УДК 004.056.7

В. І. Маліновський
Л.М. Куперштейн
Л.О. Майданевич

ПІДХОДИ ДО СТВОРЕННЯ МЕТОДУ КІБЕРЗАХИСТУ СИСТЕМ ТА СХЕМ НА БАЗІ МІКРОКОНТРОЛЕРІВ

Вінницький національний технічний університет

Анотація.
Розглянуто основні тенденції і підходи до розвитку методу і технік кіберзахисту мікроконтролерів від різних кібератак та інформаційних впливів. Відзначено актуальність кіберзахисту схем на базі мікроконтролерів у сучасному світі та проблематику їх кібербезпеки. Описані універсальні підходи кібербезпеки МК для захисту інформації в архітектурі мікроконтролерів та МК систем.
Ключові слова: мікроконтролрер (МК), IoT, побічні канали, кібератака, кіберзахист МК, шифрування, інформаційний та кіберзахист, вразливості.

Abstract.
The main trends and approaches to the development of the method of cyber-protection of microcontrollers from various cyber-attacks and information influences are considered. The relevance of cyber-protection of microcontroller-based circuits in the modern world and the issues of their cybersecurity are noted. Approaches to a universal cybersecurity method and model and information protection in the architecture of MC are described.
Keywords: microcontroller (MC), IoT, side channels, cyberattack, MC cyberdefense, encryption, information and cyberdefense, vulnerabilities.

Вступ

Останнім часом поряд із розвитком інформаційних технологій значно розвиваються технології мікроконтролерів (МК) [1, 2]. Сучасні технології інформаційних систем на базі МК набули широкого розвитку у пристроях, мережах та системах Інтернету речей (IoT). Однак, як зазначено у роботах [1, 2] дуже гостро стоїть проблема кібербезпеки МК систем і схем, яка ще не вирішена до кінця в силу ряду причин:

- складності і “жорсткості” архітектури та апаратної будови мікропроцесорів;
- складності та відсутності гнучкості зв’язків та неможливості оновлення в МК;
- складності контролю взаємозв’язків та внутрішніх інформаційних впливів на МК;
- складністю і важкістю контролю внутрішніх інформаційних комунікацій і даних в МК .

Тому, вирішення проблеми кібератак та зовнішніх інформаційних втручань по первинним і вторинним (стороннім) каналам в МК [1-2] вимагає нових підходів і залишається актуальним у МК системах із зовнішніми інтерфейсами, зв'язками і каналами зв’язку.

Метою роботи є покращення рівня кіберзахисту мікроконтролерів та їх схем. Розробка ефективних підходів кіберзахисту МК на нових принципах дозволить враховувати й компенсувати сумарні і поодинокі інформаційний впливи та кібератаки, та в оптимістичних прогнозах забезпечити повну нейтралізацію основних кіберзагроз в мікропроцесорних системах в складі як спеціалізованих і загальних систем управління.

Проблема кібербезпеки мікроконтролерів

Оцінка кіберзагроз і впливів по основним та вторинним каналам в МК розглянуті в роботах [1], дали можливість зрозуміти на рівні розробки математичної моделі оцінки факторів впливу на інформаційні процеси в МК. Основні кібер втручання та інформаційні впливи здійснюються саме по інформаційним каналам та зовнішнім інтерфейсам МК (близько 80-85% серед всіх інцидентів) інша частина по вторинним побічним каналам (близько 15-18%), в т.ч. і по каналам енергетичного

живлення; невелике число інцидентів (близько 1-2%) відбувається по незалежним непрямим каналам або із використанням інших чинників.

Для захисту МК на якісному рівні в сучасному середовищі та кіберпросторі, враховуючи широкий ландшафт кіберзагроз і поверхню кібератак, дуже складно і часто практично неможливо вирішити проблему кіберзахисту без нового релізу і апаратного перевипуску (нового виготовлення) нової архітектури МК із оптимізованою та закритою вразливістю CWE апаратного рівня. Основна проблема кібербезпеки МК полягає у складності і жорсткості архітектури і апаратної будови МК, неможливістю усунення основних вразливостей. З погляду і точки зору програміста, сам МК і його системна мікропрограма представляється для розробника набором регістрів та їх полів і супутніх змінних, в які записуються і читаються значення на кожному етапі роботи алгоритму і самої мікропрограми. Таке представлення не дозволяє точно і ефективно, а головне – повно охопити і розглянути МК, адже виникають і існують “сліпі зони” безпеки і апаратні вразливості, які неможливо виправити (“запатчити“) шляхом оновлення коду мікропрограми. Є основні характерні вразливості CWE для МК(наприклад, такі як RowHammer Rowmaster, Meltdown та Spectre, описані в [1-2]), які пов’язані із кібератаками на пам’ять МК та черговість і сам механізм порядку виконання машинних інструкцій в МК, і які є критичними.

Підходи до розробка методу кіберзахисту

Одним із супутніх завдань кіберзахисту – є актуальні і точні оцінки впливу кіберзагроз у МК [1], а також оцінки наслідків від їх впровадження в МК і супутні системи контролю. Для розробки підходів і методу кіберзахисту потрібно враховувати специфіку побудови конкретного МК, різність архітектур і різність та анізотропію модулів в складі системи мікроконтролері. Також слід враховувати специфіку побудови інтерфейсів та регістрів моніторингу та керування периферією МК.

Для нейтралізації і виявлення кіберзагроз можна використати прогресивні практики:

– проведення аналізу процесів і службових даних функціонування МК;

– інтерактивна нейтралізація кіберзагроз і шкідливих впливів, комплексного захисту МК ;

– ізоляція області роботи МК і окремих модулів мікропрограми МК (прошивки);

– підходи моніторингу і використання криптостійких та надійних алгоритмів ;

Ефективність цих підходів кіберзахисту ІС МК і досить часто і витрати на їх реалізацію не у повній мірі дозволяють отримати необхідний рівень безпеки інформаційної системи МК .

Співвідношення вартості до технічного функціонального рівня захисту МК систем, не завжди відповідають необхідному і достатньому рівню, особливо враховуючи сучасні загрози «0»-го дня і рівень сучасного шпигунського і хакерського програмного забезпечення для МК і систем управління на їх основі [2]. Відтак, локальний захист не вирішує завдання повного комплексного захисту усієї системи мікроконтролера. Завдання розробки підходів кіберзахисту МК і оцінці та врахування впливу повинно базуватись на: 1) аналізі самих кіберзагроз в МК; 2) оцінці їх окремих впливів; 3) оцінці комплексного впливу багатьох факторів; 4) точному визначенню основних і супутніх факторів впливу кіберзагроз; 5) оцінці вектору атаки і профілю захищеності МК – системи; 6) аналізі самих типів і факторів кіберзагроз . Для протидії інформаційним впливам в МК повинні застосовуватись принципи:

- індикації та визначення кіберзагрози із інтерактивним блокуванням трафіку від джерела;
- принцип ізоляції і використання захисного периметра оточення МК;
- принципи відновлення попередніх станів МК із нормальними параметрами;
- принцип визначення та організації фіксації параметрів кіберзагрози;
- принципу обфускації окремих показників та інформаційних параметрів системи (наприклад, ID MCU/MK, адрес інтерфейсів МК, адрес протоколів, тощо);
- принцип адаптивності архітектури захисту; принцип адаптивності захисту;

- принцип імплементації та включення в роботу різних по своїй суті схем в МК;

- принцип гнучкості функціоналу МК, відновлення попередніх станів МК;

Отже принципи кіберзахисту і блокування інформаційних втручань в МК, як по основним, так і по побічним каналам, має комплексний характер і використовуватиме паралельно різні підходи і принципи. Якщо спрощено зобразити основний підхід кіберзахисту, то можна показати це у вигляді структури універсального захисного периметру МК (рис. 1).

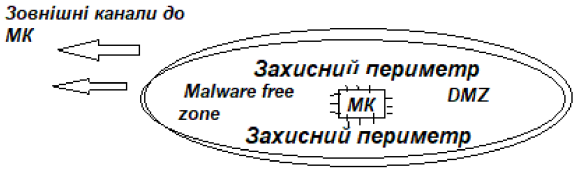

Рисунок 1. Ілюстрація узагальненого принципу побудови методу кіберзахисту МК, який покладений в основу методу комплексного кіберзахисту мікроконтролера

Узагальнений принцип ізоляції периметру МК (рис. 1) по наявним каналам та інтерфейсам зв'язку МК – як потенційним джерелом надходження кіберзагроз та інформаційних втручань в роботу МК. Принцип (рис.1) є узагальненим і полягає в створення захисного і контрольованого параметру зони захисту із МК в основі. Сам зоновий захисний периметр (із контролем даних на межі) не обмежується тільки зовнішнім захистом МК, але й може "огортати" і покривати окремі критичні зони і периферію в середині самого МК.

Висновки

Реалізація кіберзахисту МК на практиці – не проста задача і те, що легко аналізується теоретично, на практиці має зовсім інші рівні складності впровадження. На практиці досягнення дієвого, ефективного та релевантного кіберзахисту досить складно реалізувати, враховуючи ландшафт та різноманітність каналів втручань і векторів атак від сучасних кіберзагроз. Описані підходи до універсального методу і моделі кібербезпеки МК та захисту інформації в архітектурі мікропроцесорів. Розглянути окремі підходи підвищення захищеності інформації в мікропроцесорних пристроях і схемах на їх базі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Маліновський В. І. Аналіз загроз безпеки мікроконтролерів [Текст] / В. І. Маліновський , Л. М. Куперштейн // Інформаційні технології та комп'ютерна інженерія. - 2022. - № 3 [10] .- С. 21-32.

2. Шологон Ю. З. Вразливості апаратного забезпечення кіберфізичних систем./ Репозитарій Національного університету «Львівська політехніка» (Lviv Polytechnic National University Institutional Repository). - t12. c. - 2023. [Електронний ресурс]. - Режим доступу URL: http://ena.lp.edu.u. (Дата звернення 24.02.2024).

Маліновський Вадим Ігоревич — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, Україна.

Куперштейн Леонід Михайлович— канд. техн. наук, доцент, доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, Україна.

Майданевич Леонід Олександрович – канд. філос. наук, старший викладач кафедри захисту інформації Вінницького національного технічного університету, Вінниця, Україна.

Malinovskyi Vadym — PhD, associate professor, Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, Ukraine.

Kupershtein Leonid — PhD, associate professor, Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, Ukraine.

Maidanevych Leonid – PhD, Senior Lecturer, Department of Information Security, Vinnytsia National Technical University, Vinnytsia, Ukraine.