DOI 10.20535/2411-1031.2023.11.1.283816
УДК 621.391

ДМИТРО МОГИЛЕВИЧ,
РОМАН СБОЄВ

АНАЛІЗ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ОБЛАДНАННЯ ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ СИСТЕМИ

На сьогоднішній день обладнання електронних комунікаційних мереж (ОЕКМ) складається з двох взаємопов'язаних компонент. Перший – це апаратний, другий – програмний, від нормального функціонування кожного з яких залежить функціонування мережі загалом. Одним з головних понять, які характеризують здатність мережі виконувати завдання за призначенням є функціональна безпека (ФБ). Це поняття подібне до поняття надійності проте відрізняється, головним чином, тим, що в контексті надійності розглядаються всі можливі відмовні ситуації, а при розгляді ФБ лише ті, які призводять до зриву функціонування певної системи. Так, відмови поділяються на чотири категорії: виявлені безпечні та небезпечні, невиявлені безпечні та небезпечні. З точки зору ФБ розглядаються і становлять загрози лише невиявлені небезпечні. За кількістю небезпечних невиявлених відмов розділяють чотири рівні повноти безпеки. У статті також розглянуто основні міжнародні стандарти, у яких наведені визначення, кількісні характеристики основних параметрів ФБ. Так, до основних параметрів ФБ можна віднести коефіцієнт готовності системи, середній час до відмови, імовірність небезпечної невиявленої відмови. При цьому при аналізу ФБ може бути застосований математичний апарат теорії надійності. Водночас, апаратний компонент ОЕКМ є доволі широко дослідженим, а програмний компонент потребує подальшого вивчення. Також на ФБ програмної складової впливає ряд чинників, як зовнішні (сторонні зловмисні впливи, віруси, відмови апаратної складової тощо), так і внутрішні (системні помилки, алгоритмічні помилки, помилки проектування). Подальше завдання полягає у формуванні методів і заходів, спрямованих на усунення або зменшення впливу впливаючих факторів. Також, оскільки в ОЕКМ широко використовуються різні види програмного забезпечення (ПЗ), переважно системного, то на ньому й необхідно зосередити подальші дослідження.

Ключові слова: функціональна безпека, надійність, збої та відмови програмного забезпечення, обладнання електронних комунікаційних мереж.

Постановка проблеми. Сучасне обладнання електронних комунікаційних мереж можна представити у вигляді складного апаратно-програмного комплексу (АПК), що складається з двох взаємопов'язаних компонентів: апаратного − сукупності технічних засобів, що включають до свого складу каналоутворююче та кінцеве обладнання, апаратуру IP-шифрування, пристрої комутації, мультиплексування та маршрутизації; програмного – сукупності програмних засобів (ПЗ) (об'єкт, який складається із програм, процедур, правил, а також, якщо передбачено, супутніх їм документації та даних, що відносяться до функціонування ОЕКМ).

Терміни "функціональна безпека" та "надійність" взаємопов'язані, та застосовуються як при дослідженні ОЕКМ загалом, так і системного ПЗ таких мереж зокрема, адже вони описують здатність системи залишатися працездатною та виконувати свої функції під впливом певних негативних чинників.

Основна відмінність ФБ від надійності полягає в тому, що в показниках надійності враховуються всі реалізації небезпечних відмов, а при характеристиці ФБ реєструються та

враховуються лише ті відмови, які призвели до катастрофічних збитків, які позначилися на безпеці системи та втрати інформації користувачів, а інколи – і самих користувачів. Оскільки фактори, що впливають на реальні значення показників надійності та ФБ подібні, то вони можуть бути застосовані при оцінці ФБ критичних систем (до яких відносяться і ЕКМ), і способи оцінки та випробувань ФБ можуть базуватися на методах визначення надійності функціонування ПЗ.

Таким чином безперервно зростаюча складність і внаслідок цього вразливість ПЗ від випадкових негативних впливів, висунули ряд задач, що потребують подальшого дослідження, пов'язаних з надійністю та ФБ ПЗ ОЕКМ, у розряд найважливіших – стратегічних, що визначають принципову можливість та ефективність їх застосування.

Аналіз основних досліджень і публікацій. Перші дослідження в напрямку надійності ПЗ були проведені ще в другій половині XX століття. Одним з основоположників даних досліджень є Маєрс. У [0] описано широкий спектр методів, спрямованих на підвищення надійності програмного забезпечення.

У роботі [0] проведено моделювання та аналіз надійності телекомунікаційних мереж і систем є широкою темою і включає багато методів, починаючи від блок-схем надійності та інших комбінаторних методів з одного боку до моделей Маркова, мереж Петрі тощо для більш складних моделей з іншого. Є як аналітичні, так і чисельні методи. У цій статті надано характеристики телекомунікаційних систем щодо надійності та представлено кілька прикладів для ілюстрації типів математичного моделювання та аналізу, які проводяться в промислових умовах у процесі побудови надійних телекомунікаційних система. Описано телекомунікаційні моделі надійності з точки зору систем як апаратних, так і програмних компонентів.

Стаття [0] присвячена деяким важливим питанням аналізу функціональної безпеки, зокрема верифікації рівня повноти безпеки (SIL) функцій безпеки, які будуть реалізовані в рамках розподілених систем управління та захисту. Запропоновано метод, який використовує кількісні та якісні показники для перевірки SIL.

У [0] досліджуються складові забезпечення гарантоздатності автоматизованих систем, до яких висуваються підвищені вимоги у зв’язку з їх використанням у багатьох чутливих для держави сферах суспільної діяльності, включаючи національну безпеку і оборону, критичні промислові технології, енергетика та зв'язок, банківська сфера, захист навколишнього середовища, технології легітимного дистанційного навчання тощо. Визначені складові можуть суттєво впливати на якість та надійність надання інформаційних послуг у нормативно визначених умовах. Зокрема, показана особлива роль функціональної безпеки криптографічної підсистеми у плані підтримки виконання автоматизованою системою передбачених для неї завдань і функцій загалом, а також у частині забезпечення конфіденційності і цілісності інформації. Визначені складові криптографічної підсистеми, неякісна або некоректна робота яких негативно впливає на безпеку застосування цих підсистем. Проаналізовані види найбільш небезпечних атак на ці підсистеми, наведено їх класифікацію з точки зору можливості реалізації у сучасних науково-технічних умовах та залежно від потужності наявних обчислювальних засобів та технологій, на підставі чого визначено найбільш реальний та небезпечний варіант реалізації віддалених атак на програмну реалізацію криптографічної підсистеми. На підставі проведеного аналізу запропоновано метод оцінки якості криптографічних перетворень, що базується на модифікованому алгоритмі розв’язання задачі пошуку рішення систем лінійних рівнянь із спотвореними правими частинами з використанням так званого декодування на основі “списків” “вкорочених” кодів Ріда-Маллера першого порядку, Доведено коректність запропонованого алгоритму.

У [0] ЕКМ розглядаються як складні стохастичні мережі. Це ставить перед постачальником послуг величезні труднощі щодо забезпечення бажаної якості обслуговування для клієнта. Через стохастичну поведінку мережі забезпечення вимагає

серйозних зусиль, щоб змусити всю систему працювати в рамках заданого обмеження часу, вартості та частоти відмов. Пропонуються швидкі рішення задач передачі даних для надсилання необхідної одиниці даних користувача від бажаного вузла джерела до вузла призначення в межах деяких обмежень, таких як допустима частота помилок , обмеження в часі та бюджетні обмеження на технічне обслуговування. Надійність системи та продуктивність запропонованих підходів оцінюється за допомогою мінімальних шляхів. Усі вектори мінімального потоку, оцінені з мінімальних можливих шляхів, які задовольняють усі вищезазначені обмеження, розглядаються для оцінки надійності мережі. Крім того, запропоновані підходи вважаються швидшими щодо часу обчислення, ніж існуючі підходи.

У [0] розглянуто ФБ в сучасній автомобільній техніці. Сучасні транспортні засоби мають широкий спектр функцій. Деякі пропонують комфортну підтримку для сценаріїв водіння, а інші пропонують вищий рівень безпеки для водія. Збільшення кількості складних систем викликає потребу в надійній техніці, щоб уникнути або принаймні виявити та пом’якшити несправності, які можуть призвести до травм будь-якої людини. Таким чином, ціллю завжди має бути дотримання сучасного рівня техніки для визначення, проектування та впровадження будь-якої системи. Необхідність відповідати суворим вимогам безпеки стандарту *ISO 26262* створює нові виклики. Зокрема, рішення повинні гарантувати безпечну роботу автомобільних електронних систем протягом усього життєвого циклу автомобіля. ФБ залежить від механізмів безпеки всередині конструкції, які контролюють і перевіряють правильну функціональну роботу конструкції під час використання системи. Здатність цих механізмів безпеки покривати потенційні несправності визначає загальне діагностичне покриття конструкції. Як рішення, яке вирішує ці проблеми, у цьому документі представлено концепцію додаткового аналізу ефекту режиму відмови для реакції системи моніторингу, де потенційні причини відмови в умовах експлуатації клієнта аналізуються з огляду на технічний вплив на систему. Наведений метод оцінює зниження ризику шляхом моніторингу та оцінки реакції системи та сприяє наданню доказів здатності діагностичних, логічних і виконавчих механізмів досягати та підтримувати відповідний стан.

У [0] автори також розглядаються ФБ з точки зору сучасної автомобільної техніки. Автомобіль складається з кількох електронних блоків керування для підтримки різноманітних важливих для безпеки функцій. Основні системи чутливі до атак безпеки та кібербезпеки, оскільки задіяні блоки взаємопов’язані. Атаки на безпеку можуть призвести до порушення безпечної експлуатації транспортного засобу та спричинити травми пасажирам. Традиційно група безпеки виконує аналіз небезпеки та оцінку ризиків (*HARA*), а група безпеки виконує аналіз загроз та оцінку ризику (*TARA*) для оцінки ризику, пов’язаного з інцидентами безпеки. Ризик безпеки, розрахований за допомогою *HARA*, не враховує вплив інцидентів безпеки на нього. Подібним чином ризик безпеки, розрахований у *TARA*, не враховує всі аспекти функціональної безпеки, пов’язані із залученими активами. Таким чином, мета цієї статті полягає в тому, щоб об’єднати вплив загроз безпеці та атак на безпеку через єдину структуру, *THARA*. Отже, вимоги функціональної безпеки та вимоги кібербезпеки можуть бути узгоджені одні з іншими. У цій статті представлено практичне дослідження застосування інфраструктури *THARA* за допомогою аналізу ризиків безпеки та загроз безпеці.

У статті [0] розглянуто проблеми, пов’язані з мережами та протоколами ФБ в екосистемах промислового Інтернету речей. Функціональні мережі безпеки набувають першочергового значення в промислових системах завдяки прогресивним інноваціям, запровадженим парадигмою *Industry* 4.0, яка характеризується високою гнучкістю виробництва, надійністю та масштабованістю. У цьому контексті з’явилися нові та складні програми, такі як гіперавтоматизація, яка стосується поєднання робототехніки, комунікації та навчання з явною участю людей. Для цього потрібне повсюдне підключення, яке охоплює промисловий Інтернет речей, яке зазвичай досягається через бездротові системи. Наприклад,

бездротовий зв’язок сьогодні має фундаментальне значення для відкриття нових категорій автономних пристроїв, які можуть активно співпрацювати з людським персоналом у виробничому процесі. Цей складний сценарій має важливі наслідки для безпеки. Дійсно, для забезпечення задовільного рівня безпеки необхідна надійна координація між датчиками, виконавчими механізмами та обчислювальними системами, особливо у випадку інноваційних процесів і технологій, таких як мобільна та спільна робототехніка. Отже, необхідно забезпечити правильну передачу важливих для безпеки даних через мережі зв’язку. У статті розглянуто проблеми, пов’язані з мережами та протоколами ФБ в екосистемах промислового Інтернету речей. Спочатку представлено конструктивні характеристики мереж функціональної безпеки та протоколи безпеки в бездротових мережах. Потім більше конкретно розглянуто один із таких протоколів, а саме *Fail Safety over EtherCAT (FSoE)*. Результати експериментів можуть бути використані як основа для обговорення майбутніх тенденцій ФБ в епоху промислового Інтернету речей.

Метою статті є аналіз функціональної безпеки обладнання електронних комунікаційних системи.

Виклад основного матеріалу дослідження. Проведений аналіз показав, що саме ФБ програмного забезпечення ОЕКМ суттєво впливає на ФБ ОЕКМ в цілому й тому потребує більш детального дослідження. Програмне забезпечення, на відміну від апаратного, можна вважати змінною частиною мережевих пристроїв.

Програмне забезпечення поділяють на (рис.1):

1) системне:

– базовий рівень *(firmware)* – драйвери;

– операційні системи (ОС) – набір програм, які забезпечують взаємодію інших програм з базовими програмами та апаратними засобами;

– службовий рівень – програми в складі ОС;

2) прикладне – забезпечує виконання конкретних завдань на комп'ютері, Наприклад текстові та графічні редактори, диспетчери файлів, архіватори даних, *WEB*-браузери тощо.

3) інструментальне / сервісне (системи програмування) – ПЗ, призначене для використання в ході створення архітектури, розробки, оновлення та інсталяції програм. Прикладом є різні середовища розробки.

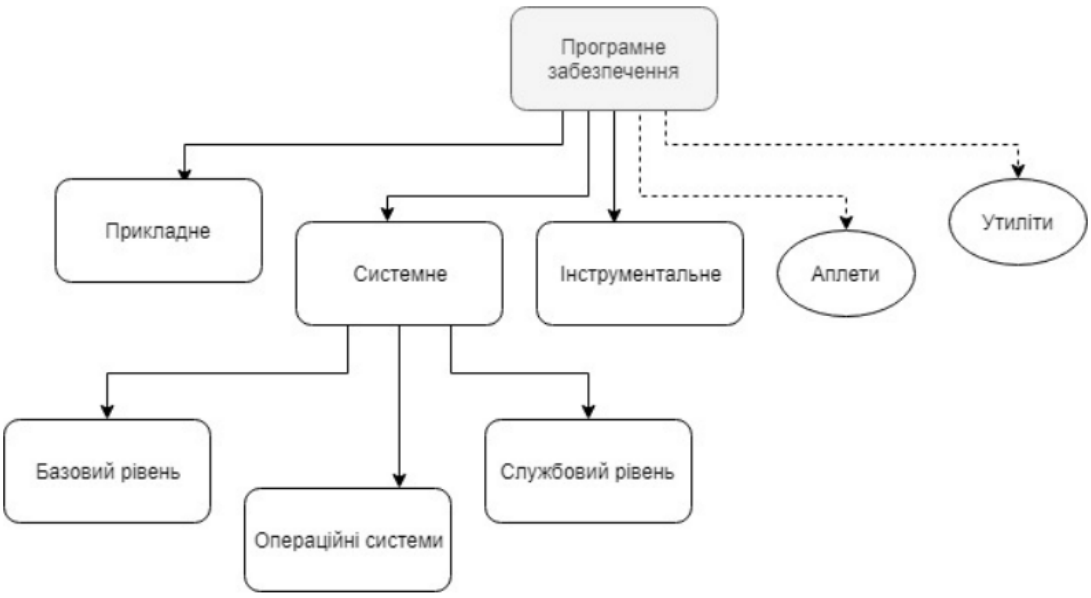

Рисунок 1 – Класифікація ПЗ

Додатково виділяють утиліти та аплети. *Утиліти* – корисні програми з обмеженими функціями. Деякі утиліти поставляються з операційними системами. Як і програми, утиліти, як правило, встановлюються окремо і можуть використовуватися незалежно від решти операційної системи. *Аплети* – це короткі комп'ютерні програми, які розширюють функції основної програми. Іноді вони поставляються з операційною системою як допоміжні застосунки. Вони також можуть бути створені незалежно, у процесі використання мов програмування.

Найбільш поширеним, та, відповідно, таким, що здійснює найбільший вплив на ФБ в електронних комунікаційних мереж є саме системне ПЗ обладнання.

Збитки від дефектів та помилок системного ПЗ можуть мати кумулятивний характер, і проявлятися, у певних відмовних ситуаціях, які впливають на надійність, але не відображаються на ФБ.

Накопичення таких відмов з часом може призводити до наслідків, що порушують функціональну безпеку ОЕКМ та їх застосування. Таким чином, додатково зближуються поняття надійності та ФБ складних систем та ПЗ, відповідно. Але при однакових джерелах загроз та їх проявах ці поняття можна розділити за величиною наслідків та шкоди при виникненні відмовних ситуацій.

Основні поняття в галузі ФБ систем та програмних продуктів характеризуються факторами, пов'язаними з виникненням небезпечних станів, що призводять до втрати працездатності. Якщо ці події не виявляються і не усуваються спеціально введеними до складу системи засобами забезпечення ФБ, то виникають небезпечні відмови та їх наслідки. При дослідженні ФБ доцільно використовувати терміни й поняття, які наведені в стандарті *IEC 61508* [9]. Згідно з [0] ФБ – частина загальної безпеки, що відноситься до устаткування, що піддається керуванню (УПК) та системи керування УПК, та залежить від коректного функціонування систем електронних пристроїв та програмованих електронних пристроїв, пов'язаних з безпекою та інших засобів зниження ризику.

Для забезпечення заданого рівня ФБ необхідне виконання наступних типів вимог:

1) до функцій безпеки, які виконуються системою керування;

2) до імовірності задовільного виконання функцій безпеки.

Ці вимоги формуються після проведення аналізу ризиків системи.

За методами та ресурсами, необхідними для досягнення заданих значень ФБ доцільно обчислювати інтенсивності відмов та частку безпечних відмов, що визначають рівні повноти безпеки (РПБ).

Частка безпечних відмов (ЧБВ або *safe failure fraction* (*SFF*)) – властивість елемента, пов'язаного з безпекою, що визначається співвідношенням середніх інтенсивностей відмов безпечних та небезпечних виявлених відмов до безпечних та небезпечних відмов.

Відповідно, необхідно провести класифікацію відмов. Небезпечні відмови – призводять до втрати ФБ системи та / або до втрати її безпечного стану. Безпечні – призводять до помилкового відключення виходу і зупинки контрольованого технологічного процесу (помилкове спрацювання) (рис. 2) [0].

З точки зору надійності розглядаються всі типи відмов, з точки зору ФБ – тільки небезпечні невиявлені відмови. Оскільки кількість небезпечних невиявлених відмов безпосередньо виміряти неможливо, то їх рахують як різницю між загальною кількістю відмов, і ЧБВ.

Частка безпечних відмов визначається за формулою:

$$SFF = (\sum \lambda_S + \sum \lambda_{DD}) / (\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DD}). \quad (1)$$

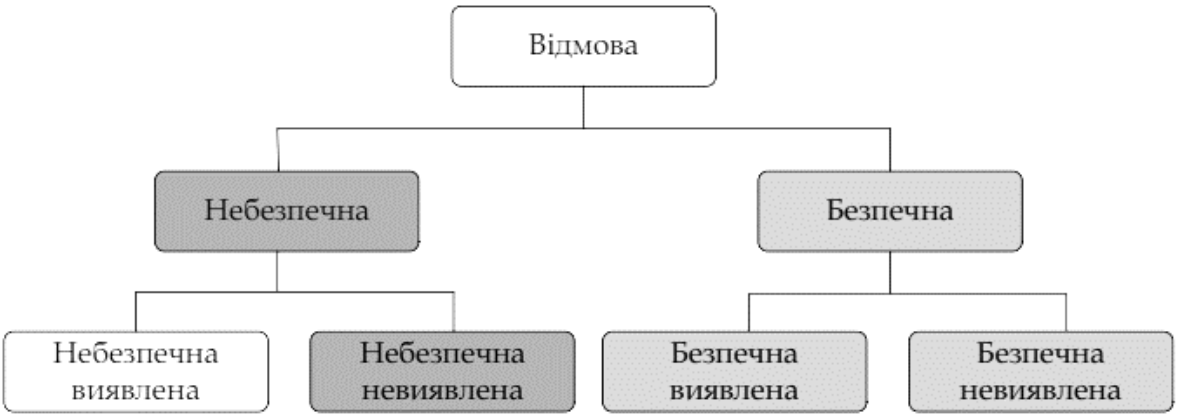

Рисунок 2 – Класифікація відмов за впливом на ФБ та можливістю виявлення

Наочно ЧБВ представлена на рис. 3.

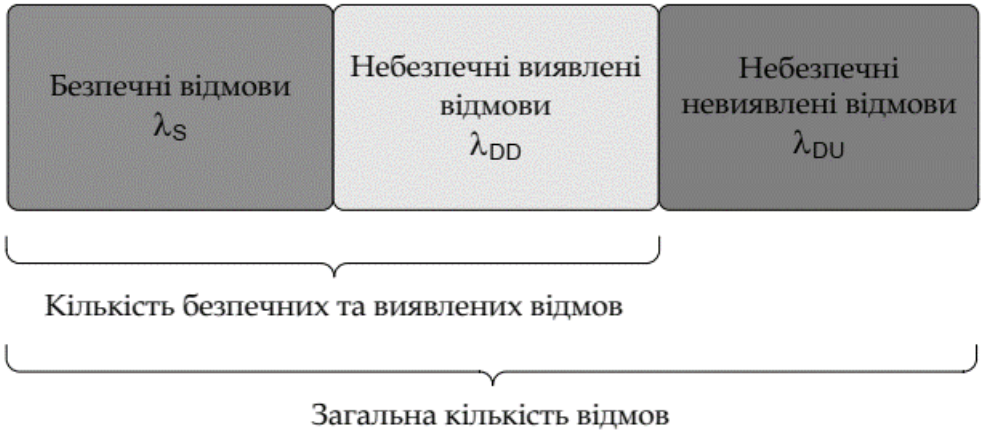

Рисунок 3 – Співвідношення відмов

До основних показників ФБ можна віднести: імовірність безвідмовної роботи ($P(t)$); ймовірність небезпечної відмови ($P_{\text{НВ}}(t)$); середній час напрацювання до небезпечної відмови; інтенсивність небезпечних відмов (λ_{DU})(рис.3); коефіцієнт готовності $K_{\text{г}}$.

Усі показники розраховуються, використовуючи вже наявні інстурменти теорії надійності.

Імовірність безвідмовної роботи ($P(t)$) – імовірність того, що відмова не відбудеться за визначений час безвідмовної роботи (або час напрацювання до небезпечної відмови ($T_{\text{НВ}}$)):

$$P(t) = P(T_{\text{НВ}} > t). \quad (2)$$

Імовірність безвідмовної роботи приймає значення від 0 до 1, при цьому, вона дорівнює одиниці в початковий момент часу й дорівнює нулю при часі, що наближається до нескінченності.

Імовірність небезпечної відмови ($P_{\text{НВ}}(t)$) – імовірність того, що відмова відбудеться за визначений час. Імовірність відмови доповнює імовірність безвідмовної роботи до повної групи подій:

$$P_{\text{НВ}}(t) = 1 - P(t). \quad (3)$$

Важливим припущенням є те, що інтенсивність відмов є сталою за часом, а час розподілений за експоненціальним законом.

Середній час напрацювання до небезпечної відмови визначається як визначений інтеграл в межах від нуля до нескінченності для імовірності безвідмовної роботи за часом:

$$T_{\text{НВ}}(t) = \int_0^{\infty} P(t)dt \,. \tag{4}$$

Коефіцієнт готовності $K_Г$ – імовірність того, що ПЗ лишиться в працездатному стані в будь-який довільний проміжок часу, крім запланованих періодів, протягом яких застосування ПЗ не передбачається. Розраховується коефіцієнт готовності, як відношення напрацювання до відмови до суми напрацювання до відмови та середнього часу відновлення після відмови ($T_{\text{В}}$)*:*

$$K_{\text{Г}} = \frac{T_{\text{НВ}}}{T_{\text{НВ}} + T_{\text{В}}} \,. \tag{5}$$

Оцінка показників ФБ визначається стандартом *IEC 60812:2006 Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)* [0].

Також необхідно враховувати, що в основу формування вимог до ФБ має бути покладено визначення переліку та характеристик потенційних загроз безпеці та встановлення можливих джерел їх виникнення.

Зовнішніми дестабілізуючими факторами, що впливають на ФБ ПЗ, є:

– навмисні, негативні впливи осіб з метою спотворення, знищення або розкрадання програм, даних та документів системи та ПЗ як наслідки порушення інформаційної безпеки, що відбиваються також на функціональній безпеці;

– помилки та несанкціоновані впливи оперативного, адміністративного та обслуговуючого персоналу в процесі експлуатації системи та ПЗ;

– спотворення в каналах телекомунікації інформації, що надходить від зовнішніх джерел та передається споживачам, а також неприпустимі значення та зміни характеристик потоків інформації від об'єктів зовнішнього середовища;

– збої та відмови в апаратному компоненті;

– віруси, що поширюються по каналам електронних комунікацій і впливають на інформаційну та функціональну безпеку;

– зміни складу та конфігурації комплексу взаємодіючої апаратури системи або ПС за межі, перевірені під час випробувань чи сертифікації.

До внутрішніх джерел загроз ФБ ПЗ відносяться:

– системні помилки при постановці цілей та завдань проектування функціональної придатності ПЗ та системи;

– дефекти та помилки при визначенні функцій, умов і параметрів зовнішнього середовища, в якому належить застосовувати програмні засоби і систему, що захищаються;

– алгоритмічні помилки проектування при безпосередньої алгоритмізації функцій забезпечення безпеки апаратури, програмних засобів та баз даних при визначенні структури та взаємодії компонентів функціональних комплексів програм, і навіть під час використання інформації баз даних;

– помилки та дефекти програмування в текстах програм та описах даних, а також у вихідної та результуючої документації на компоненти ПЗ;

– недостатня ефективність використовуваних методів та засобів оперативного захисту програм та даних, забезпечення безпеки функціонування та відновлення працездатності системи в умовах випадкових та навмисних негативних впливів від довкілля.

Повне усунення перелічених вище загроз ФБ ОЕКМ принципово неможливе.

Необхідно оцінювати вразливість функціональних компонентів системи для різних, негативних впливів та ступінь їх впливу на основні характеристики якості та безпеки, а також сумарний ризик. Залежно від цього слід розподіляти ресурси для створення системи та її компонентів. у результаті мають бути сформовані відповідні методи та контрзаходи, які,

своєю чергою, визначають необхідні функції та механізми засобів забезпечення працездатності та безпеки.

Контрзаходи – спеціалізовані системи та засоби, які включають сукупність взаємозалежних нормативних документів, організаційно-технічних заходів та відповідних їм методів та ПЗ, призначених для попередження та/або ліквідації негативних наслідків відмовних ситуацій, різних загроз безпеки, їх виявлення та локалізації. Створення таких комплексів підвищення безпеки передбачає планування та реалізацію цілеспрямованої політики комплексного забезпечення ФБ системи, а також ефективний розподіл ресурсів на контрзаходи та засоби Контрзаходи роблять для зменшення вразливостей та виконання політики безпеки. Але і після введення цих контрзаходів можуть зберігатися залишкові ризики, які допустимі внаслідок обмеженості ресурсів.

Для прямих кількісних вимірів ФБ необхідні інструментальні засоби, вбудовані в операційну систему або у відповідні компоненти та функції ПЗ. Ці засоби повинні в динаміці реального часу автоматично реєструвати відмовні ситуації, дефекти та спотворення обчислювального процесу програм та даних, що виявляються апаратним, програмно-алгоритмічним контролем або користувачами.

Накопичення та систематизація проявів відмов під час виконання програм дозволяє оцінювати основні показники безпеки, допомагає визначати причини збоїв та відмов та готувати дані для покращення ФБ ПЗ. Регулярна реєстрація та узагальнення таких даних сприяє усуненню ситуацій, що негативно впливають на ФБ та інші характеристики ПЗ.

Висновки. Отже основна відмінність між надійністю та ФБ ОЕКМ полягає у тому, що при оцінці значень ФБ враховуються тільки ті відмови, які призводять до зриву функціонування ОЕКМ. При створенні складних комплексів програм основне завдання полягає в виявленні дестабілізуючих факторів, а також у створенні методів та засобів зменшення їх впливу на ФБ. У результаті мають бути сформовані відповідні методи та контрзаходи, які, своєю чергою, визначають необхідні функції та механізми засобів забезпечення працездатності та ФБ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] G. J. Myers. *Software reliability: principles and practices*. New York, USA:Wiley, 1976.

[2] V. B. Mendiratta, “Reliability Analysis in Telecommunications”, *Notices of the American Mathematical Society,* vol. 67, no. 6, 2020, doi: http://doi.org/10.1090/noti2095.

[3] M. Sliwinski, E. Piesik, and J. Piesik, “Integrated functional safety and cyber security analysis”, *IFAC-PapersOnLine*, vol. 51, no. 24, pp. 1263-1270, 2018, doi: https://doi.org/10.1016/j.ifacol.2018.09.572.

[4] Г. М. Гулак, “Метод оцінювання функціональної безпеки інформаційних технологій для створення гарантоздатних автоматизованих систем”, *Кібербезпека: освіта, наука, техніка*, № 3 (7), 2020, doi: https://doi.org/10.28925/2663-4023.2020.7.153164.

[5] S. Kumari, R. Kumar, S. Kadry, S. Namasudra, and D. Taniar, “Maintainable stochastic communication network reliability within tolerable packet error rate”, *Computer Communications*, vol. 178, no. 1, pp. 166-168, 2021, doi: https://doi.org/10.1016/j.comcom.2021.07.023.

[6] C. Rajasimha, R. Arjun, and G. Chandrashekhar, “Supplemental FMEA for monitoring and system response of electronic power steering control system functional safety”, *SAE Technical Paper*, 2022, doi: https://doi.org/10.4271/2022-28-0404.

[7] V. Agrawal, B. Achuthan, A. Ansari, and V. Tiwari, “Threat / hazard analysis and risk assessment: a framework to align the functional safety and security process in automotive domain”, *SAE Int. J. Transp. Cyber. & Privacy*, vol. 4, no. 2, 2021, doi: https://doi.org/10.4271/2021-01-0148.

[8] G. Peserico, A. Morato, F. Tramarin, and S. Vitturi, “Functional safety networks and protocols in the industrial internet of things era”, *Sensors*, vol. 21, no. 18, 2021, doi: https://doi.org/10.3390/s21186073.
[9] IEC 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements. [Online]. Available: https://webstore.iec.ch/publication/5515. Accessed on: Feb. 19, 2023.
[10] Є. Бабешко, О. Ілляшенко, та В. Харченко. *Функційна безпека індустріальних систем. Стандарт IEC 61508*, Київ, Україна, 2019. [Електронний ресурс]. Доступно: https://tk185.appau.org.ua/whitepapers/aCampus-whitepaper-IEC-61508+++.pdf. Дата звернення: Січ. 11, 2023
[11] IEC 60812:2006 Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA). [Online]. Available: https://webstore.iec.ch/publication/3571. Accessed on: Jan. 05, 2023.

Стаття надійшла до редакції 27.04.23.

REFERENCES

[1] G. J. Myers. *Software reliability: principles and practices*. New York, USA:Wiley, 1976.
[2] V. B. Mendiratta, “Reliability Analysis in Telecommunications”, *Notices of the American Mathematical Society*, vol. 67, no. 6, 2020, doi: http://doi.org/10.1090/noti2095.
[3] M. Sliwinski, E. Piesik, and J. Piesik, “Integrated functional safety and cyber security analysis”, *IFAC-PapersOnLine*, vol. 51, no. 24, pp. 1263-1270, 2018, doi: https://doi.org/10.1016/j.ifacol.2018.09.572.
[4] G. M. Hulak, “The method of assessing the functional safety of information technologies for the creation of guarantee-capable automated systems”, *Cyber security: education, science, technology*, no. 3 (7), 2020, doi: https://doi.org/10.28925/2663-4023.2020.7.153164.
[5] S. Kumari, R. Kumar, S. Kadry, S. Namasudra, and D. Taniar, “Maintainable stochastic communication network reliability within tolerable packet error rate”, *Computer Communications*, vol. 178, no. 1, pp. 166-168, 2021, doi: https://doi.org/10.1016/j.comcom.2021.07.023.
[6] C. Rajasimha, R. Arjun, and G. Chandrashekhar, “Supplemental FMEA for monitoring and system response of electronic power steering control system functional safety”, *SAE Technical Paper*, 2022, doi: https://doi.org/10.4271/2022-28-0404.
[7] V. Agrawal, B. Achuthan, A. Ansari, and V. Tiwari, “Threat / hazard analysis and risk assessment: a framework to align the functional safety and security process in automotive domain”, *SAE Int. J. Transp. Cyber. & Privacy*, vol. 4, no. 2, 2021, doi: https://doi.org/10.4271/2021-01-0148.
[8] G. Peserico, A. Morato, F. Tramarin, and S. Vitturi, “Functional safety networks and protocols in the industrial internet of things era”, *Sensors*, vol. 21, no. 18, 2021, doi: https://doi.org/10.3390/s21186073.
[9] IEC 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements. [Online]. Available: https://webstore.iec.ch/publication/5515. Accessed on: Feb. 19, 2023.
[10] E. Babeshko, O. Ilyashenko, and V. Kharchenko, *Functional safety of industrial systems Standard IEC 61508*, Kyiv, Ukraine, 2019. [Online]. Available: https://tk185.appau.org.ua/whitepapers/aCampus-whitepaper-IEC-61508+++.pdf. Accessed on: Jan. 11, 2023.

[11] IEC 60812:2006 Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA). [Online]. Available: https://webstore.iec.ch/publication/3571. Accessed on: Jan. 05, 2023.

DMYTRO MOGYLEVYCH,
ROMAN SBOIEV

ANALYSIS OF FUNCTIONAL SAFETY OF ELECTRONIC COMMUNICATION SYSTEM EQUIPMENT

Today, the equipment of electronic communication networks (EECN) consists of two interconnected components. The first is hardware, the second is software, the normal functioning of each of which depends on the functioning of the network in general. One of the main concepts characterizing the network's ability to perform tasks as intended is functional safety (FS). This concept is similar to the concept of reliability, but differs mainly in that in the context of reliability, all possible failure situations are considered, and when considering FS, only those that lead to the failure of the certain system functioning. Failures are divided into four categories: detected safe and dangerous, undetected safe and dangerous. From the point of view of FS, only undetected dangerous ones are considered and constitute threats. According to the number of dangerous undetected failures, there are four levels of security completeness. The article also considers the main international standards, which provide definitions and quantitative characteristics of the main parameters of FS. So, the main parameters of FS include the system availability ratio, the average time to failure, and the probability of a dangerous undetected failure. At the same time, the mathematical apparatus of reliability theory can be applied in the analysis of FS. At the same time, the hardware component of EECN is quite widely researched, and the software component needs further study. Also, the FS of the software component is affected by a number of factors, both external and internal. The further task consists in the formation of methods and measures aimed at eliminating or reducing the impact of influencing factors. Also, since various types of software, mainly system software, are widely used in EECN, it is necessary to focus further research on it.

Keywords: functional safety, reliability, failures and rejections of software, equipment of electronic communication networks.

Могилевич Дмитро Ісакович, доктор технічних наук, професор, завідувач Спеціальної кафедри № 3, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-4323-0709, mogilevich4@gmail.com.

Сбоєв Роман Юрійович викладач Спеціальної кафедри № 3, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-7496-3737, roman.sboyev@gmail.com.

Mogylevych Dmytro, doctor of technical science, professor, chief of the Special department No. 3, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Sboiev Roman, teacher, of the Special department No. 3, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.