УДК 004.056

В. І. Маліновський, Л. М. Куперштейн

АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ МІКРОКОНТРОЛЕРІВ

Вінницький національний технічний університет, Вінниця

Анотація. В статті розглянуто і приведено матеріали окремих досліджень щодо основних проблем безпеки у мікроконтролерах, які функціонують в складі систем управління як загальних, так і спеціалізованих пристроїв. Зокрема в матеріалах досліджень проаналізовані основні тенденції розвитку загроз безпеки і наведено основні вектори атак. Проаналізовано закордонний та вітчизняний досвід прояву несанкціонованих впливів та кіберзагроз в основні найбільш критичні місця архітектури мікроконтролерів. Аналіз показав, що базовими точками прояву загроз безпеки втручань в роботу мікроконтролера є: регістри, стек, АЛП, пам'ять (EEPROM та Flash), порти введення-виведення, схеми та інтерфейси передачі даних в МК, схеми додаткового функціоналу підключення до зовнішніх периферійних пристроїв і канали підключення осцилятора тактової частоти. Крім того, проведено дослідження основних загроз пам'яті мікроконтролерної системи, а саме: втручання із прямим доступом до пам'яті, доступ до регістрів керування і доступ до буфера мікроконтролера, переповнення стеку буфера, віддалений запуск коду, зовнішній доступ та атаки по вторинним каналам (в т.ч. по зовнішнім лініям передачі даних у МК), зміна порядку адресації в МК, зміна/підміна значень адрес і нумерації стеку, втручання в роботу регістрів даних та індикації стану портів введення/виведення мікроконтролера. Також досліджено ряд механізмів захисту мікроконтролерів, які у комплексі дозволяють знизити ризики несанкціонованих впливів на мікроконтролерну систему. До них відносяться такі: циклічний контроль надмірності коду, моніторинг живлення і моніторинг ресурсів, використання ізольованості і контролю функціональності системи тактування, контроль цілісності та достовірності вмісту пам'яті, контроль зовнішніх фізичних і електричних параметрів МК, віртуалізація основного обчислювального процесу та його багаторівневе резервування копіюванням і відновленням попередніх станів, Використання криптографічних систем і алгоритмів обробки даних, використання багаторівневої програмно-апаратної ізоляції.

Ключові слова: кіберзахист, кіберзагроза, інформаційна безпека, вразливість, мікроконтролер.

Abstract. In the article the materials of individual studies of the main security problems in microcontrollers operating as part of control systems of both general and specialized devices were considered and analyzed. In particular, the main trends of security threats were analyzed and the main attacks vectors were presented. Foreign and domestic experience of manifestation of unauthorized influences and cyber threats in the main most critical places of microcontroller architecture is analyzed. The analysis showed that the basic places of security threats and interventions to the microcontroller are: registers, stack, LPA, memory (EEPROM and Flash), input-output ports, circuits and interfaces for data transfer to the MC, circuits for additional functionality for connecting to external peripheral devices and channels for connecting the clock oscillator. In addition, explorations were carried out on the main threats of the microcontroller system memory, namely: interference with direct memory access, access to control registers and access to the microcontroller buffer, buffer stack overflow, remote code execution, external access and attacks on secondary channels (including via external data lines in the MC), changing the order of addressing in the MC, changing / replacing the values of addresses and stack numbering, interfering with the work of data registers and indicating the state of the input / output ports of the microcontroller. A number of protection mechanisms for microcontrollers have also been studied, which together can reduce the risks of unauthorized actions on the microcontroller system. These include: cyclic code redundancy control, power monitoring and resource monitoring, the using of isolation and control of the functionality of the clock system, control of the integrity and reliability of the memory contents, control of external physical and electrical parameters of the microcontroller, virtualization of the main computing process and its multi-level redundancy and restoration of previous states, the using of cryptographic systems and data processing algorithms, the using of multi-level software and hardware isolation.

Key words: cyber protection, cyber threat, information security, vulnerability, microcontroller.
DOI: https://doi.org/10.31649/1999-9941-2022-55-3-21-32.

Вступ

Сучасні технології інформаційних систем на базі мікроконтролерів та мереж досить активно набувають динамічного стрімкого розвитку в останні роки і впроваджуються у все ширші сфери людської діяльності. Останні роки розвитку цифрових та інформаційних технологій набув особливо великих темпів: від впровадження в традиційні сфери автоматизації і цифрових технологій систем загального призначення до розвитку прогресивних спеціалізованих систем із мікроконтролерними архітектурами та штучним інтелектом, систем робототехніки і автоматики у вигляді конкретних науково-промислових вітчизняних та закордонних розробок.

Разом із тим набуває розвитку і швидких темпів ескалація сучасних кібератак у різних галузях [1-4], зокрема і на галузь цифрових інформаційних технологій мікроконтролерних систем. Кількість кібератак пропорційно збільшується із ростом цифрових технологій, на що вказує закордонний та вітчизняний досвід [3-20]. Для нейтралізації і вчасного попередження, проведення аналізу процесів функціонування мікроконтролерів (МК) і нейтралізації цих загроз використовується різні методи [3, 4, 5, 8, 11], зокрема й в більшості комплексні системи інформаційного захисту – ізоляція області роботи МК, підходи моніторингу, криптостійкі надійні алгоритми, антивірусні платформи і мережеві системи аналізу трафіку [4, 5, 21-23]. Ефективність цих методів, підходів і систем та досить часто й затрати на їх реалізацію не у повній мірі дозволяють отримати необхідний рівень безпеки враховуючи сучасні загрози «0»-го дня і рівень сучасного шпигунського і хакерського програмного забезпечення для МК і систем управління на їх основі [8, 10-16].

Метою статті є проведення аналізу сучасних та найбільш актуальних загроз безпеці мікроконтролерів в результаті їх функціонування в складі як спеціалізованих так і загальних систем управління для більш повного та цілісного розуміння можливих недоліків у їх захисті та подальшої оцінки ризиків їх використання.

Проблема інформаційної безпеки сучасних МК систем і потенційні шляхи її вирішення

Досить часто виникають задачі локального захисту даних і забезпечення безпеки мікроконтролерів на локальному рівні, наприклад в кінцевих пристроях чи сенсорах Інтернету речей (IoT) [6]. Такі кінцеві пристрої або датчики (сенсори) являють собою кінцеві інформаційні вузли із МК і з досить складною архітектурою та програмно-апаратною основою (досить часто являють собою окремий WEB-сервер) із підключенням по каналам із різними мережевими протоколами до центральних системи управління. Для задач захисту таких застосунків в локальних місцях неможливо та/або не ефективно використовувати складну і досить вартісну окрему інфраструктуру із комплексним антивірусним захистом або комплексну систему захисту інформації (програмно-апаратну платформу, або суто програмну антивірусну платформу), так як локальне розміщення і технічний рівень кінцевої локальної точки інформаційного пристрою не є повноцінною обчислювальною системою [7].

Середовище кіберзагроз МК продовжує зростати, оскільки додається все більше варіацій застосувань взаємопов'язаних МК пристроїв. Екосистема мікропроцесорних пристроїв, мікроконтролерів і в т.ч. пристроїв Інтернету речей на базі МК в сучасному світі збільшується із збільшенням кількісті елементів, взаємозв'язків та обсягів даних. Те, як сучасні компанії, які експлуатують МК пристрої, справляються із більшістю відомих інформаційних ризиків і загроз, часто залежить від стратегічного підходу до створення попереджувального плану інформаційних втручань і кібератак на пристрої із МК, замість того, щоб розраховувати на відповідну швидку реакцію до та після інциденту, в мінімально можливий час. Уникнути «сліпих зон» безпеки при збереженні пильності в інформаційній системі — завдання, яке здатні оцінити більшість організацій. Для прикладу сучасні засоби інформаційних втручань в промислові МК пристрої дозволяють успішно реалізовувати шкідливий функціонал і втручання в процеси МК шкідливим ПЗ [5], наприклад: Stuxnet, Flame, miniFlame, Duqu, Gauss, Reign, Wiper, Shamoon, яке експлуатує вразливості програмного коду МК систем і систем індустріального контролю в складі АСУ ТП на базі мікроконтролерів. Це дозволяє впроваджувати шкідливий код і здійснювати інформаційні втручання із порушенням штатного функціоналу МК засобів і їх функціонування вцілому. За даним компанії Cisco Systems Inc. [8], яка є лідером галузі телекомунікацій і займає передові позиції в галузі кібербезпеки інформаційних систем – розвиток засобів для здійснення інформаційних втручань і атак, а також їх функціоналу і широти сфери застосувань значно перевищує рівні розробки сучасних засобів виявлення, попередження і захисту (IPS/IDS/SecD). І особливо це стосується загрозу у формі шкідливого ПЗ і спеціалізованого вузько орієнтованого шкідливого ПЗ для МК систем, яке експлуатує вразливості Meltdown та Spectre [9-13].

Важливою є проблема, що полягає у збільшенні ескалації загроз та збільшенні збоїв у появі невизначених помилок при виконанні операцій ділення чисел з плаваючою комою, причиною яких була відсутність декількох входжень в таблицю пошуку, використовувану для прискорення обчислень [3, 4]. Цей недолік, хоч і проявлявся рідко і не на всіх вхідних даних в МК, отримав широкий розголос і привів до відкликання окремих лінійок мікроконтролері і обладнання, в якому вони використовувались. Це звісно призвело до великих втрат для компаній і корпорації виробників.

Також, експертами в галузі кібербезпеки виявлено атаку, що дозволяє непомітно модифікувати пам'ять в середовищах віртуалізації ресурсів мікропроцесорів і мікроконтролерів високої продуктивності [10]. Сучасні кіберзагрози і інформаційні ризики від діяльності кваліфікованих хакерів із спеціалізованим ПЗ досить значні. Останні дослідження показують можливість зламу ключів захищених віртуальних середовищ і середовищ віртуалізації МК із непомітним встановленням шкідливого ПЗ (шкідливі програмні модулі) [8-13,15-18]. Так, група дослідників з Амстердамського технічного університету виявили нову атаку, що дозволяє модифікувати пам'ять віртуальної машини [15, 16]. Вчені представили докладний опис атаки, що отримала назву Flip Feng Shui (дослівно можна перекласти як «перевернутий феншуй»), згідного якого хакери можуть зламати ключі захищених віртуальних машин і області захищеної пам'яті в МК системах або непомітно встановити шкідливе ПЗ на МК системи. Суть атаки полягає у тому, що спочатку зловмисники отримують доступ до пам'яті і до її віртуального середовища в МК. Потім записується копія сторінки пам'яті, яка за службовими даними вже існує у вразливій області пам'яті. З метою економії місця ідентичні сторінки об'єднуються і записуються в одну і будуть збережені в одному і тому ж місці пам'яті на фізичній машині, забезпечуючи хакерам можливість вносити зміни в основну пам'ять обчислювальної системи. Атака можлива завдяки вразливості Rowhammer [16 - 18], що дозволяє здійснювати маніпуляції з бітами (bit-flipping) і змінювати вразливі комірки пам'яті в МК системі. Даний тип атак стосується більше високорозрядних МК систем (із 32- та 64-розрядністю). Атаки були продемонстровані на операційних системах Debian і Ubuntu для процесорів і зовнішньої пам'яті у високорозрядних МК системах. В ході першої з них їм вдалося підключитися до віртуальної машини через скомпрометовану SSH-сесію (дослідники змінили один біт відкритого RSA-ключа жертви [15-16]). У другому випадку за допомогою модифікованого URL і програми apt-get дослідники встановили шкідливий програмний пакет.

Для вирішення таких проблем безпеки потрібна розробка окремих алгоритмічних і організаційних підходів або невеликих програмно-апаратних систем безпеки для МК (пристроїв або засобів мікропроцесорного захисту), які дозволять захистити інформаційні процеси в МК, в кінцевих точках введення/виведення даних в МК, які можуть забезпечити ефективний, недорогий і дієвий локальний захист від більшої частини кіберзагроз.

Розробка і впровадження таких локальних підходів і способів або кінцевих пристроїв «обв'язки» (зовнішньої периферії МК) є актуально і перспективною задачею для забезпечення локального захисту даних кінцевих інформаційних точок і алгоритмічних процесів обробки даних в МК, що в кінцевому варіанті дозволить підвищити надійність і стабільність їх функціонування.

За функціональним призначенням такі пристрої та/або заходи повинні реалізовувати наступні функції:

– швидкий аналіз і виявлення інформаційних загроз в локальному середовищі оточення МК та/або в зовнішньому пристрої/сенсорі, до якого він підключається ;

– поведінковий аналіз трафіку і інформаційних процесів і функціонального стану локального зовнішнього пристрою/датчика кінцевої інформаційної точки;

– виявлення «інформаційних аномалій» - нехарактерних станів і аномальної поведінки роботи мікропроцесорного пристрою і зовнішнього середовища навколо нього;

– виявлення втручань та неідентифікованих підключень та/або вторгнень в систему і канали зв'язку;

– наявність надійних і стійких функціональних алгоритмів мікропрограм функцій і програмного коду функцій і процедур, у тому числі в аспекті криптографії;

– оперативне інформування центрального пристрою/центральну систему безпеки про внутрішньо загрозу або потенційну загрозу або спроби/намагання вторгнення до системи;

– «прозорість» для інформаційного трафіку і непомітність за фізичними і інформаційними характеристиками;

– швидка і ефективна обробка в режимі реального часу, або режимі, наближеному до реального часу, для оперативного опрацьовування співмірному за швидкістю основного трафіку від кінцевої інформаційної точки;

– оперативне знешкодження або мінімізація ризиків від кіберзагроз та забезпечення захисту локальної кінцевої точки від вторгнень або помилок у роботі.

Необхідність швидкої обробки даних від локальної кінцевої точки і моніторингу процесів із попередньою адаптацією до актуального стану в часі є запорукою впровадження системи на базі мікропроцесорних засобів захисту із власною функціональною малою (орієнтованою на МК) програмно-апаратною архітектурою захисту, що орієнтована на конкретні локальні задачі і процеси Розробка і впровадження інноваційних перспективних засобів мікропроцесорного захисту для мінімізації та ліквідації інформаційних загроз в кінцевих локальних точках і пристроях, які б могли працювати автономно і відокремлено від основної системи, де розгорнута комплексна система захисту дозволило б побудувати ефективну і більш захищену інформаційну інфраструктуру сучасних систем обробки і передачі даних. Такі підходи і методи автономного локального захисту відрізняються відносно невеликою вартістю, орієнтовані під конкретні локальні задачі дозволяють підвищувати захист даних у кінцевих точках і можуть стати частиною комплексної стратегії захисту даних на інформаційних об'єктах.

Сучасні загрози безпеки у мікроконтролерах

Основними загрозами в сучасних архітектурах мікроконтролерів є [5, 7, 9-22]:

– прямий і опосередкований доступ до пам'яті, доступ до регістрів, буфера ОЗП, тощо;

– переповнення /буфера, зчитування буфера при несанкціонованому доступі до нього;

– віддалене виконання коду, та/або зовнішній доступ до ліній передачі даних у МК, зчитування із зовнішніх ліній передачі даних в МК ;

– зміна порядку адресації в МК, зміна/підміна значень адрес;

– окремі вразливості ядра та інших компонент, вразливості архітектури, вразливості і вплив на процеси роботи арифметико-логічного пристрою (АЛП) мікроконтролера (в т.ч. і мікропроцесора);

– доступ до ресурсів МК та до окремих регістрів (в т.ч. конфігураційних із зовні), пряму втручання/пересилка команд керування і передачі даних;

– переповнення стеку адрес, переповнення пам'яті, пряма зчитування значень стека, злам та несанкціоноване втручання в ядро системи;

– несанкціоноване втручання і зчитування і надсилання команд і даних із ліній портів мікроконтролера;

– втручання у роботу спеціальних регістрів даних та індикації стану портів введення/виведення МК;

– зміна слідування порядку команд управління та/або перехоплення їх і потоків даних як у ядрі та/або області ядра мікропроцесорної системи, так і у зовнішній периферії;

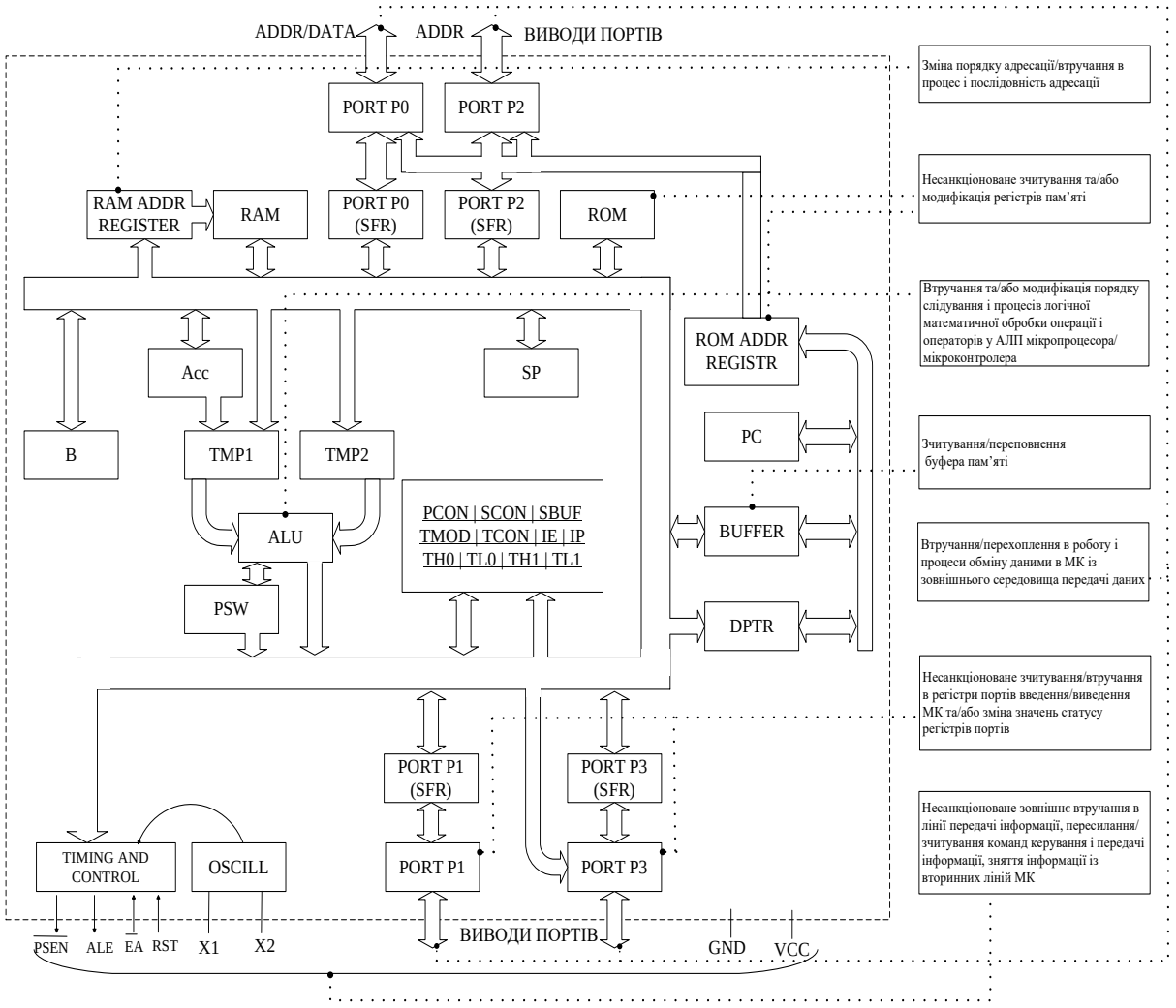
– несанкціоноване зовнішнє втручання в роботу ліній передачі даних та/або вторинних ліній – зовнішніх ліній передачі інформації і інтерфейсів в мікроконтролері. Сюди також можна віднести несанкціоноване (стороннє) пересилання/ зчитування команд керування МК, зчитування інформаційних потоків та/або окремих послідовностей блоків даних прийому/передачі даних до/від МК;

– загрози і атаки, що полягають у блокуванні обчислювального процесу за сторонніми зовнішніми вхідним і вихідним каналами в т.ч. із втручанням по вторинним функціональним каналам, і такими як енергоживлення;

– загрози «нульового дня» і загрози запуску шкідливого коду шляхом впровадження в основну підпрограму (в т.ч. загрози запуску «сліпих/порожніх» циклів в підпрограмі, зміна і переповнення пам’яті МК шліхом запуску ресурсоємкого програмного коду тощо);

– інші потенційні загрози фізичного і прямого електромагнітного впливу на мікропроцесорну систему.

Місця основних загроз в архітектурі мікроконтролера наведено на рисунку1.



Рисиунок 1 –Місця основних загроз в архітектурі мікроконтролера

Прояв основних загроз в архітектурі МК зумовлений недосконалістю окремих блоків, вузлів і зв’язків, а також наявністю вразливостей і незахищених місць і точок впровадження впливу та інформаційних втручань. До самих основних і небезпечних інформаційних загроз, та самих інтенсивних по характеру прояву в МК – є загрози втручання в пам’ять на різних рівнях. Іншим по інтенсивності прояву та характеру впливу є загрози по вторинним (побічним) каналам, які також проявляються.

Основні загрози пам’яті в МК архітектурі наведено на рисунку 2. Загрози пам’яті МК відносяться до основних фундаментальних кіберзагроз в МК і часто накладаються на рівень інформаційних загроз

ядра. Зони зчитування та запису даних при несанкціонованому втручанні і впровадженні стороннього функціоналу по побічним каналам в роботу мікроконтролера показано на рисунку 3.

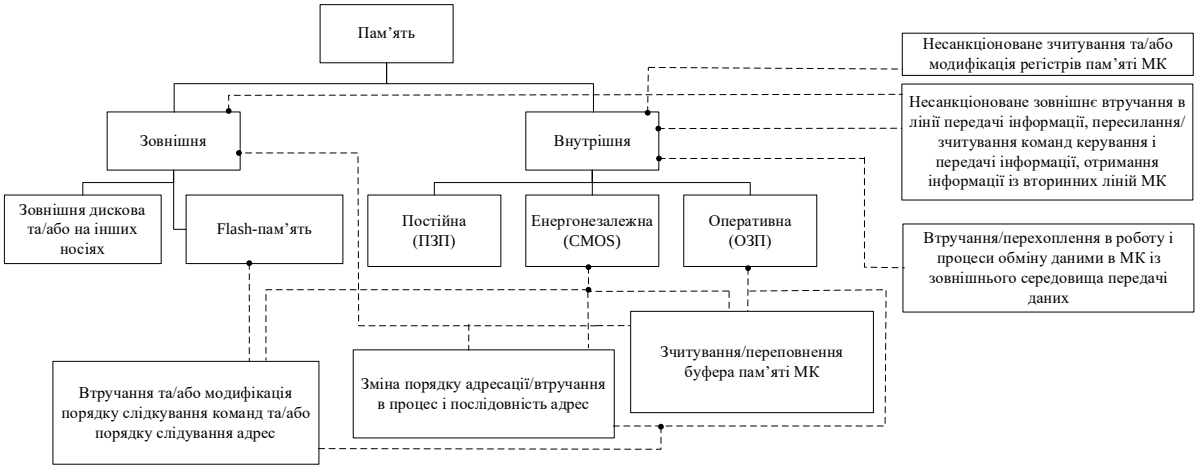


Рисунок 2 − Основні загрози пам'яті мікроконтролерної системи

Загрози пам’яті в МК можуть бути поділені на :

- втручання із прямим доступом до пам’яті (DMA-Direct Memory Acsses);
- доступ до регістрів керування і доступ до буфера мікроконтролера;
- переповнення стеку буфера;
- зчитування буфера пам’яті;
- віддалений запуск коду;
- зовнішній доступ та атаки по вторинним каналам, а також по зовнішнім лініям передачі даних у МК;
- зміна порядку адресації в МК, зміна/підміна значень адрес і нумерації стеку;
- втручання в роботу регістрів даних та індикації стану портів введення/виведення мікроконтролера.

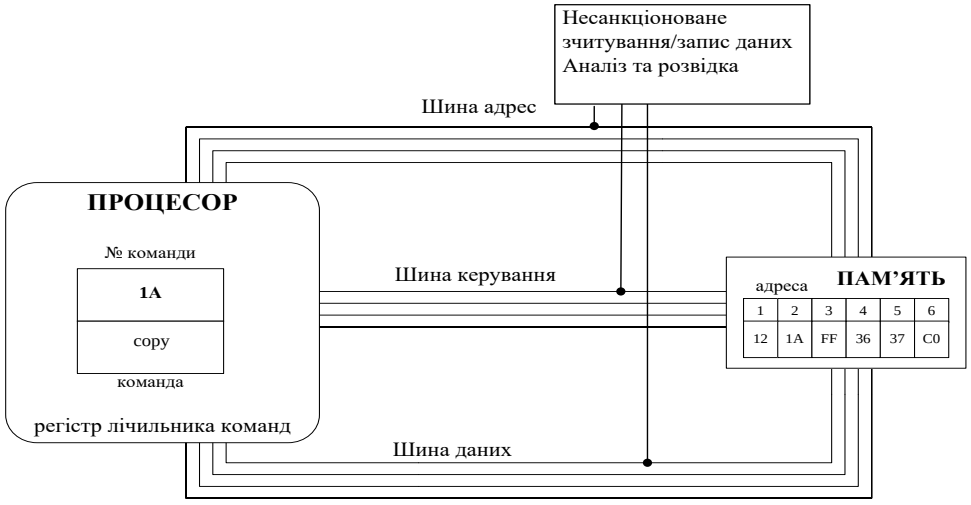


Рисунок 3 – Ілюстрація зон зчитування та запису даних при несанкціонованому втручанні в роботу мікроконтролера

Основними зонами несанкціонованого зчитування даних (рис. 3) є шина даних, шина адрес, шина керування, в яких дані представлені і можуть бути інтерпретовані при зчитуванні. Основний напрямок атак – втручання в шину адрес і шину керування: а) на рівні регістрів управління і регістрів стану; б) на рівні модифікації і з прямим підключенням сигналів до електричних ліній відповідних шин (якщо вони зовнішні і не входять у внутрішню топологію електронної інтегральної схеми МК).

Основні «слабкі» місця в архітектурі мікроконтролера для реалізації кібератак наведено на рисунку 4.

Базовими точками прояву загроз безпеки (рис. 4) і втручань в роботу мікроконтролера є: регістри; стек; АЛП; пам’ять (EEPROM та Flash); порти введення-виведення і схеми та інтерфейси передачі даних в МК; схеми додаткового функціоналу підключення до зовнішніх периферійних пристроїв і канали підключення осцилятора тактової частоти.

Основні тенденції у МК-системах свідчать про підвищення ризиків впровадження кіберзагроз для рівня апаратного функціонування мікроконтролерів. Все більше значення і вагу з точки зору кібербезпеки функціоналу МК і засобів має стабільність та автентичність внутрішніх інформаційних процесів.

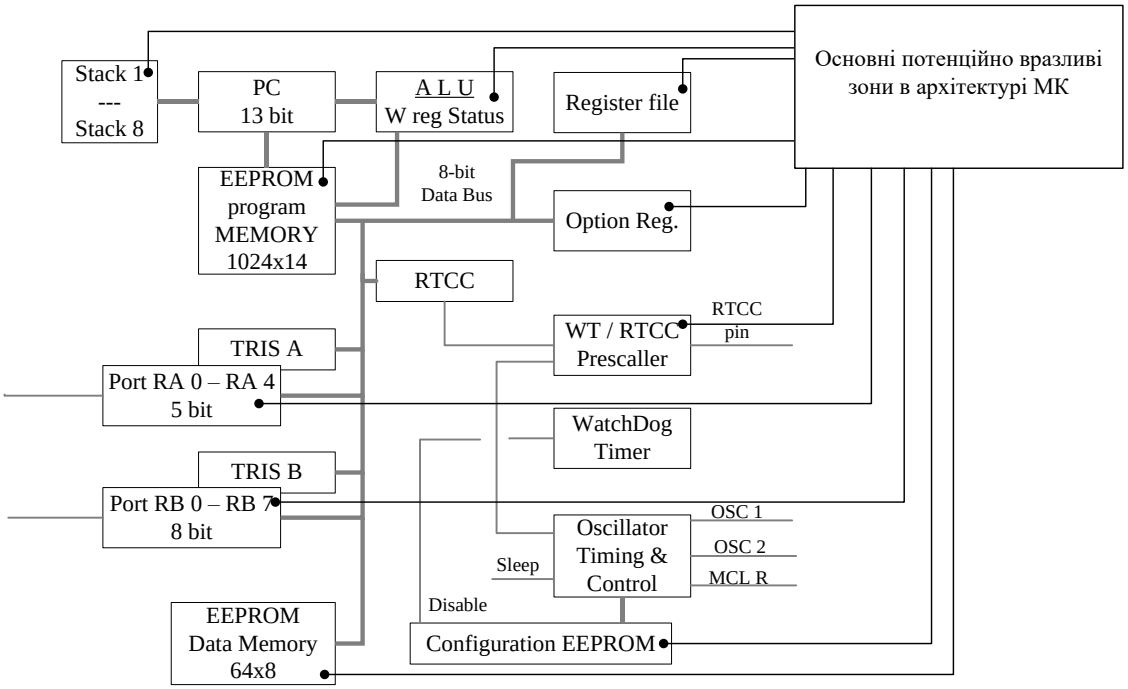


Рисунок 4 – Основні «слабкі» місця в архітектурі мікроконтролера для реалізації кібератак

До основних вразливостей, що проявляються в МК на фізичному рівні можна віднести [4, 9, 13, 14, 16, 17]:

- вразливості через вплив на команди і підміна команд керування;
- зміна порядку слідування команд і зміна технологічного циклу і алгоритму мікропрограми;
- недосконаліть коду програми і потенційно наявні «слабкі» місця в машинному коді ПЗ ;
- вразливості в архітектурі МК, потенційно-небезпечні і можливі комбінації команд МК;
- вразливості пам’яті;
- не захищеність коду у ПЗП та ОЗП, кеш-пам'яті. Також не захищеність трактів АЦП і ЦАП;
- вразливості пов’язані із можливістю прямого читання буфера і його переповнення;
- вразливості ядра і таймерної системи, а також системи переривань мікропроцесора;
- вразливості і генерація замкнутих пустих циклів і циклів переповнення пам’яті МК;
- неправомірне і нелогічне шкідливе використання механізму зовнішніх переривань і механізму апаратного і програмного скидання (функції: «reset»);
- вразливості «0»-го дня – не виявлені сучасні вразливості МК;
- випадкові загрози та/або недосконалості і помилки в програмному коді, наявність «не опрацьованих критичних» та/або проблемних місць в програмному коді;
- недосконаліть і незахищеність архітектури МК.

На рисунку 5 наведено основні канали надходжень кіберзагроз із зовнішнього середовища.

На рисунку 6 наведено фрагмент сучасної електронної схеми із мікроконтролером та позначено найбільш ймовірні місця реалізації кібератак. Електронна схема МК є вразливим місцем в електричній частині і дозволяє при наявності фізичного доступу здійснювати підключення до ліній і портів МК. Основними потенційними кіберзагрозами є атаки зовнішніми каналами:

1) інформаційні втручання із зовнішнього середовища через порти;
2) через інтерфейси МК;
3) через схему і лінії управління;
4) втручання в механізм ланки тактового генератора частот МК.

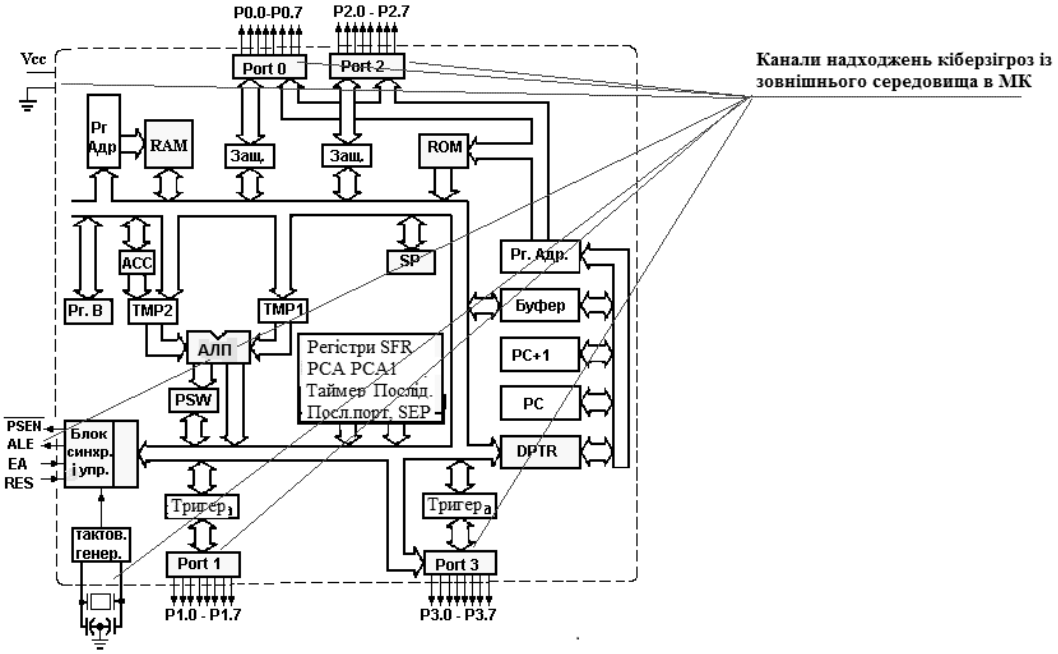


Рисунок 5 – Канали надходжень кіберзагроз із зовнішнього середовища у пам’ять і внутрішню структуру і систему МК (на базі архітектури RISC)

Найбільш високі за інтенсивністю >52% складають загрози типу 1) та 2), близько >25% складають загрози втручання в лінії керування - пункт 3). Втручання і підключення до схеми ланки тактового генератора частот МК як правило не велике >5-8% із врахуванням специфіки втручання в механізм формування тактів МК.

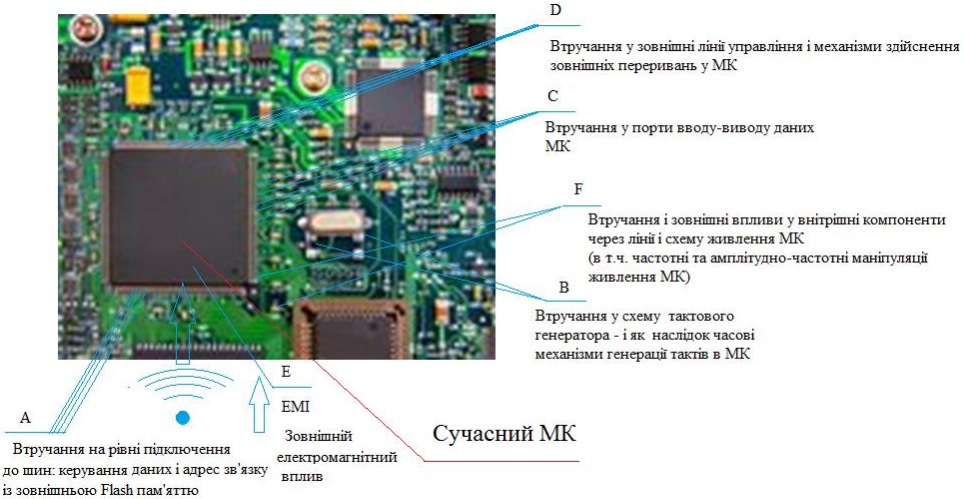


Рисунок 6 – Зовнішній вигляд сучасного МК в складі електронної схеми

Основними і найбільш значимими зовнішніми загрозами і інформаційними втручаннями у МК є (рис. 6) [9-18, 20-21]:

– втручання у зовнішні лінії і механізми переривань МК;
– втручання у порти введення-виведення даних у МК;
– втручання і зовнішні впливи на схему МК через схему живлення (в тому числі різні модуляції живлення);
– втручання у схему тактового генератора МК;
– втручання на рівні підключення до шин передачі даних і керування пам’яттю МК, а також обміну даними із іншими блоками і зовнішньою периферією;
– зовнішній електромагнітний вплив на МК.

Електронна схема і зовнішні електричні підключення МК до сторонніх периферійних пристрої (в т.ч. зовнішньої Flash та/або EEPROM – пам'яті) є вразливим місцем і дозволяє при наявності фізичного доступу і підключення, або шляхом зовнішніх електромагнітних наведень здійснювати втручання та інформаційних вплив на процес оброблення даних в МК та здійснювати різноманітні атаки на нього.

Підходи до забезпечення безпеки процесів передачі і оброблення інформації в мікроконтролерах

Оскільки інформаційні загрози в мікропроцесорних трактах систем в т.ч. і мікропроцесорних пристроях Інтернету речей (IoT) досить часто є складними і мають комплексний характер і етапність проведення, то й рішення, спрямовані на захисти обчислювального процесу і алгоритмів роботи мікропрограм контролера керування також повинні мати комплексний підхід.

Для забезпечення закриття потенційно небезпечних критичних місць архітектури МК використовують одиничні і комплексні підходи для організації необхідного стану захищеності [9, 19-23]:

– Підходи, що ґрунтуються на апаратній основі, в яких використовується циклічний контроль надмірності коду (cyclic redundancy check calculate), тобто обчислюється контрольна сума, яка виявляє помилки при передачі або зберіганні даних. Це не тільки забезпечує перевірку цілісності коду, а й означає, що сигнатура може бути розрахована під час його роботи.

– Моніторинг живлення і моніторинг ресурсів – ще один метод із високим ступенем захисту. Для визначення причини скидання і, таким чином, забезпечення скидання тільки за допомогою автентифікованого доступу до системи управління статусом прапора POR/ PDR / BOR / PVD. Статуси, які забезпечує система: power-on reset – скид при увімкненні; power-down reset – скид при вимкненні; brown-out reset – скид при зниженні напруги живлення; programmable voltage detector - програмований детектор напруги. Для ефективного виявлення маніпуляцій та ведення журналу це доповнюється функцією «Read-While-Write» – читання під час запису, тобто зчитування одного слова під час запису іншого слова).

– Підходи, що передбачають використання ізольованості і контролю функціональності CSS (Clock Security System – «система безпеки тактування») заснована на тому, що якщо при використанні зовнішнього генератора (у мікроконтролерах серії ST32 він позначений як HSE) як джерело сигналу тактової частоти, що забезпечує стабільність роботи системи і гарантованість її «не зависання» в невизначеному стані, а зможе виконати якісь дії, SYSCLK або PLL (система фазового автопідстроювання частоти), відбудеться зрив генерації, то CSS автоматично переключить всю систему працювати від вбудованого RC-генератора (у мікроконтролерах серії ST32 він позначений як HSI). Таким чином, якщо щось трапиться з тактовими сигналами, можна перевести об'єкт управління мікроконтролером в безпечний стан. Крім того, сторожовий таймер (Watchdog) та віконний сторожовий таймер (Window Watchdog) також контролюють часові вікна незалежно один від одного.

– Контроль цілісності та достовірності вмісту пам'яті, що забезпечуються перевіркою та виправленням помилок коду Error Correction Code та перевіркою парності. Тут також забезпечується додатковий захист від атак, спрямованих на недопущення зараження систем помилками коду.

– Контроль зовнішніх фізичних і електричних параметрів МК. Наприклад, датчик температури безперервно вимірює температуру середовища, що оточує мікроконтролер. Це необхідно для того, щоб переконатися, що вона залишається в зазначеному діапазоні, і таким чином уникнути ризику пошкодження при спеціальному тривалому нагріванні.

– Використання сучасних інноваційних підходів до захисту мікропроцесорних систем – використання алгоритмів віртуалізації основного обчислювального процесу та його багаторівневе резервування копіюванням/фіксуванням і відновленням попередніх t_{i-1}, t_{i-2}, ..., t_{i-n} станів обчислювального процесу. У випадку настання кіберзагрози вектор параметрів і стану обчислювального процесу відновлюється із попередніх значень обчислювальних параметрів до моменту настання кібератаки в МК системі. У випадку настання кіберзагрози вектор параметрів і стану обчислювального процесу відновлюється із попередніх значень в часових проміжках t_{i-1}; t_{i-2}; t_{i-m}. t_m тобто:

$$\varphi(t_i, f(x,y,z,t,n,d)t_i) = \varphi'\left(t_i, f(x,y,z,t,n,d,t_i)\right) - \mu\Delta t_{i-1}\left(f\left(t_{i-1}, f(x,y,z,t,n,d,t_{i-1})\right)\right);$$

$$\varphi'\left(t_i, f(x,y,z,t,n,d,t_i)\right) = \sum_{j=0}^{n}\binom{n}{t}\mathrm{F}(\varphi'(t_i, f(x,y,z,t,n,d)t_i) - \mu\Delta t_{i-1}\left(f\left(t_{i-1}, f(dx,dy,dz,dt,dn,dd,t_{i-1})\right)\right)$$

де $\varphi(t_i, f(x,y,z,t,n,d)t_i)$ – поточний вектору функції обчислювального процесу групи параметрів даних події при настанні кіберзагрози; $\varphi'\left(t_i, f(x,y,z,t,n,d,t_i)\right)$ – актуальний параметр реального функції у реальному часі; $\varphi'\left(t_i, f(x,y,z,t,n,d,t_i)\right) - \mu\Delta t_{i-1}\left(f\left(t_{i-1}, f(x,y,z,t,n,d,t_{i-1})\right)\right)$ – функція попереднього стану вектору параметрів обчислювального процесу для групи параметрів даних x,y,z,t,n,d до події на-

стання кіберзагрози та/або кібератаки (вектором стабільних параметрів x, y, z, t, n, d – вважаються параметри, які не піддані кібератаці та/або інформаційному впливу відносно змінених параметрів x', y', z', t', n', d' в результаті інформаційного впливу та/або кібератаки); $f(t_{i-1}, f(x, y, z, t, n, d, t_{i-1}))$ – значення функції різниці зміни параметрів обчислювального процесу на дискретному проміжку часу Δt_{i-1} і коефіцієнта μ відносно попереднього стану із різницею в часі t_{i-1}; t_i – актуальний час ; $f(x, y, z, t, n, d)t_i)$ – значення функції обчислювального процесу в актуальному (реальному, поточному) часі із залежністю параметрів обчислювального процесу x, y, z, t, n, d є Mn, де Mn – поле множини параметрів даних і змінних в обчислювальному процесі. $F(\varphi'(t_i, f(x, y, z, t, n, d)t_i)$ – поточний вектору функції обчислювального процесу групи параметрів даних події при настанні кіберзагрози для окремої групи пристроїв периферії МК і взятої сукупності значень комплексної функції параметрів змінних і констант обчислювального процесу для локальної області пристроїв та/або периферії та або окремої області в МК ; $f(t_{i-1}, f(x, y, z, t, n, \Delta t_{i-1}, t_{i-1}))$ – функція різниці зміни параметрів обчислювального процесу на дискретному проміжку часу Δt_{i-1} відносно попереднього стану за попередній проміжок часу t_{i-1}, взятої для окремої групи пристроїв та/або периферії та або окремої області в МК і взятої сукупності значень комплексної функції обчислювального процесу; n – сукупність пристроїв та/або периферії та або окремої області в МК.

Даний підхід в складі методу реалізується за рахунок відновлення попереднього стану обчислювального процесу , який може бути описаний правою частиною верхнього виразу формули (1), тобто за рахунок відновлення параметрів і значень функції із збережених копій і параметрів функції попередніх значень в пам'яті і за допомогою інших додаткових методів і засобів. Недоліком даного підходу є потреба у значній мірі додаткових ресурсів мікроконтролера і в т.ч. пам'яті для резервування попередніх станів обчислювального процесу.

– Використання криптографічних систем і алгоритмів обробки даних в мікроконтролерних системах із надійним криптографічним захистом. Даний підхід потребує зокрема спеціалізованої архітектури МК із криптографічною периферією (кодер/декодер) і відноситься до числа спеціалізованих надійних МК систем;

– Використання багаторівневої програмно-апаратної ізоляції , до якої відноситься: ізоляція програмного коду і методів доступу до потоків даних і потоків програмного коду команд і даних; фізична ізоляція електричної частини мікропроцесорної системи; інформаційна ізоляція мікропроцесорної системи; електрична ізоляція і в т.ч. електромагнітна ізоляція системи мікроконтролера; фільтрація вторинних шумів до/від МК, електрична ізоляція і фільтрація ліній живлення і ліній передачі даних від/до зовнішніх кіл, такі як датчики та/або кола управління; перевірка і ретельна кореляція програмного коду перед програмуванням/оновленням на предмет виявлення вразливостей в системі мікроконтролера; перевірка та моніторинг стану МК системи; використання шифрування і кодування даних для МК із підвищеним рівнем захисту (використовується в захищених і кіберстійких мікроконтролерних системах).

Для захисту від інформаційних втручань та впливу, кібератак і кіберзагроз в мікроконтролери автоматизованих і автоматичних систем, а також та IoT пристроїв в контексті сучасних підходів Industry X.0 та робототехніки, кіберфізичних систем, все більш актуальними стають комплексні підходи захисту, в т.ч. захист апаратного периметра підключення МК і втручання в роботу мікропрограм і ПЗ. Основні зусилля направляються на захист мікропрограм і пам'яті мікроконтролерів. Але не достатньо зусиль і уваги приділяється захисту інформаційним втручанням по вторинним каналам і лініям зв'язку із МК. Сучасні підходи передбачають визначення і використання захищених зон і периметру МК. Використовуються рішення в галузі автентифікації і криптографічного захисту архітектури МК, використання зон «0»-вої довіри при роботі МК платформи і взаємодії із іншими модулями.

Деякі сімейства мікроконтролерів вже містять багато функцій безпеки, а також функції забезпечення безпеки власного ПЗ. Річ у тім, що мікроконтролери є основними компонентами серед управління в підключених системах. Їхні постачальники вже використовують процеси розробки та сертифікацію за відповідними стандартами безпеки. А постачальники напівпровідників також гарантують, що можуть запропонувати своїм клієнтам комплексне безпечне рішення.

Висновки

Аналіз поширеності мікроконтролерів у сучасному світі довів свою затребуваність і актуальність використання. На сьогодні не можливо уявити роботу електронних пристроїв без мікроконтролерів. Це як і спеціалізовані обчислювальні пристрої, як пристрої загального призначення, в тому ччислі і різноманітні побутові пристрої. Оскільки мікроконтролери обробляють інформацію різного характеру і взаємодіють із різними периферійними пристроями, вони стають жертвами численних різноманітних кібератак через недоліки або помилки допущені при їх розробці. При цьому складність ситуації ще у тому, що виправити виявлені вразливості програмних шляхом не завжди виявляється можливим. У такому випадку

уся серія пристроїв стає непридатною до використання. Аналіз досліджень показав, що основні вразливості МК на фізичному рівні пов'язані із командами керування, мікропрограмою, пам'яттю та системою переривань. Серед атак найбільш розповсюдженими є зовнішні втручання у порти введення-виведення даних, впливи на схему МК через схему живлення, втручання у схему тактового генератора МК, підключення до шин передачі даних і керування пам'яттю МК, зовнішній електромагнітний вплив на МК та ін. Як показало дослідження загрози безпеки мікроконтролерам можуть бути досить критичними і потрібно занадто прискіпливо підходити до процесів їх проектування, тестування та виробництва адже одна вразливість може призвести до компрометації усього пристрою на його основі. При організації захисту доцільно притримуватися комплексного підходу для забезпечення багаторівневого захисту системи.

Список літератури

[1] В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович, *Основи інформаційної безпеки*. Вінниця: ВНТУ, 2013, 221 с.

[2] Концепція технічного захисту інформації в галузі зв'язку України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF#Text. Дата звернення: 15 серпня 2022.

[3] John R. Vacca, *Computer and Information Security Handbook*. Burlington, USA: Morgan Kaufmann Publishers, 2017, 1280 p.

[4] С. Г. Антонов, С. М. Климов, "Методика оценки рисков нарушения устойчивости функционирования программно-аппаратных комплексов в условиях информационно-технических воздействий", *Надежность*, Том 17, №1, С. 32-39. 2017.

[5] Software Security Guidance. [Online]. Available: https://www.intel.com/content/www/us/en/developer/topic-technology/software-security-guidance/overview.html. Accessed on: August 15, 2022.

[6] V. S . Kharchenko, Internet of Things for Industry and Human Application. In Volumes 1-3. Volume 1. Fundamentals and Technologies. Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019, 605p.

[7] V. V. Sklyar, V. V. Yatskiv, N. G. Yatskiv, Dependability and Security Internet of Things: Practicum. Ministry of Education and Science of Ukraine, National Aerospace University "KhAI", Ternopil National Economic University, 2019, 98 p.

[8] Cisco cybersecurity reports. [Online]. Available: https://www.cisco.com/c/en_hk/products/security/security-reports.html. Accessed on: August 15, 2022.

[9] Meltdown and Spectre: Which systems are affected by Meltdown? [Online]. Available: https://meltdownattack.com/#faq-systems-meltdown. Accessed on: August 15, 2022.

[10] The Anatomy of Security Microcontrollers for IoT Applications. [Online]. Available: https://www.digikey.com/en/articles/the-anatomy-of-security-microcontrollers-for-iot-applications. Accessed on: August 15, 2022.

[11] Speculative Processor Vulnerability [Online] Available: https://developer.arm.com/Arm%20Security%20Center/Speculative%20Processor%20Vulnerability. Accessed on: August 15, 2022.

[12] Cache Speculation Side-channels white paper. ARM Developer Forum. Specification. [Online]. Available: https://developer.arm.com/documentation/102816/0205. Accessed on: March 8, 2022.

[13] Kernel Side-Channel Attack using Speculative Store Bypass - CVE-2018-3639. [Online]. Available: https://access.redhat.com/security/vulnerabilities/ssbd. Accessed on: March 8, 2022.

[14] ISO/IEC, «Information technology — Security techniques-Information security risk management» ISO/IEC FIDIS 27005:2008. [Online]. Available: https://www.iso.org/standard/42107.html. Accessed on: August 15, 2022.

[15] Modern security for microcontrollers. [Online]. Available: https://get.meriac.com/docs/eSAME-MicrocontrollerSecurity.pdf. Accessed on: August 15, 2022.

[16] S. Yegulalp. Rowhammer hardware bug threatens to smash notebook security. [Online]. Available: https://www.infoworld.com/article/2894497/rowhammer-hardware-bug-threatens-to-smash-notebook-security.html. Accessed on: August 15, 2022.

[17] K. Bains, J. Halbert, C. Mozak, T. Schoenborn and etc. "Row hammer refresh command", U.S. Patent Appl. 2014/0059287 A1, Feb. 27, 2014. [Online]. Available: https://patents.google.com/patent/US20140059287. Accessed on: August 15, 2022.

[18] Cisco Systems security advisory. Row Hammer Privilege Escalation Vulnerability. [Online]. Available: https://training.ti.com/core-cybersecurity-concepts-and-their-relation-microcontroller-security-hardware Accessed on: August 15, 2022.

[19] Core cybersecurity concepts and their relation to microcontroller security hardware. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20150309-rowhammer.html. Accessed on: August 15, 2022.

[20] S. Govindavajhala, A. W. Appel. "Using Memory Errors to Attack a Virtual Machine". [Online]. Available: https://www.cs.princeton.edu/~appel/papers/memerr.pdf. html. Accessed on: August 15, 2022.
[21] Yuan Xiao, Yinqian Zhang, Radu Teodorescu, Speechminer: a Framework for investigating and measuring speculative execution vulnerabilities. [Online]. Available: https://arxiv.org/pdf/1912.00329.pdf. Accessed on: August 15, 2022.
[22] Introduction to STM32 microcontrollers security. [Online]. Available: https://www.st.com/resource/en/application_note/dm00493651-introduction-to-stm32-microcontrollers-security-stmicroelectronics.pdf. Accessed on: August 15, 2022.

Стаття надійшла: 04.09.2022.

References

[1] V. A. Luzhetskyi, A. D. Kozhukhivskyi, O. P. Voitovych, *Osnovy informatsiinoi bezpeky*. Vinnytsia: VNTU, 2013, 221 p. [in Ukrainian].
[2] Kontseptsiia tekhnichnoho zakhystu informatsii v haluzi zviazku Ukrainy. [Online]. Available: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF#Text. Accessed on: August 15, 2022.
[3] John R. Vacca, *Computer and Information Security Handbook*. Burlington, USA: Morgan Kaufmann Publishers, 2017, 1280 p.
[4] S.H. Antonov, S.M. Klymov, "Metodyka otsenky ryskov narushenyia ustoichyvosty funktsyony-rovanyia prohrammno-apparatnыkh kompleksov v uslovyiakh ynformatsyonno-tekhnycheskykh vozdeistvyi", *Nadezhnost*, Tom 17, №1, 32-39 pp. 2017 [in Russian].
[5] Software Security Guidance. [Online]. Available: https://www.intel.com/content/www/us/en/developer/topic-technology/software-security-guidance/overview.html. Accessed on: August 15, 2022.
[6] V. S . Kharchenko, Internet of Things for Industry and Human Application. In Volumes 1-3. Volume 1. Fundamentals and Technologies. Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019, 605p.
[7] V. V. Sklyar, V. V. Yatskiv, N. G. Yatskiv, Dependability and Security Internet of Things: Practicum. Ministry of Education and Science of Ukraine, National Aerospace University "KhAI", Ternopil National Economic University, 2019, 98 p.
[8] Cisco cybersecurity reports [Online]. Available: https://www.cisco.com/c/en_hk/products/security/security-reports.html. Accessed on: August 15, 2022.
[9] Meltdown and Spectre: Which systems are affected by Meltdown? [Online]. Available: https://meltdownattack.com/#faq-systems-meltdown. Accessed on: August 15, 2022.
[10] The Anatomy of Security Microcontrollers for IoT Applications. [Online]. Available: https://www.digikey.com/en/articles/the-anatomy-of-security-microcontrollers-for-iot-applications. Accessed on: August 15, 2022.
[11] Speculative Processor Vulnerability. [Online] Available: https://developer.arm.com/Arm%20Security%20Center/Speculative%20Processor%20Vulnerability. Accessed on: August 15, 2022.
[12] Cache Speculation Side-channels white paper. ARM Developer Forum. Specification. [Online]. Available: https://developer.arm.com/documentation/102816/0205. Accessed on: March 8, 2022.
[13] Kernel Side-Channel Attack using Speculative Store Bypass - CVE-2018-3639 [Online]. Available: https://access.redhat.com/security/vulnerabilities/ssbd. Accessed on: March 8, 2022.
[14] ISO/IEC, «Information technology − Security techniques-Information security risk management» ISO/IEC FIDIS 27005:2008. [Online]. Available: https://www.iso.org/standard/42107.html. Accessed on: August 15, 2022.
[15] . Modern security for microcontrollers. [Online]. Available: https://get.meriac.com/docs/eSAME-MicrocontrollerSecurity.pdf. Accessed on: August 15, 2022.
[16] S. Yegulalp. Rowhammer hardware bug threatens to smash notebook security. [Online]. Available: https://www.infoworld.com/article/2894497/rowhammer-hardware-bug-threatens-to-smash-notebook-security.html. Accessed on: August 15, 2022.
[17] K. Bains, J. Halbert, C. Mozak, T. Schoenborn and etc., "Row hammer refresh command", U.S. Patent Appl. 2014/0059287 A1, Feb. 27, 2014. [Online]. Available: https://patents.google.com/patent/US 20140059287. Accessed on: August 15, 2022.
[18] Cisco Systems security advisory. Row Hammer Privilege Escalation Vulnerability. [Online]. Available: https://training.ti.com/core-cybersecurity-concepts-and-their-relation-microcontroller-security-hardware Accessed on: August 15, 2022.
[19] Core cybersecurity concepts and their relation to microcontroller security hardware. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20150309-rowhammer.html. Accessed on: August 15, 2022.

[20] S. Govindavajhala, A. W. Appel. "Using Memory Errors to Attack a Virtual Machine". [Online]. Available: https://www.cs.princeton.edu/~appel/papers/memerr.pdf. html. Accessed on: August 15, 2022.
[21] Yuan Xiao, Yinqian Zhang, Radu Teodorescu, Speechminer: a Framework for investigating and measuring speculative execution vulnerabilities. [Online]. Available: https://arxiv.org/pdf/1912.00329.pdf. Accessed on: August 15, 2022.
[22] Introduction to STM32 microcontrollers security. [Online]. Available: https://www.st.com/resource/en/application_note/dm00493651-introduction-to-stm32-microcontrollers-security-stmicroelectronics.pdf. Accessed on: August 15, 2022.

Відомості про авторів

Маліновський Вадим Ігорович – кандидат технічних наук, доцент кафедри захисту інформації.

Куперштейн Леонід Михайлович – кандидат технічних наук, доцент кафедри захисту інформації.

V. I. Malinovskyi, L. M. Kupershtein

SECURITY THREATS ANALYSIS OF MICROCONTROLLERS

Vinnytsia National Technical University, Vinnytsia