469.

[9] *Колесникова Т.* Программирование микроконтроллеров в программной среде NI Circuit Design Suite — Multisim 12.0. Компоненты и технологи. 2014. № 6 (155). С. 144–148.

[10] *Ляшенко О,* Журіло О. Моделювання можливих загроз інформаційної безпеки в системах з використанням мікроконтролерів AVR. Global Cyber Security Forum : матеріали першого міжнародного науково-практичного форуму, 14–16 листопада 2019 р. Харків: ХНУРЭ, 2019. С. 68–69.

[11] *Квашнін В. О.,* Бабаш А. В., Квашнін В. В. Програмування та застосування мікроконтролерів STM32F4Discovery: монографія. Краматорськ: ЦТРІ «Друкарський дім», 2017. 143 с.

[12] TinaCloud. URL: http://www.tinacloud.com (дата звернення 02.02.2020).

Надійшла до редколегії 26.05.2020