УДК 004.056:681.2

В.І. Маліновський, Л.М. Куперштейн, В.В. Лукічов

МАТЕМАТИЧНА МОДЕЛЬ ОЦІНКИ КІБЕРЗАГРОЗ ТА ІНФОРМАЦІЙНИХ ВПЛИВІВ У МІКРОКОНТРОЛЕРАХ

Вінницький національний технічний університет

Анотація. В роботі наведено матеріали окремих досліджень аналізу впливу кіберзагроз на інформаційні процеси в мікроконтролерах (МК). Проведено оптимізацію існуючої математичної моделі кіберзагроз та оцінювання інформаційних впливів, а також виконано оцінку і аналіз основних інформаційних ризиків кіберзагроз у мікроконтролерах, які працюють в складі систем управління різноманітних як загальних, так і спеціалізованих пристроїв. Проведено вдосконалення математичної моделі кіберзагроз для оцінки кіберзагроз у мікроконтролерах із врахуванням факторів самих інформаційних впливів. Визначено основні показники оцінки ризиків кіберзагроз в мікроконтрролерах, які враховуються в математичній моделі кіберзагроз для інформаційної системи мікроконтролерів. Вдосконалена математична модель описує сумарний вплив інформаційних загроз та втручань та основні вектори кібератак у МК. Дана модель також дозволяє оцінювати додаткові шкідливі фактори впливи та інформаційні втручання по вторинним каналам із метою їх врахування та компенсації. Проведене комп'ютерне моделювання показало на практиці результати і характер впливу кіберзагроз на інформаційну безпеку МК. Модель дозволяє визначати та оцінювати вплив домінуючих кіберзагроз на основні аналізу основних ризиків у мікроконтролерах, які працюють в складі складних систем та систем Інтернету речей. В роботі також наведено розвиток основних положень по створенню векторної математичної моделі оцінки загроз та впливів у МК, що може бути використано при формуванні повної векторної моделі та методу оцінки впливів і загроз на стан інформаційної безпеки і стабільності функціонування МК. Це може дати змогу оцінити основні показники стабільності роботи як окремих блоків, так і всієї інформаційної системи мікроконтролера. Модель також може дозволити проводити оцінку усереднених значень впливів інформаційних втручань на стабільність функціонування МК, оцінювати величину усереднених кіберзагроз і вразливостей інформаційної системи мікроконтролера. Запропонована модель призначена і може бути використана при розробці методу підвищення рівня інформаційної захищеності мікроконтролерів та суміжних схем для забезпечення їх більш стабільного і безпечного функціонування.

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

Abstract. The paper is presents the research materials of the analysis cyber threats and their influences on information processes in microcontrollers (MC). The optimization of the existing mathematical model of cyber threats influences(impacts) on the information assessment was carried out. Also was performs of the evaluation and analysis of the main information risks of cyber threats in microcontrollers, which work as part of control and automation systems of various general and specialized devices. The mathematical model of cyber threats has been improved for the more data assessments of cyber threats in microcontrollers systems, taking into account the interference of factors of the informational influences. The main indicators of the risk assessment of cyber threats in microcontrollers are determined, which are taken into account in the mathematical model of cyber threats for the information system of microcontrollers. The improved mathematical model describes the total impact factors of information threats, its influences and the main vectors of cyber attacks in MC. This model also will describes and makes possible to evaluate additional harmful factors, and information influences through secondary channels on the data processes in MC's with the aim of it's compensation compensating. The performed researches by computer simulations and modeling were shown in practice the results and their nature of the cyber threats influences on information security of the MC's. The model allows determine and assess the impact of dominant cyber threats and the main risks in microcontroller information systems, what work as part of complex automation systems or Internet of Things devices. The work also provides the development of the main principles' of the creating a vector mathematical model which will describes and assessings the impacts of the cyber threats on MC's. It's results can be used for the formation of a complete vector mathematical model and method for precision assessing of the cyber threats effects in MC's for it's more information security and stability. This can make it possible to evaluate the main stability indicators of entire information system of the microcontroller. The model can also make possible to estimate the average values of the effects of information influences on the stability of the functioning of the MC. It also can estimate of the averaged value of cyber threats impacts for determine of main vulnerabilities in information system of the microcontroller. The proposed model is designed and can be used for the future further development of a method for increasing of the information security level of microcontrollers and their adjacent circuits for ensure their more stable and safe functioning.

Key words: cyber protection, cyber threat, information security, vulnerability, microcontroller, model.

DOI: https://doi.org/10.31649/1999-9941-2024-59-1-69-82.

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. Новітні технології інформаційних систем на базі мікроконтролерів впроваджені і впроваджуються й досі у вже досить широке поле пристроїв у всіх сферах людської діяльності і продовжують розширюватись і еволюціонувати [1]. Мікроконтролери (МК) все більше входять до складу широкого спектру пристроїв як загального, так і спеціального призначення і посідають центральне місце в основних ланках систем управління, автоматики і робототехніки та забезпечують керування сучасними цифровими пристроями [1, 2]. МК керуються і програмуються із використанням сучасних середовищ розробки функціональних мікропрограм на базі гнучких алгоритмів у системних мовах програмування С, С++, Assembler, що дозволяє будувати достатньо гнучкі стабільні системи управління на базі МК.

МК набули особливо великих значень і темпів в останні роки: від впровадження в традиційні МК системи, і до впровадження МК в спеціалізовані системи, як працюють в складі цифрових систем із залученням високорівневих IT- технологій [1-2, 4].

Але існує проблема стабільності і кібербезпеки основних робочих циклів мікропрограми МК та проблема несанкціонованих зовнішніх інформаційних втручань та впливів у МК по основним інтерфей-

сам і побічним (стороннім) каналам [1]. Кіберзагрози і інформаційні втручання за рахунок несанкціонованих підключень по стороннім вторинним каналам у МК можуть стати причиною нестабільності і відмов функціонування підпрограм мікроконтролера і наслідком виведення із ладу всієї системи управління на базі МК [1-4]. Тому кібербезпека інтерфейсів і вторинних каналів, а також мікропрограми МК (прошивки мікроконтрлерів) та їх основних інформаційних процесів – складна і до кінця не вирішена проблема, яка потребує оцінки і комплексного підходу та й досі актуальна [1].

Оцінка кіберзагроз і впливів по основним та вторинним каналам в МК – актуальна та необхідна проблема, яка потребує якісного і ефективного вирішення. Базовим у рішенні цієї проблеми на попередньому рівні є завдання розробки нової чи удосконалення існуючої математичної моделі оцінки факторів впливу на інформаційні процесів в МК. Це дозволить оцінити та врахувати ці фактори в основних процесах МК і дасть змогу отримати відповідь на питання «як протидіяти чи компенсувати впливи і кіберзігрози у сучасних мікроконтролерах?».

Метою статті є вдосконалення математичної моделі оцінювання кіберзахищеності інформаційної системи мікроконтролерів на основі розширення механізму оцінювання впливу інформаційних втручань і кіберзагроз на інформаційну стабільність процесів у мікроконтролерах, що враховує сумарний і окремі фактори впливу кіберзагроз.

Очікується, що математична модель буде достатньо точно оцінювати стан безпеки інформаційної системи мікроконтролера (МК), із врахуванням оцінки ризиків і сучасних кіберзагроз для мікропрограм та інформаційної системи МК.

Відомі підходи опису кіберзагроз та впливів у мікроконтролерах

Відома математична модель оцінки впливу кіберзагроз в інформаційних системах і схемах у вигляді математичної моделі порушника кібербезпеки інформаційної системи [5]. Ця модель досить добре описує процеси у взаємопов'язаних модульних комплексних інформаційних системах.

Також відомі моделі шкідливого впливу на відмовостійкість інформаційних систем [6] та моделі вразливостей апаратного забезпечення кіберфізичних систем [7], якими є системи із мікроконтролерами.

В контексті безпеки система управління із мікроконтролерами, перспективним є завдання вдосконалення і адаптування математичної моделі саме для мікроконтролерів із оцінкою впливу кіберзагроз та негативних факторів впливу по первинним та вторинним каналам у МК. Також модель повинна враховувати ризики для інформаційної системи самого МК. Для цього необхідно реалізувати синтез відомих моделей дестабілізуючих факторів кіберзагроз і впливів у МК.

Одним із супутніх завдань кіберзахисту МК і його підпрограми – є актуальні і точні оцінки впливу загроз, а також оцінки наслідків від їх впровадження у МК та супутні системи контролю. Для цього потрібна адаптація математичної моделі оцінки стану безпеки і оцінки кіберзагроз саме для інформаційної системи мікроконтролерів із врахуванням як факторів впливу, так і факторів захисту.

Проблематика аналізу і чисельної оцінки кібербезпеки системи мікроконтролера

Досить часто задачі аналізу стану локального захисту окремих ресурсів в архітектурі МК і захисту даних прирівнюються до завдання забезпечення повної кібербезпеки всієї системи мікро контролера [1]. Але досить часто це не відповідає реальному стану речей і необхідному рівню захисту, так як на локальному рівні можна захистити тільки конкретні ресурси. Наприклад, в кінцевих пристроях і інтерфейсах МК [1, 4, 6, 7] захист даних та інформаційних процесів в інформаційній системі мікроконтролера (ІС МК) не може гарантувати 100%-го захисту даних, що знаходяться у пам'яті та інших ресурсах МК. Тому аналітика локального захисту не вирішує завдання опису і моделювання повного комплексного захисту усієї системи інформаційної системи мікроконтролера. До того ж, неповнота, окремих функцій та аргументів в існуючих моделях та відсутність динамічних оцінок впливів призводять до низького рівня відповідності реальних процесів кіберзагроз у ІС МК та їх не вірної оцінювання. Тому завдання розробки математичної моделі для оцінки і врахування адекватного впливу повинно базуватись на:

– на аналізі самих інформаційних процесів кіберзагроз в МК;
– на оцінці впливів їх окремих компонент;
– на оцінці комплексного впливу багатьох факторів кіберзагроз в МК;
– на точному визначенню основних і супутніх факторів інформаційних втручань у МК;
– на оцінці вектору атаки і профілю захищеності МК – системи;
– на аналізі самих типів і факторів кіберзагроз і їх впливів на інформаційний процес МК системи.

Тому задача оцінки ризиків прояву кіберзагроз у МК зводиться до розроблення методики і математичної моделі оцінювання ризиків і опису процесів інформаційних впливів із максимальним врахуванням факторів впливу (факторів кіберзагроз) на МК-систему. Також важливо, щоб математична модель, яка буде вдосконалюватись враховувала вплив загроз «0-го» дня і найбільш впливові кіберзагрози, які можуть становити значні ризики і повинні бути враховані. Модель повинна бути максимально адекватною і простою в оперуванні, повинна дозволяти проводити аналіз інформаційної МК системи.

Варіанти і типи кіберзагроз для МК продовжують збільшуватись [1]. Сьогодні додаються все більше варіацій застосувань взаємопов'язаних МК пристроїв, їх протоколів і інтерфейсів МК [1-7] , це призводить до збіль-

шення кількість додаткових кіберзагроз і потенційних негативних інформаційних впливів по вторинним каналам МК. Сучасні засоби інформаційних втручань в промислові МК пристрої дозволяють успішно реалізовувати шкідливий функціонал дистанційно і втручатись у процеси МК шкідливим програмним забезпеченням (ШПЗ) [1, 4-7]. Наприклад, варіанти впливу ШПЗ: Stuxnet, Flame, miniFlame, Duqu, Gauss, Regin, Wiper, Shamoon, які експлуатують вразливості програмного коду МК Meltdown and Spectre [1] та інші складні шкідливі механізми із використанням обфускації, метаморфних перетворень виконавчого коду мікромодулів ШПЗ із приховуванням їх функціоналу і ознак. Окремі варіанти такого ШПЗ впроваджуються в системи індустріального контролю в складі автоматичних систем управління технологічними процесами (АСУ ТП) та інших електронних пристроїв на базі мікроконтролерів. Це дозволяє робити ін'єкції шкідливого коду і здійснювати інформаційні втручання із порушенням штатного режиму і функціоналу МК, суміжних засобів їх функціонування.

Модель оцінки кіберзагроз у МК дозволить оцінити ступінь впливу і може бути використана при оцінці наслідків в системах, підходах і методик захисту МК від кіберзагроз та інформаційних впливів. Особливо це стосується загрозу у формі ШПЗ у вигляді мікрокоду чи ініціації сторонніх шкідливих команд чи переривань, або мікромодулів ПЗ, спеціалізованого або вузько-орієнтованого шкідливого впливу по вторинним і первинним каналам в МК. Також загрозу представляють окремі мікромодулі ПЗ, які можуть бути викликані в самій мікропрограмі МК для МК систем, яке експлуатує вразливості МК.

Все це потребує адекватної оцінки і аналітики, що можна здійснити за допомогою математичної моделі оцінки загроз в мікро контролерах.

Розробка математичної моделі оцінки інформаційних впливів і кіберзагроз в ІС МК

Основними загрозами в сучасних архітектурах мікроконтролерів розглянуті в роботах [5, 7]. В роботі [5] проводився огляд математичних моделей для безпеки в інформаційних системах. Дані принципи та інтерпретація процесів частково справедлива і для МК систем із врахуванням окремих особливостей та конкретики і жорсткості опорної архітектури мікропроцесора із врахуванням моделей безпеки «Bell and LaPadulla», «Clarck Wilson Model» , «Roscoe-Woodcock» «CSP-model» [5], в яких описані підходи безпеки моделі захисту складних інформаційних систем. При розробці моделі безпеки в МК повинні використовуватись підходи імітаційного моделювання, які ґрунтуються на ймовірностях для розв'язання проблем поширення інформаційних загроз в середовищах комплексних комунікацій і розподілених блоків і окремих взаємопов'язаних обчислювальних функцій.

Так у [5] представлено математичні модель кібербезпеки інформаційної системи:

$$i(x,y)=\sum_{k=1}^{l} i_k(x,y)=\sum_{k=1}^{l} g_k\cdot p_k\cdot q_k(x)\cdot f_k(x,y) \qquad (1)$$

де, x та y – ресурси нападу і, відповідно, захисту, і при цьому справедливим є співвідношення $\sum_{k=1}^{l} x_k = X;\ \sum_{k=1}^{l} y_k = Y;$ k – номер об'єкта в складі МК(до об'єктів можуть бути віднесені окремі периферійні блоки в МК: наприклад, АЛП, ОЗП, ПЗП, регістри, тощо); g_k – відносна вартість інформації на k-му об'єкті (через g_k також позначається сам об'єкт); p_k — імовірність нападу на k-й об'єкт; $q_k\ (x)$ — щільність імовірності виділення нападом ресурсів x на k-ий об'єкт; $f_k(x,y)$ — імовірність вилучення інформації з k-го об'єкту, яку розглядаємо як динамічну вразливість об'єкта.

Дана модель [5] досить точно дозволяє описати процеси впливу в ІС (інформаційних системах) та в тому числі й у МК, але при їх взаємодії в рамках кожного інформаційного об'єкта і в сукупності, що досить зручно і компактно при описі впливів та різних факторів (і захисту і нападу) на об'єкт, а також дозволяє відносно оцінити ступінь впливу і взаємодії різних процесів між собою у математичному вигляді.

Також модель враховує таку відносно важливу величину (параметр) як вартість ресурсів, що є важним чинником при виборі технологій і систем захисту, а також оцінки їх ефективності. Але, вказана математична модель не враховує специфіку і характер процесів в кожному конкретному об'єкті та/або елементі інформаційної системи, а також не враховує й інтенсивність впливу різних процесів (і процесів захисту інформації і процесів нападу/атак на інформаційні ресурси) і питому вагу інформації в системі (відносний показник якості інформаційних даних в кожній конкретній підсистемі та/або об'єкту, які входять до складу системи).

Тому очевидно, що при оцінці впливу ресурсів нападу і захисту x та y – в кожному конкретному об'єкті та/або інформаційній системі потрібно враховувати специфіку інформаційного впливу із відповідними коефіцієнтами h_x f_y, і при цьому для всієї інформаційної системи, яка складається із l об'єктів справедливим є співвідношення:

$$\sum_{k=1}^{l} x_k = X;\ \sum_{k=1}^{l} y_k = Y;\ \ X > X';\ \ Y > Y';\ \sum_{k=1}^{l} x_k h_x = X';\ \sum_{k=1}^{l} y_k h_y = Y', \qquad (2)$$

Також модель (1) і модель (2) не враховує функції ефективності нападу, і захисту $f_d(X)$; $f_d(Y)$ і відповідні коефіцієнти ефективності захисту і відбиття атак μ_{eX} і їх щільності. Ці функції ефективності нападу і захисту є залежностями від комплексного аргумента, який залежить від багатьох умов і в т.ч. й особливостей побудови об'єкта . В такому випадку функція (1), яка представляє математичну модель оцінки кіберзахищеності ІС МК перепишеться як:

$$I(X,Y)=\sum_{k=1}^{l} i_k(x,y)=\sum_{k=1}^{l} g_k \cdot p_k \cdot q_k(x)\cdot f_k(x,y)\cdot \mu_{eX}(x,y)\cdot f^{d}{}_{k}(x,y), \tag{3}$$

де x та y – ресурси нападу і відповідно захисту, $\sum_{k=1}^{l} x_k h_x = X'$; $\sum_{k=1}^{l} y_k h_y = Y'$; k – позначення і індекс/номер системного об'єкта/системного елемента (наприклад, АЛП, RAM-ROM, інтерфесу, регістру, тощо і .т.п.) в МК; $f^{d}{}_{k}(x,y)$ – функція співвідношення ефективності захисту до нападу і до атак у інформаційній системі МК відповідно; g_k – відносна ціна(вартість) інформації на k-му об'єкті – блоці МК (окремо через g_k – може бути умовно позначений і сам блок в системі МК: наприклад окремий блок в архітектурі МК); p_k –ймовірність реалізації кіберзагрози на k-й блок в архітектурі МК; $q_k(x)$ – щільність ймовірності кіберзагроз у ресурсі x на k-й блок; $f_k(x,y)$ – функція ймовірності втрат/пошкодження/витоків інформації із k-го блоку в архітектурі МК, яку розглядаємо як динамічну вразливість k-го блоку в архітектурі МК. Прояв $f_k(x,y)$ може бути різним і призводити до: втрат; пошкодження; витоку; вилучення; модифікації даних в k-го блоку в архітектурі МК. В залежності від типу реалізації кіберзагрози; $\mu_{eX}(x,y)$ – функція ефективності захисту та ідентифікації ресурсу (функція ефективності захисту і відбиття кібератак в системі МК), $\mu_{eX}(x,y)\approx n\cdot\sum_{k=1}^{l}\mu_{eXk}(x,y)$. Причому $n\cdot$ – питомі коефіцієнти пропорційності і адаптації; $\mu_{eXk}(x,y)$ – функція ефективності захисту та ідентифікації ресурсу одиничного k-го блоку в архітектурі МК.

В залежності від типів кібератак може бути виконані різні прояви впливів в системі МК і зокрема сам процес впровадження може бути здійснений із різним ступенем адаптації та ефективності. Без врахування ефективності, в самому простому варіанті модель (3) може мати вигляд :

$$I(X,Y)\approx\sum_{k=1}^{l} i_k(x,y)=\sum_{k=1}^{l} g_k \cdot p_k \cdot q_k(x)\cdot f_k(x,y)\cdot f^{d}{}_{k}(x,y), \tag{4}$$

але модель (4) не може врахувати процес ефективності процесів впровадження інформаційних впливів, що важливим і у більшій мірі враховує конкретні практичні умови, максимально наближені до реальє дуже
них. Тому модель (3) є більш точною і враховує додаткові показники ніж модель (4) за рахунок введення додаткових параметрів і показників, зокрема функції ефективності нападу, і захисту до атак у інформаційній системі МК відповідно. Але в окремих випадках, коли ефективність впровадження кібератак і їх умови не дуже важлива, або нею можна знехтувати (в окремих випадках для спрощення і ототожнення простих розрахунків) може бути використана модель (4).

Як правило функція співвідношення ефективності захисту до нападу і до атак у інформаційній системі МК $f^{d}{}_{k}(x,y)$ та сама – функції ймовірності втрат/пошкодження/витоків інформації або їх захисту $f_k(x,y)$, мають експоненційну або квадратичну залежність , тобто $f_i(x,y)=n\cdot k\cdot e^{x}\cdot e^{y}$, *або* $f_i(x,y)=n\cdot k\cdot(x^2+y^2)$. В той ж час функція ефективності захисту $\mu_{eXk}(x,y)$ – як правило лінійну залежність $y = n\cdot k\,(\cdot x+y) + b_k$.

Функції функція співвідношення ефективності захисту до нападу забезпечує певну адаптивність системи до умов впливу та інформаційних втручань. Тому можна говорити про забезпечення певного ступеню адаптації інформаційного захисту до умов впливів і втручань (в т.ч. кіберзагроз) в мікроконтролерах.

Математична модель (4) є більш ефективною за (3), та точніше дозволяє оцінювати вплив на інформаційні об'єкти і саме у підсистеми ІС МК, що входить до складу інформаційної системи МК. А також підходить для оцінки впливу і захисту від загроз і атак (в т.ч. інформаційних втручань по побічним каналам) для мікропроцесорних систем. Ресурси нападу ілюструють множину функціоналу інформаційних зовнішніх і внутрішніх втручань в роботу основного циклу мікропрограми МК в т. ч. в порядок команд структуру і запис даних у стек пам'яті, тощо.

Модель опису загроз в (4) забезпечує розгляд по значно ширшим і вищим показникам ефективності загроз і захисту критичних даних в МК і в тому числі і МК для пристроїв IoT (Internet of Things, Інтерне-

ту речей) порівняно з іншими, непрямими ,методами. Модель може використовуватись для швидкої оцінки рівня загроз і факторів для їх попереднього аналізу у мікропроцесорних системах, в т.ч. для оперативного блокування трафіку і інформаційних потоків команд по побічних сторонніх каналах у МК IoT – по основному вектору загрози. Це такі загрози як:

– 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 ресурсоємного програмного коду тощо);

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

Підходи із використанням векторних моделей

Також, додатково модель (3) і її частковий випадок – модель (4) опису кібербезпеки інформаційної системи МК на базі поєднання комплексу технології і різних методик захисту функціональних блоків і вузлів МК може бути доповнена математичною моделлю опису інформаційних процесів у МК. Математична модель (4) описується функцією оцінки кіберзахищеності ІС МК, в той час векторні моделі на базі марківських ланцюгів [6] дозволяють відтворювати і описувати складні інформаційні процеси в мікроконтролерах із використанням теорії графів і інформаційних системах. Це виконується за допомогою функції графів параметрів із метаданими вкладеності в моделі взаємодії інформаційних процесів. Тобто, відтворення інформаційного процесу – як явища (на приклад, основного та шкідливого процесу (процесу кіберзагрози)) описується функцією графу – або просто графом із набором векторних параметрів.

Такі графи із X_n – вершинами у вигляді парної взаємодії описуються дискретними функціями взаємодії [6]:

$$G = (X_i, E_i) \tag{5}$$

де $X_i = \{x_1, x_2, \ldots, x_n\}$ – множина вершин графу; $E_i = \{e_1, e_2, \ldots, e_n\}$ – множина ребер графу.

Із врахуванням модульності архітектури МК складання його із k-блоків та і-зв'язків модель (5) перепишеться:

$$G = (X_i, Y_i, R_k'_i, n_i,) \tag{6}$$

де $Y_i = \{y_1, y_2, \ldots, y_n\}$ – множина ребер графу із врахуванням їх проекцій, $Y_i = f(E_i)$; $R'_i = \{r_1, r_2, \ldots, r_n\}$ – множина граней(які пов'язані через кути) графу(метаграфу); n_i – кінцева кількість елементів множин.

Кожне ребро метаграфу об'єднує дві підмножини вершин:

1. $X_i = \{x_1, x_2, \ldots, x_n\}$ – множина вершин графу;
2. $E_i = \{e_1, e_2, \ldots, e_n\}$ – множина ребер графу.

Метаграфом при цьому є граф із розширеними параметрами. Множина граней метаграфу саме для ІС МК і із врахуванням особливостей модульності архітектури МКдовщоляє відтворити процес в ІС МК і може бути визначена як:

$$R_k' = f_k(r_i) \cdot G_k = f_k(r_i) \cdot (X_i , Y_i) \quad (7)$$

Саме графічне представлення рівня мета графу показує взаємовплив і взаємозв'язки векторів , що описують параметри, і більш детально розглянуто у роботах опису векторних моделей [6].

Векторна модель представляється у вигляді графу процесів обробки в МК із метаданими і комплексом зв'язків у МК.

Модель, що описується формулами (6) для *n*-рівневого обчислювального процесу в МК передбачає, що чіткі зв'язки між елементами системи МК (наприклад, МК в пристрої IoT) існують тоді, коли зв'язки між окремими обчислювальними блоками і стадіями мікропрограми існують та чітко встановлені на верхніх рівнях взаємодії між ними. Це ж правило стосується і процесів в комунікаціях і передачі блоків даних в трактах передачі даних МК (порти та інтерфейси вводу-виводу). І наприклад, для моделі МК із 3-ма інформаційними блоками (об'єктами в архітектурі МК) формула матиме вигляд:

$$G_{comm} = f\{X_1, X_2, X_3, R_1, R_2, R_3\} \quad (8)$$

Зв'язки ребер метаграфу e_i між елементами обчислювального процесу мікропрограми МК передбачають взаємодію між елементами будь-якого рівня і включають множини [6] : $R_i = \{r_i^1, r_i^2, \dots , r_i^k\}$.

Множина процесів виконання інструкцій в інформаційній системі МК (в ядрі АЛП МК) і представлена елементами x_i (припустимо, $i=6$, АЛП - 6-й блок в архітектурі МК) в множині $X_6 = \{x_6^1, x_6^2, \dots , x_6^k\}$. із зв'язками $R_6 = \{r_6^1, r_6^2, \dots, r_6^k\}$.

Тому сусідні множини зв'язків $R_5 = \{r_5^1, r_5^2, \dots , r_5^k\}$ і $R_7 = \{r_7^1, r_7^2, \dots , R_7^k\}$ є взаємопов'язаними з $R_6 = \{r_6^1, r_6^2, \dots , r_6^k\}$ і визначаються по пов'язаним значенням і певним визначеним правилам.

Із врахуванням комплексної і модельної будови ІС МК формула (8) конкретизується і перепишеться у вигляді сум функції векторного добутку :

$$G = F\{X_1R_1, X_2R_2, X_3R_3, \dots X_iR_i, \dots . X_kR_k, \} \rightarrow \sum_{i=1}^{k} \vec{F}\{X_iR_i\} \quad (9)$$

Враховуючи область і вектор взаємодії процесів і роботи сервісів у комунікаційних трактах та інтерфейсах ІС МК, можна визначити особливості функцій і параметрів для системи характеристик параметрів МК в результаті передачі даних в комунікаціях ІС МК. Враховуючи використання стеку різних спеціалізованих протоколів і інтерфейсів, а також інколи необхідність шифрування (в окремих випадках) за допомогою спеціальних протоколів захисту даних, які працюють на вищому рівні для захисту каналу і даних в них, можна вважати, що система ІС МК в складі IoT знаходиться під впливом різних факторів і в тому числі факторів інформаційних втручань і факторів загроз кібербезпеки. Основною проблемою в МК IoT є різна обчислювальна і передавальна взаємодія окремих частин блоків команд і спільне використання ресурсів архітектури МК, що робить доступними одні частини ресурсів одних процесів доступними для інших. А також інформаційна «прозорість» інформаційно-комунікаційних трактів різних за архітектурою МК пристроїв, що створює можливості для проходження і проникнення інформаційних загроз. Крім того, специфіка і особливості використання різних архітектур і високо різність побудови МК не дозволяє використовувати традиційні моделі і засоби безпеки, орієнтовані на мультифункціональні платформи застосовувати їх до МК. Тому вирішення задач інформаційної безпеки МК вимагає комплексного диференційованого підходу і захисту комунікаційних складових, особливосте архітектур МК і впливів до зовнішніх інформаційних втручань – як основного вектору атак. Проблемою є також доступність та безпека зовнішніх комунікацій при дії невизначених процесів і роботою із неперевіреними потоками даних при взаємодії МК із зовнішньою периферією у складі електронних апаратних схем (рис. 1), які також можуть бути скомпрометовані. Місця основних загроз та впливів по стороні зовнішніх інтерфейсів і портів МК у зв'язаній архітектурі мікроконтролерної системи також показано на рисунку 1.

Напрямки суміжних інформаційних втручань (в т.ч. кіберзагроз несанкціонованого дистанційного доступу чи DDoS-атак в МК) у комплексній мікропроцесорній системі із різними взаємопов'язаними МК та іншими елементами, які показані на рис. 1 можуть бути комплексними і описуватись моделлю (8), за умови вірної побудови і врахування зв'язків між блоками і процесами. Наявність додаткових інформаційних комунікацій і блоків в інформаційні системі із МК є додатковим фактором загроз і ризиків інформаційної безпеки для МК системи (i+1), яка повинні бути враховані в моделях (5) та (8) . По функції інформаційного впливу це наближено до оцінок, які дані у [5]. Це приблизно відповідає залежностям: $G_{comm} = f\{X_i X_{i+1}, R_i R_{i+1}\} = f(x,y)$.

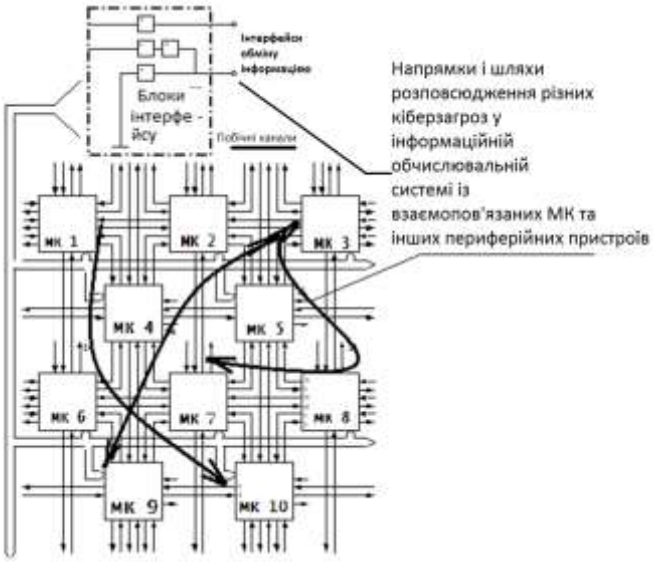
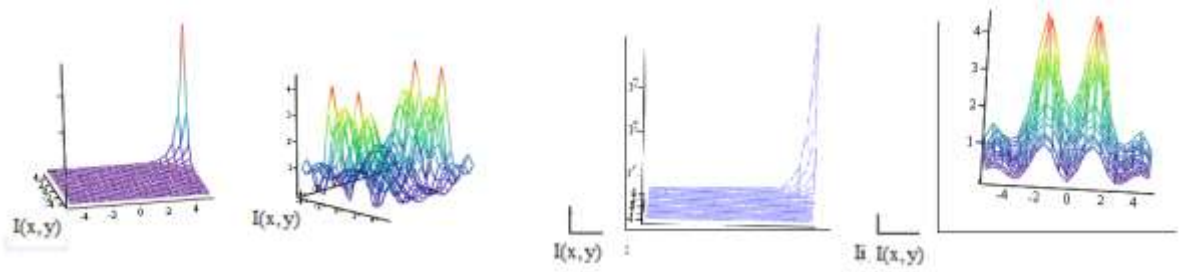


Рисунок 1 – Напрями розповсюдження потенційних інформаційних впливів (в т.ч. кіберзагроз) в комплексній та пов’язаній електронній системі на базі МК і окремих інформаційних блоків

Можна показати результати моделювання математичної моделі (4) і провести умовну оцінку характеру функції впливу для 3-х елементної системи, як це показано на рис. 2.



а) б)

Рисунок 2 – Вигляд інтегральної функції комплексних впливів та втручань у інформаційний процес у мікропрограмі МК по моделі (4): а) вигляд функції поверхні (частковий випадок випливу загроз у ІС МК із 3-ма параметрами та частковим випадком (*k=3*; *d=1*; i=3); б) вигляд функції інтегрального впливу з іншого боку (під іншим кутом вигляду)

Оскільки за моделлю (3) та (4), інтегральна функція комплексних впливів та втручань у інформаційний процес у ІС МК є функцією 2-х змінних – фона формує графік поверхні. Результати моделювання (рис. 2) по моделі (3) свідчать, що цей графік поверхні має лавиноподібний пик, що характеризує різкий і стрімкий вплив інтегральних складових кіберзагроз на інформаційних процес у МК починаючи із деякого порогового значення. Це також і свідчить про суттєвий і швидкий стрибок у інформаційному процесі в ІС МК: різкий негативний вплив на фунціонал інформаційного процесу МК, який значно зростає починаючи із деякого порогу. Починаючи із певного значення. Враховуючи баланс ресурсів моделі (3) - (4) та функції співвідношення ефективності захисту до нападу і до атак $f^{d}{}_{k}(x,y)$ у ІС МК, аналітично можна стверджувати, що відстань від початкової 0-ї точки координат до цього пику буде залежати від вхідних параметрів системи в моделі (3) - (4) і буде домінуючи залежати від самої функції ймовірності втрат/пошкодження/витоків інформації $f_k(x,y)$. Сам характер функції (рис. 2), як зазначалось вище, може мати нелінійний (експоненційний або квадратичний) прояв, в залежності від вхідних умов. Динаміка та експериментальні дослідження це підтверджують.

Як видно із рис. 2, комплексний вплив інформаційних впливів у ІС МК має узагальненюючий інтегральний нелінійно-наростаючий характер із пропорційним збільшенням величини амплітуди функції, в залежності від числа і значень факторів кіберзагроз у МК. Тобто, як видно із рис. 2: із ростом числа каналів впливів і загального число факторів загроз, сумарна функція впливу збільшується пропорційно із їх збільшенням.

На рис. 3 показані графіки цієї ж інтегральної функції комплексних впливів та втручань у інформаційний процес у мікропрограмі МК по моделі (3)-(4), за умов певного спрощення і обмеження вхідних умов , коли функція моделі (4) представляється функцією однієї змінної $I(x,y) \rightarrow I(x)|_{\lim y\ fxi(x,y)\to 0}$. Тобто в моделі (3)-(4) показано, що функція двох змінних в результаті деякого спрощення початкових умов замі-

нюється функцією однієї змінної (*df(x,y)→ df(x)|y→const*) із зведенням цієї функції до одновимірної функції при числовому заданні другої змінної у вигляді кінцевої константи на скорочених вхідних проміжках даних. В таких умовах графік може бути представлена функцією однієї змінної для задачі спрощення моделювання і чисельних задач. Графік такої функції є вже двовимірним графіком і включає спрощення завдання моделювання моделі (3)-(4), і показаний на рис. 3.

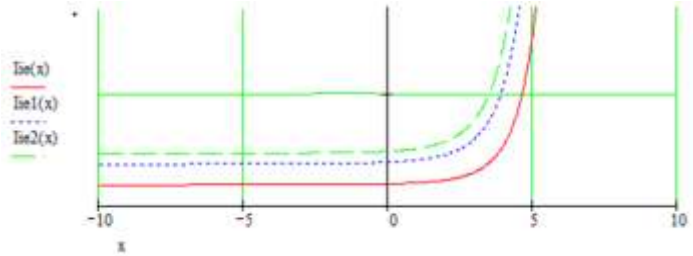


Рисунок 3 – Вигляд спрощеної інтегральної функції комплексних впливів та втручань у інформаційний процес ІС МК по моделі (4): вигляд деякого числа спрощених функцій із 3-ма параметрами (*k=3*; *d=1*; i=3)

При побудові моделі у МК із моделюванням функції розподіл зв'язків вкладень інформаційних процесів взаємодії у МК були враховані взаємозв'язки факторів множин *e* та *X* у моделях (3), (4), (6) та (8).

Математичні моделі що описуються формулами(3), (6) та (9) на відміну від існуючих враховують особливості модульності будови архітектури МК і безпековий вектор основних загроз – взаємопов'язані графи процесів в т. ч. вплив компонент графа із комунікаційні трактів МК та їх взаємозв'язки, а також множину піделементів взаємодії різних інформаційних процесів між собою в МК, а також і в його пам'яті.

Підходи до методу мінімізації ризиків кіберзагроз із врахуванням варіабельних факторів

Підходи до методу мінімізації ризиків полягають в тому, що якщо відома чи може бути простежена залежність між ресурсами нападу і ресурсами захисту, тобто *x=f(y)*, згідно (1), то можна згенерувати чи компенсувати негативний вплив ресурсів нападу x → *x', x' = f(y, x) ma y= f(x', x)* та самої ефективності нападу(як показано у (4)), і таким чином зменшити вплив на інформаційний процес негативного фактору впливу ресурсів нападу: $f_k(x, y) \rightarrow f_{k\,min}(x, y)$ у основному інформаційному процесі k-го блоку в архітектурі МК $i_k(x, y)$.

Основна ідея підходу методу мінімізації ризиків втручань в інформаційний процес МК полягає у тому, що якщо відома чи може бути визначена дія чи величина впливу кіберзагрози, відповідно може бути згенерована відповідна величина функції корекції в моделі (3) і (4), яка компенсує вплив:

$$f'_d(X)= F(f_d(Y)); \quad f'_x(x,y)\rightarrow f_{x\,min}(x,y); \quad \mu_{ex}(y,x)\rightarrow \mu_{ex\,ma}(y,x)_i \tag{10}$$

Одними з найбільш поширених моделей для оцінювання інформаційної безпеки є стохастичні ймовірнісні моделі, що основуються на ризиках [7, 8]. Зокрема, до таких належать ті, що дозволяють оцінювання ймовірності подій, які відбуваються за певним сценарієм. Тоді використовується така формула для обчислення ймовірності небажаної події *X* та *R*:

$$P(X)_{MK} = \sum_{i}^{n} \overline{P(X \mid R_i)} \cdot \overline{P(R_i)}\,, \tag{11}$$

де $P(R_i)$– ймовірність реалізації події кіберзагрози чи інформаційного втручання R_i; $P(X|R_i)$ – ймовірність виникнення події кіберзагрози *X* внаслідок гіпотези R_i.

Для зручності при ресурсному підході до оцінювання інформаційної безпеки результати формалізують в таблиці (табл. 1).

Заповнення таблиці 1 і визначення ймовірностей і типу загроз для МК відбувається поблоково в залежності від його архітектури і наявності блоків по формулі (11), індивідуально в кожному окремому випадку.

При коректному визначенні інформаційних ресурсів в ІС МК – сума ймовірностей в останньому рядку таблиці повинна наближатись до одиниці: $P_{kSUM}(X_{SUM}) \rightarrow 1$, що описує повну групу подій. Відповідно на основі оцінок цих ймовірностей та ймовірностей виникнення загроз інформаційному ресурсу визначити ймовірність настання хоча б однієї з них, використовуючи формулу, наведену вище оцінюють інтегральну ймовірність для всього об'єкту.

Для оцінки рівня впливу загрози та інформаційних втручань в трактах МК і в його трактах комунікацій (побічні канал) для інформаційних систем МК запропоновано використовувати оцінку відповідності DOC-стандартів CVSS, та отримувати інтегральні оцінки для МК-системи із орієнтованими на комплексну взаємодію факторів і взаємозв'язки різних інформаційних частин мікропрограми МК між собою (формули (3)-(7)). Так , рівень інформаційних втручань можна наближено оцінити за допомогою (4).

Таблиця 1 – Табличне представлення загроз і факторів впливу у моделі кібербезпеки МК

Назва і тип загрози та її ймовірність	**Інформаційні блоки (системні об'єкти) в складі архітектури МК**			
	Інформ. блок 1 (наприклад, АЛП)	**Інформ. блок 2 (наприклад, ОЗП)**	**Інформ. блок і**	**Інформ. блок k (наприклад, ПЗП)**
Загроза1, $P_1(X_1)=0.2$	0.22*	0.21*	…	0.24*
Загроза2, $P_2(X_2)=0.3$	0.31*	0.32*	…	0.34*
…	…	…	…	…
Загрозаі, $P_i(X_i)=0.1$	0.13*	0.12*	…	0.11*
Загроза k (k =i+1), $P_k(X_k)=0.05$	0.051*	0.052*	…	0.053*
Сумарно по всім загрозам $i=1 .. N$	По всім інформаційним блокам(об'єктам) МК: $k=1 .. N$, $P_{kSUM}(X_{SUM}) = 1$			

*-знак вказує на те, що значення ймовірностей введені для прикладу для окремого часткового випадку.

Запропонована модель оцінки фактору кіберзагроз і інформаційних втручань у ІС МК може з високою ефективністю і точністю використовуватись у діагностиці функціонального стану МК в т. ч. і на практиці.

На базі моделі рис. 2 враховуючи основний вектор загрози – напрямки канальної передачі даних по зовнішнім вторинним каналам та інтерфейсам МК, було запропоновано модель із врахуванням багатоканальності впливу і забезпеченням комплексного захисту даних на базі комутації каналів із використанням різних протоколів обміну, а також шифрування даних в МК у різні періоди часу із періодом T_i, в моделі захисту каналів інформаційних комунікацій ІС МК.

Схема впливу кіберзагрози на ІС МК може бути представлена як багатовекторна багатоканальна модель взаємодії – на рисунку 4.

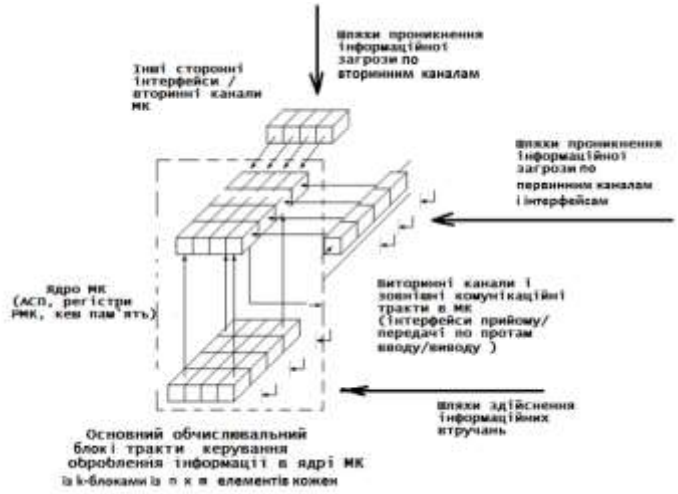


Рисунок 4 – Умовна ілюстративна схема інформаційних впливів (впровадження кіберзагроз) по основним і вторинним каналам у багатомодульному середовищі ІС МК

Дана схема (рис. 4) ілюструє комплексний фактор реалізації та напрямки ризиків і інформаційних втручань в каналах і інформаційно-комунікаційних трактах реалізації передавання даних в МК системах. Також вона дозволяє надати орієнтовні оцінки ризиків і шляхи їх нейтралізації.

Об'єктивні показники моделі :

- Канальні загрози інформаційній безпеці, що характеризуються ймовірністю реалізації, пропорційною кількості комунікацій в системі і можуть бути візуально проілюстровані ;
- Вразливі точки (точки реалізації загроз інформаційної системи або системи запобігання загрозам (системи інформаційної безпеки враховуються);
- Враховується ризики – чинники, що відображує можливі наслідки від реалізації кіберзагроз і вплив їх на інформаційну безпеку МК. Зокрема фактори: втрати/ модифікації/ несанкціоноване зчитування інформації та ризики, що відображають вірогідні втрати - прямі та непрямі.

Як зазначено авторами у [1, 2], для нейтралізації і вчасного попередження кіберзагроз використовуються прогресивні практики:

– проведення аналізу процесів функціонування МК;

– нейтралізація кіберзагроз і шкідливих впливів;

– використання комплексних підходів до інформаційного захисту в МК системі;

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

– підходи моніторингу і використання криптостійких та надійних алгоритмів;

– використання антивірусних платформ і мережевих систем аналізу трафіку.

Ефективність цих методів та підходів захисту ІС МК і досить часто й затрати на їх реалізацію не у повній мірі дозволяють отримати необхідний рівень безпеки інформаційної системи МК .

Співвідношення вартість/технічний функціональний рівень захисту систем і заходів захисту інформаційних систем МК не завжди відповідають необхідному і достатньому рівню, особливо враховуючи сучасні загрози «0»-го дня і рівень сучасного шпигунського і хакерського програмного забезпечення і методів запису /зчитування інформації для МК і суміжних із ними систем. А також недостатність і ґрунтовність оцінки впливу загроз за рахунок відсутності часто моделей і методик оцінювання інформаційних впливів на ІС МК .

Враховуючи складність вектору динамічність процесу впливу кіберзагроз в ІС МК, варіації їх рівня у часі t_i для складної і комплексної ІС МК системи, математична модель (3) – (4) можна представити у вигляді динамічної моделі оцінки загроз у різні моменти часу:

$$i_k(x,y,t) = \sum_{k=1}^{l} g_k \cdot p_k \cdot q_k(x) \cdot f_k(x,y,t_i,\frac{dj_i}{dt}); \qquad (12)$$

$$I(X,Y,t) \approx \sum_{k=1}^{l} i_k(x,y,t) = \sum_{k=1}^{l} g_k \cdot p_k \cdot q_k(x) \cdot f_k(x,y,t_i,\frac{dj_i}{dt}) \cdot \mu_{eX}(x,y,t_i,\frac{dj_i}{dt}) \cdot f_d(X,t_i,\frac{dj_i}{dt}) \cdot f_d(Y,t_i,\frac{dj_i}{dt}).$$

де, $f_k(x,y,t_i,\frac{dj_i}{dt})$ – динамічна функція появи загроз і втручань, яка характеризує їх інтенсивність та динаміку прискорень $\frac{dj_i}{dt}$ у часі t_i ; j – показник усередненої швидкості впливів кіберзагроз.

Дана модель (12) враховує динамічний характер впливу кіберзагрози та інформаційні втручання по різним інформаційним каналам втручань та розвиток їх у часі, що забезпечує розгляд по значно ширшим і вищим показникам ефективності при аналізі загроз і вчасного реагування на них і як наслідок підвищення ймовірності і швидкості їх виявлення і забезпечення захисту критичних даних і процесів в архітектури МК. Як результат дії вчасного і швидкого виявлення і ідентифікації загроз та впливів механізмами виявлення у комунікаційних трактам та інтерфейсах в МК можлива конкретна швидка дія по її нейтралізації – відсікання блокування цих каналів. Потім, на другій стадії передбачається запуск процесів відновлення гілок і даних алгоритмів мікропрограми МК або пере запуск окремих функцій чи всієї мікропрограми МК. При порівнянні із іншими моделями виявлення і захисту та іншими не прямими методами, дана модель (12) сумісно із моделями (5) та (8) може використовуватись для проведення швидкого динамічного аналізу і оцінки впливів, із подальшим прийняттям рішення про блокування інформаційного потоку із шкідливим фактором по *i*-му каналу в МК.

Запропонована модель оцінки впливу кіберзагроз та інформаційних впливів може із достатньою високою ефективністю використовуватись у практиці аналізу і захисту складових ІС МК (із різними архітектурами) в складі різних пристроїв як загального так і спеціального призначення, зокрема й пристроїв IoT. Саме різноманіття інформаційних загроз та потенційних шкідливих впливів в ІС МК може бути представлено у вигляді наступних логарифмічної залежності кількості загроз N_{MK} , що визначається кількстю всіх потенційно-можливих інформаційних загроз і впливів m_{MK} та n-кількістю їх точок і каналів впровадження (і в т.ч. і потенційних вразливостей системи МК) . Залежність, яка це описує може бути подана у вигляді:

$$I_{cyber} = log\ N_{MK} = log\ m_{MK}^{\ n} = nlogm_{MK} \qquad (13)$$

В такому випадку кількість інформації, яка описує всі можливі потенційні ризики й самі кіберзігрози в МК із n-кількістю точок впровадження і повною кількості загроз m_{MK} , та приблизною усередненою питомою ймовірністю появи кожної кіберзагрози (чи потенційного впливу) може бути описано як:

$$H_{cyberthreat} = -n\sum_{i}^{m_{mk}} \cdot p_{iMK} \log_2 p_{iMK} \cdot \qquad (14)$$

Формула описує втрати ентропію можливих кіберзагроз в МК і можу бути використана при побудові мапи кіберзагроз та моделі кіберзагроз в мікропроцесорі.

Орієнтовні втрати інформації при настанні кіберзагрози в МК можно оцінити по питомим ймовірностям появи кіберзагроз $P(y_i) \rightarrow p_{iMK}$ і ймовірностей самих подій $P(xj|yi) \rightarrow p_i$ основних ланок обчислювального процесу у внутрішній підпрограмі МК (прошивці МК):

$$H_{MK}(X \mid Y) = -n\sum_{i=1}^{n_{mk}} \cdot \sum_{j=1}^{m_{mk}} \cdot p_{MK}(y_i) \times p_{MK}(x_j \mid y_i) \times \log_2 p_{MK}(x_j \mid y_i) \quad (15)$$

Модель оцінки інформаційних втручань у множині потенційних загроз точок обчислювального процесу ІС МК при захисті комунікацій в інформаційно-комунікаційних трактах ІС МК на базі комутації пакетів в різні часові інтервали Т (із потенційним використанням шифрування) із використанням асинхронної передачі в різні інтервали часу :

$$F(T_{xi}Pr(t)) = f_t(t, 1P_{r.i}(x), H_{cyberthreat}) \cdot N \rightarrow f_t(t, 1P_{r.i}(x), H(X|Y)) \cdot \quad (16)$$

де, N – кількість всіх доступних машинних слів даних у біт/байт, враховуючи комбінацію їх формуванню по внутрішніми алгоритмам M; T_{xi}– часовий проміжок зміни машинного слова при різному режимі кодування і перетворення (оброблення) при обробленні і передаванні в архітектурі ІС МК.

Даний підхід передбачає виконання синхронізації комутаторів сторони А із стороною В у ІС МК і синхронна комутація в часі із шифровуванням даних в кожному новому вікні Ті іншим протоколом і з доступного пулу підтримуваних протоколів та забезпечення переключення кожен раз новим алгоритмом по циклу комутації.

На базі цієї моделі і підходу мінімізації (нейтралізації) і визначення кіберзагроз та шкідливих інформаційних втручань в ІС МК, можливий аналіз ризиків та кількісне оцінювання впливу кіберзагрроз в ІС МК із врахуванням впливу різних негативних факторів, їх величини та динаміки у ІС МК. Різна їх інтенсивність та нестабільні і незавжди визначені умови кіберзагроз у МК, різна інтенсивність інформаційних втручань робить задачу їх аналізу важкою, а завдання їх нейтралізації і протидії – складним і важким на практиці. В подальшому планується розробити інноваційні модель і метод захисту інформаційних процесів у ІС МК від кіберзагроз, який буде базуватись на інноваційних підходах функціональних мікро- і нано- сервісах перевірки безпеки процесів і гілок мікропрограм, визначення (ідентифікації кіберзагроз) що працюють безпосередньо в складі основної мікропрограми (прошивки) МК у вигляді окремої функції/об’єкту наряду із основним функціоналом і основними функціями МК в складі мікропрограми. Також , даний підхід повинен передбачати перевірку зовнішніх підключень і порядку слідування команд керування та переривань у МК, для контролю безпеки і виявлення втручань по побічним каналам. Передбачається врахування взаємодії МК із іншими інформаційними елементами в складі апаратних засобів і пристроїв автоматизації. Даний підхід і положення методу планується адаптувати до центральної частини архітектури МК і до канального рівня із захистом організації каналів інформаційної системи МК і суміжних підсистем та із організації моделі моніторингу ІС МК із різними інтенсивностями і декількома основними типами кіберзагроз у них.

Розроблена математична модель може стати основою для аналізу стабільності інформаційних процесів і бути використана при розробці зовнішніх засобів ІС МК, які послідовно підключаються до/або функціонують в складі основної архітектури ІС МК чи підсистем та засобів для прямого і непрямого аналізу та вимірювання шкідливих впливів і функціоналу мікро ПЗ (мікропрограм) мікро контролерів та кіберзагроз в їх коді.

Аналіз і нейтралізація сучасних кіберзагроз апаратного рівня [7-15] і шкідливого коду в мікропрограмі і трафіку в інтерфейсах МК і в складі обчислювального процесу повинна відбуватись в онлайн-режимі та в режимі реального часу (чи наближеному до реального часу). Використання комплексу технологій мережевого захисту основних мережевих протоколі і обчислювальних процесів, а також захисту трафіку передбачає умовно максимальну мінімізацію кіберзагроз та ризиків їх появи та дотримання критерію:

$$k \rightarrow min\ R_t\ , \quad (17)$$

де R_t – узагальнена ймовірність появи інформаційних ризиків в системі МК ($R_t \in M_r$) , де M_r – множина інформаційних ймовірностей загроз (мапа кіберзагроз), згідно (4) та (6).

Для побудови збалансованої системи інформаційної та кіберзбезпеки МК потрібно спочатку провести комплексний аналіз ризиків у сфері інформаційної безпеки біомедичної системи передачі даних . Потім визначити оптимальний рівень ризику для організації на основі заданого критерію. Систему інформаційної безпеки (контрзаходи) потрібно будувати так, щоб досягти заданого рівня ризику і заданого допустимого рівня інформаційного шкідливого впливу в ІС МК.

Висновки

В статті було розглянуто матеріали окремих досліджень, як власних так і досвіду закордонних вчених і спеціалістів, які ґрунтуються на роботах по аналізу ризиків мікроконтролерів, проведеної авторами раніше у [1]. В даній ж статті проведено розробку математичної моделі оцінки шкідливих впливів інформаційних втручань та кіберзагроз на основні аналізу домінуючих інформаційних ризиків і кіберзагроз у мікроконтролерах, які працюють в складі систем управління різноманітних як загальних так і спеціалізованих пристроїв. Приведене удосконалення математичної моделі саме для аналізу кіберзагроз у мікро

контролерах, із врахуванням різних факторів кіберзагроз та інформаційних впливів. Аналіз факторів приведено для мікроконтролерів, які працюють в складі систем управління різноманітних та спеціалізованих обчислювачів. Визначено основні показники моделі загроз та інформаційних впливів у МК, яка описує сумарний вплив інформаційних загроз і вектори кібератак у МК. В роботі також проведено оцінку і прогнози розвитку математичної моделі, проведено оцінку впливів базових типів кіберзагроз і факторів ризику для мікро контролерів. Це дає змогу оцінити основні усереднені сумарні впливи із боку кіберзагроз і вразливостей на стабільність функціонування МК і окремі місця в його архітектурі. Також модель може використовуватись при розробці підходів і методів стабільного і безпечного функціонування електронних систем на базі мікроконтролерів як загального, так і спеціального призначення.

Список літератури

[1] В.І. Маліновський, Л.М. Куперштейн, Аналіз загроз безпеки мікроконтролерів, «Інформаційні технології та комп‘ютерна інженерія», Вінниця, ВНТУ, №3(55), С. 21-32, 2022.

[2] Маліновський В.І. Мінімізація факторів кіберзагроз і спеціалізовані підходи до інформаційного захисту мікропроцесорних систем індустріального Інтернету речей. Матеріали LI-ї Науково-технічної конференції факультету інформаційних технологій та комп`ютерної інженерії (ФІТКІ), Вінниця, Україна: ВНТУ, 2022. [Електронний ресурс]. Режим доступу URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15000 . (Дата звернення 13.02.2024).

[3] Cybersecurity Enablers in MSPM0 MCUs: Application Note / Texas instruments Incorporated, 19.p., 2023. [Електронний ресурс]. Режим доступу URL: https: // https://www.ti.com/lit/an/slaae29/slaae29.pdf?ts=1708675272061&ref_url=https%253A%252F%252F www.google.de%252F . (Дата звернення 24.02.2024).

[4] Шологон Ю. З. Вразливості апаратного забезпечення кіберфізичних систем. Репозитарій Національного університету «Львівська політехніка» (Lviv Polytechnic National University Institutional Repository), 12.с., 2023. [Електронний ресурс]. Режим доступу URL: http://ena.lp.edu.u . (дата звернення 24.02.2024).

[5] Ю.М. Щебланін, Д.І. Рабчун, Математична модель порушника інформаційної безпеки. Кібербезпека: освіта, наука , техніка. №1(1), С.63-72, 2018, ISSN 2663-4023.

[6] В. М. Савченко, О. В. Мнушка. Модель безпеки інформаційної системи на базі технологій IoT. Вісник Національного технічного університету "ХПІ". № 28(1353), 2019, ISSN 2079-0031.

[7] Yuan Xiao, Yinqian Zhang, Radu Teodorescu. Speechminer: a Framework for investigating and measuring speculative execution vulnerabilities. [Електронний ресурс]. Режим доступу URL: https://arxiv.org/pdf/1912.00329.pdf. (Дата звернення: 20.10.2023р.).

[8] Meltdown and Spectre: Which systems are affected by Meltdown. [Електронний ресурс]. Режим доступу URL: https://meltdownattack.com/#faq-systems-meltdown. (Дата звернення: 20.10.2023р.).

[9] Meltdown and Spectre: Which systems are affected by Meltdown. [Електронний ресурс]. Режим доступу URL: https://meltdownattack.com/#faq-systems-meltdown. (Дата звернення: 20.10.2023р.).

[10] Speculative Processor Vulnerability. ARM Developer Forum. Specifications Updated, March 8, 2022. [Електронний ресурс]. Режим доступу URL: https://developer.arm.com/Arm%20Security%20Center/Speculative%20Processor %20Vulnerability. (Дата звернення: 20.10.2023р.).

[11] Cache Speculation Side-channels white paper. ARM Developer Forum. Specifications Updated March 8, 2022. [Електронний ресурс]. Режим доступу URL: https://developer.arm.com/documentation/102816/0205/. (Дата звернення: 20.10.2023р.).

[12] Kernel Side-Channel Attack using Speculative Store Bypass – CVE-2018-3639. [Електронний ресурс]. Режим доступу URL: https://access.redhat.com/security/vulnerabilities/ssbd . (Дата звернення: 20.10.2023р.).

[13] Kakareka, Almantas, У Vacca, John. Computer and Information Security Handbook. Morgan Kaufmann Publications, Elsevier Inc., p. 393, ISBN 978-0-12-374354-1.

[14] Serdar Yegulalp Rowhammer hardware bug threatens to smash notebook security / by Serdar Yegulalp// InfoWorld, March 9, 2015. [Електронний ресурс]. Режим доступу URL: https://www.infoworld.com/article/2894497/rowhammer-hardware-bug-threatens-to-smash-notebook-security.html. (Дата звернення: 20.10.2023р.).

[15] Kuljit Bains et al. Patent US № 20140059287 A1: Row hammer refresh command. [Електронний ресурс]. Режим доступу URL: https://patents.google.com/patent/US20140059287. (Дата звернення: 20.10.2023р.).

[16] Introduction to STM32 microcontrollers security. Application note. ST Microelectronics, 58 p., 2023. [Електронний ресурс]. Режим доступу URL:

https://www.st.com/resource/en/application_note/an5156-introduction-to-stm32-microcontrollers-security-stmicroelectronics.pdf. (Дата звернення: 22.02.2024р.).

[17] Automatic Microprocessor Performance Bug Detection / E. C. Barboza, S. Jacob, M. Ketkar, M.Kishinevsky, M., Gratz, P., & Hu, J. IEEE International Symposium on High-Performance Computer Architecture (HPCA). IEEE Publications, 2021. [Електронний ресурс]. Режим доступу URL: https://arxiv.org/pdf/2011.08781.pdf . (Дата звернення: 22.02.2024р.).

[18] Automatic Microprocessor Performance Bug Detection / Barboza, E. C., Jacob, S., Ketkar, M., Kishinevsky, M., Gratz, P., & Hu, J. IEEE International Symposium on High-Performance Computer Architecture (HPCA). IEEE Publications, 2021. [Електронний ресурс]. Режим доступу URL: https://doi.org/10.1109/hpca51647.2021.00053/ . (Дата звернення: 22.02.2024р.).

Стаття надійшла: 04.04.2024.

References

[1] V.I. Malinovs′kyy, L.M. Kupershteyn, Analiz zahroz bezpeky mikrokontroleriv, «Informatsiyni tekhnolohiyi ta komp‘yuterna inzheneriya», Vinnytsya, VNTU, №3(55), S. 21-32, 2022.

[2] Malinovs′kyy V.I. Minimizatsiya faktoriv kiberzahroz i spetsializovani pidkhody do informatsiynoho zakhystu mikroprotsesornykh system industrial′noho Internetu rechey. Materialy LI-yi Naukovo-tekhnichnoyi konferentsiyi fakul′tetu informatsiynykh tekhnolohiy ta komp`yuternoyi inzheneriyi (FITKI), Vinnytsya, Ukrayina: VNTU, 2022. [Elektronnyy resurs]. Rezhym dostupu URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15000.

[3] Cybersecurity Enablers in MSPM0 MCUs: Application Note / Texas instruments Incorporated, 19.p., 2023. [Elektronnyy resurs]. Rezhym dostupu URL: https: // https://www.ti.com/lit/an/slaae29/slaae29.pdf?ts=1708675272061&ref_url=https%253A%252F%252Fwww.google.de%252F . (Data zvernennya 24.02.2024).

[4] Sholohon YU. Z. Vrazlyvosti aparatnoho zabezpechennya kiberfizychnykh system. Repozytariy Natsional′noho universytetu «L′vivs′ka politekhnika» (Lviv Polytechnic National University Institutional Repository), 12.s., 2023. [Elektronnyy resurs]. Rezhym dostupu URL: http://ena.lp.edu.u . (data zvernennya 24.02.2024).

[5] YU.M. Shcheblanin, D.I. Rabchun, Matematychna model′ porushnyka informatsiynoyi bezpeky. Kiberbez-peka: osvita, nauka , tekhnika. №1(1), S.63-72, 2018, ISSN 2663-4023.

[6] V. M. Savchenko, O. V. Mnushka. Model′ bezpeky informatsiynoyi systemy na bazi tekhnolohiy IoT. Visnyk Natsional′noho tekhnichnoho universytetu "KHPI". № 28(1353), 2019, ISSN 2079-0031.

[7] Yuan Xiao, Yinqian Zhang, Radu Teodorescu. Speechminer: a Framework for investigating and measuring speculative execution vulnerabilities. [Elektronnyy resurs]. Rezhym dostupu URL: https://arxiv.org/pdf/1912.00329.pdf. (Data zvernennya: 20.10.2023r.).

[8] Meltdown and Spectre: Which systems are affected by Meltdown. [Elektronnyy resurs]. Rezhym dostupu URL: https://meltdownattack.com/#faq-systems-meltdown. (Data zvernennya: 20.10.2023r.).

[9] Meltdown and Spectre: Which systems are affected by Meltdown. [Elektronnyy resurs]. Rezhym dostupu URL: https://meltdownattack.com/#faq-systems-meltdown. (Data zvernennya: 20.10.2023r.).

[10] Speculative Processor Vulnerability. ARM Developer Forum. Specifications Updated, March 8, 2022. [Elektronnyy resurs]. Rezhym dostupu URL: https://developer.arm.com/Arm%20Security%20Center/Speculative%20Processor %20Vulnerability. (Data zvernennya: 20.10.2023r.).

[11] Cache Speculation Side-channels white paper. ARM Developer Forum. Specifications Updated March 8, 2022. [Elektronnyy resurs]. Rezhym dostupu URL: https://developer.arm.com/documentation/102816/0205/. (Data zvernennya: 20.10.2023r.).

[12] Kernel Side-Channel Attack using Speculative Store Bypass – CVE-2018-3639. [Elektronnyy re-surs]. Rezhym dostupu URL: https://access.redhat.com/security/vulnerabilities/ssbd . (Data zvernennya: 20.10.2023r.).

[13] Kakareka, Almantas, U Vacca, John. Computer and Information Security Handbook. Morgan Kaufmann Publications, Elsevier Inc., p. 393, ISBN 978-0-12-374354-1.

[14] Serdar Yegulalp Rowhammer hardware bug threatens to smash notebook security / by Serdar Yegulalp// InfoWorld, March 9, 2015. [Elektronnyy resurs]. Rezhym dostupu URL: https://www.infoworld.com/article/2894497/rowhammer-hardware-bug-threatens-to-smash-notebook-security.html. (Data zvernennya: 20.10.2023r.).

[15] Kuljit Bains et al. Patent US № 20140059287 A1: Row hammer refresh command. [Elektronnyy re-surs]. Rezhym dostupu URL: https://patents.google.com/patent/US20140059287. (Data zvernennya: 20.10.2023r.).

[16] Introduction to STM32 microcontrollers security. Application note. ST Microelectronics, 58 p., 2023. [Elektronnyy resurs]. Rezhym dostupu URL: https://www.st.com/resource/en/application_note/an5156-introduction-to-stm32-microcontrollers-security-stmicroelectronics.pdf. (Data zvernennya: 22.02.2024r.).

[17] Automatic Microprocessor Performance Bug Detection / E. C. Barboza, S. Jacob, M. Ketkar, M.Kishinevsky, M., Gratz, P., & Hu, J. IEEE International Symposium on High-Performance Computer Architecture (HPCA). IEEE Publications, 2021. [Elektronnyy resurs]. Rezhym dostupu URL: https://arxiv.org/pdf/2011.08781.pdf . (Data zvernennya: 22.02.2024r.).

[18] Automatic Microprocessor Performance Bug Detection / Barboza, E. C., Jacob, S., Ketkar, M., Kishinevsky, M., Gratz, P., & Hu, J. IEEE International Symposium on High-Performance Computer Architecture (HPCA). IEEE Publications, 2021. [Elektronnyy resurs]. Rezhym dostupu URL: https://doi.org/10.1109/hpca51647.2021.00053/ . (Data zvernennya: 22.02.2024r.).

Відомості про авторів

Маліновський Вадим Ігорович – к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Vadim Malinovskyi – PhD (Eng), Associate Professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia

Куперштейн Леонід Михайлович – к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Leonid Kupershtein – PhD (Eng), Associate Professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia

Лукічов Віталій Володимирович – к.т.н., доц. каф. захисту інформації, Вінницький національний технічний університет, м. Вінниця

Vitalii Lukichov – PhD (Eng), Associate Professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia

V. Malinovskyi, L. Kupershtein, V. Lukichov

MATHEMATICAL MODEL FOR ASSESSING CYBER THREATS AND INFORMATION IMPACTS IN MICROCONTROLLERS

Vinnytsia national technical university, Vinnytsia