УДК 004.738.5:004.056 **doi: 10.32620/reks.2018.3.07**

Аль-Хафаджі Ахмед Валід

Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», Україна

РОЗРОБЛЕННЯ МЕТОДИКИ PSMECA АНАЛІЗУ ПРИ ЗАСТОСУВАННІ IoT КОМПОНЕНТІВ У СИСТЕМАХ ФІЗИЧНОЇ БЕЗПЕКИ

Системи фізичної безпеки використовуються для того, щоб завчасно попередити відомий вектор атак. В даній статті представлено дослідження та оцінювання систем фізичної безпеки використовуючи методику PSMECA (аналіз режимів, наслідків та критичності фізичної безпеки). ***Об'єктом*** *дослідження і аналізу є система фізичної безпеки Міністерства освіти і науки Іраку (як інфраструктура об'єктів регіону), а також територія компактного проживання студентів та співробітників. В даній роботі розглядаються питання організації систем фізичного захисту, які використовують пристрої з низьким енергоспоживанням і функціонують у середовищі Інтернету речей.* ***Метою*** *дослідження є опис та розроблення системи фізичної безпеки, яка функціонує у середовищі Інтернету речей, а також розроблення схеми досліджень і розробок моделей і методів аналізу ризиків, моделей функцій і компонентів, моделей відмов систем фізичної безпеки і проведення дослідження і аналізу виникнення відмов систем фізичної безпеки. Представлено узагальнену структурно-ієрархічна схема системи фізичної безпеки інфраструктури регіону, а також показано прикладне застосування схеми на прикладі система фізичної безпеки студентського містечку одного з університетів м. Багдад, Ірак. Функціональна схема моделювання об'єкту дослідження показана і базується на використанні мікрокомп'ютеру Raspberry Pi і мікроконтролеру Arduino. Представлені теоретико-множинні моделі функцій, компонентів і відмов досліджуваної системи, а також побудована проекція ієрархічної структури відмов в таблиці основних структурних елементів системи фізичної безпеки. IDEF0 діаграма, що показує сценарій відключення електричного живлення (випадкового або навмисного) у зв'язку підсистем освітлення і відеоспостереження, представлена. Схема процесу дослідження та розроблення моделей і методів аналізу ризиків систем фізичної безпеки проводиться у роботі. Побудована PSMECA таблиця для системи відеоспостереження, завдяки якій можна більш точно визначити причину виникнення відмови в системі фізичної безпеки та значення критичності відмови.*

Ключові слова: *PSMECA, FMECA, Raspberry Pi, атака, Інтернет речей, куб критичності, регіональна інфраструктура, система фізичної безпеки.*

Вступ

Актуальність теми дослідження. Стан розвитку і досягнень в науці та техніці, який дуже важко оцінити через гетерогенність ідей та рішень, став рушійною силою для створення безлічі науково-практичних розробок. Звичайно, що для сучасного світового суспільства, для цих інновацій необхідно враховувати такі життєві аспекти, як релігійний, політичний та соціально-культурний стани в країні, які часто впливають на розповсюдження науково-технічних рішень.

Якщо брати до уваги те, що об'єктивно безперечно існує набір позитивних сценаріїв використання науково-технічних досягнень, то також, звичайно, необхідно враховувати потенційно деструктивні дії та/або сценарії. Однією з систем, на котру такі руйнівні дії можуть бути спрямованими, є системи фізичної безпеки (англ. physical security systems, PSS) складних об'єктів (наприклад, будівлі державних установ, університети тощо).

Стан проблеми дослідження. Існує декілька визначень систем фізичної безпеки [1 – 3]. Найбільш розповсюдженим є «системи фізичної безпеки – це такі системи, що дозволяють контролювати та управляти доступом до певних об'єктів, і рівень їх функціонування є критичним показником в досягнені готовності систем» [2]. Також існує декілька підходів для забезпечення гарантоздатності та резільєнтності таких систем [4 – 6].

Отже, в рамках цієї дослідницької роботи, з однієї сторони, об'єктом дослідження є підсистеми фізичної безпеки регіональних інфраструктур, а з іншого боку – включає в себе кінцевий (детерміністичний) набір підсистем (компонентів), з яких система фізичної безпеки складається. Кожна підсистема (компонент) може бути представлена структурно у вигляді окремих елементів і зв'язків між ними.

Системи фізичної безпеки позиціонуються для того, щоб попередити завчасно відомий вектор атак,

шляхом використання існуючих розробок в галузі технічного захисту інформації та/або забезпечення фізичної безпеки. В даній роботі розглядаються аспекти забезпечення фізичної безпеки з використанням пристроїв з низьким рівнем енергоспоживання. Проте це потребує деякої зміни алгоритмів функціонування и взаємодії у рамках загальної системи забезпечення фізичної безпеки. Крім того, виникає завдання узгодження або позиціонування системи забезпечення безпеки з використанням пристроїв, що функціонують у середовищі Інтернету речей, в загальну систему забезпечення фізичної безпеки.

Постановка завдання

Постановка та формулювання завдання дослідження безпосередньо включає в себе саме дослідження функціонування систем фізичної безпеки. В дослідженнях [7 – 9] подано формулювання визначення систем фізичної безпеки та підходів до її забезпечення. В загальному випадку, системи фізичної безпеки можуть бути представлені відповідною підсистемою в межах інтегрованої системи безпеки установи (об'єкта, регіону). *Об'єктом дослідження і аналізу* є система фізичної безпеки об'єкту, що належить до Міністерства освіти і науки Іраку (як інфраструктура об'єктів регіону), а також територія компактного проживання студентів та співробітників, тобто студмістечко.

Крім того, в даному досліджені необхідно зібрати таку інформацію:

– типи відмов, що можуть статися в системі;

– як ці відмови розподіляються по підсистемам (компонентам) та їх елементами;

– яка ймовірність їх виникнення;

– наскільки високим є ризик успішної атаки на захищаємий об'єкт;

– скільки часу може знадобитися для відновлення нормального режиму роботи пошкодженої підсистеми (або її компонента);

– оцінку критичності кожного певного типу атак, які можуть бути набором (вектором) однієї та/або декількох відмов (сценарій відмов) за умови їх природного чи штучного виникнення;

– визначення достатніх та економічно ефективних контрзаходів для того, щоб усунути виявлені (або навіть перспективні) атаки, вразливості та загрози або ускладнити (або навіть унеможливити) їх експлуатацію зловмисниками [10].

Актуальна декомпозиція дійсної системи фізичного захисту певного об'єкта інфраструктури регіону може бути представлена шляхом групування компонентів та елементів у відповідності до особливостей технічної реалізації (рис. 1).

Після створення (проектування) структурно-ієрархічної схеми необхідно дослідити та проаналізувати поведінку системи та окремих елементів та взаємодії між ними протягом часу.

Таким чином, *метою* даної роботи є опис та розроблення системи фізичної безпеки, яка функціонує у середовищі Інтернету речей, а також розроб-

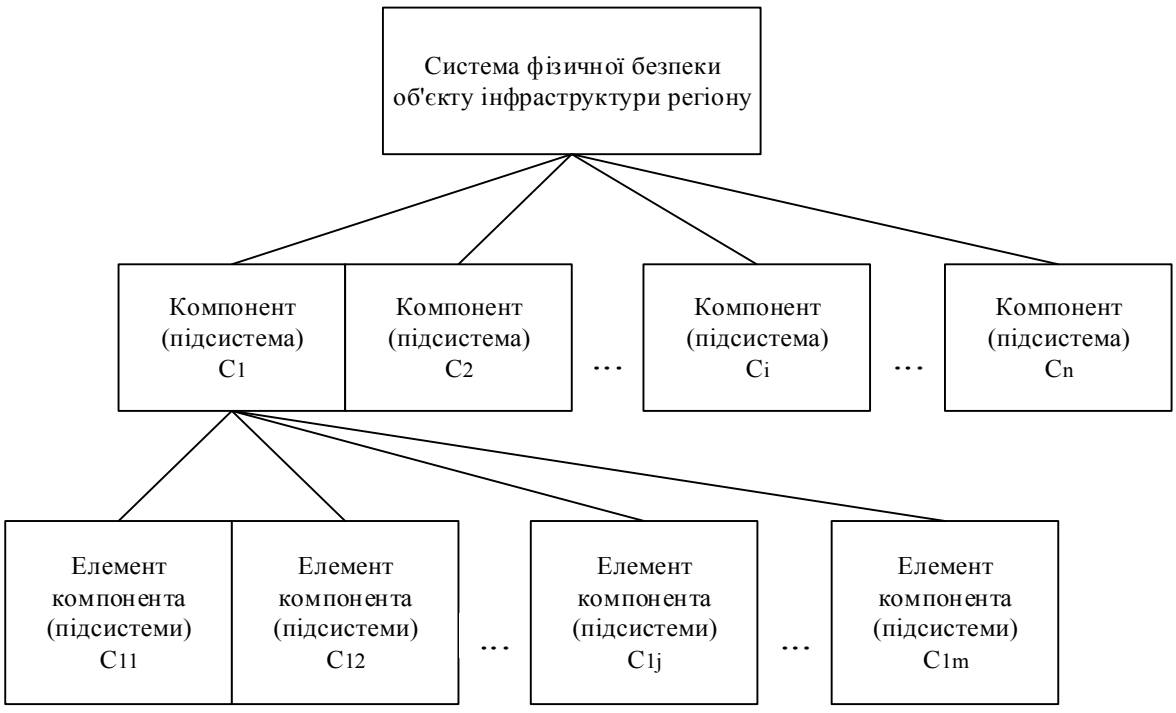

Рис. 1. Узагальнена структурно-ієрархічна схема системи фізичної безпеки інфраструктури регіону

лення схеми досліджень і розробок моделей і методів аналізу ризиків, моделей функцій і компонентів, моделей відмов систем фізичної безпеки і проведення дослідження і аналізу виникнення відмов систем фізичної безпеки.

Розроблення системи фізичної безпеки, що функціонує у середовищі Інтернету речей

Приклад практичної реалізації структурно-ієрархічної схеми системи фізичної безпеки об'єкта інфраструктури регіону може бути представлений сукупністю наступних підсистем:

– підсистема виявлення руху / вторгнення;
– підсистема контролю доступу;
– підсистема моніторингу 24/7;
– підсистема сигналізації / оповіщення;
– підсистема відеоспостереження (англ. Closed-Circuit Television, CCTV);
– підсистема освітлення;
– підсистема комунікацій тощо.

Узагальнену структурно-ієрархічна схему системи фізичної безпеки об'єкта інфраструктури регіону необхідно заповнити вищезгаданими підсистемами. Результат представлено на рис. 2. Для даного випадку, при моделюванні як прототип головного модуля використовується мікрокомп'ютер Raspberry Pi [11, 12].

Базова схема функціонування прототипу пристрою «Відеоспостереження» поєднує в собі комплекс апаратних та програмних компонентів, що дозволяє виявляти проблемні зони в системі фізичної безпеки (рис. 3). Функціонально прототип виконаний з малопотужного мікрокомп'ютера Raspberry Pi, підключеного до мережі досліджуваного об'єкта з набором зовнішніх датчиків, об'єднаних за допомогою радіочастотної ідентифікації (RFID) з можливістю ідентифікації дальньої дії (до 50 метрів [13]).

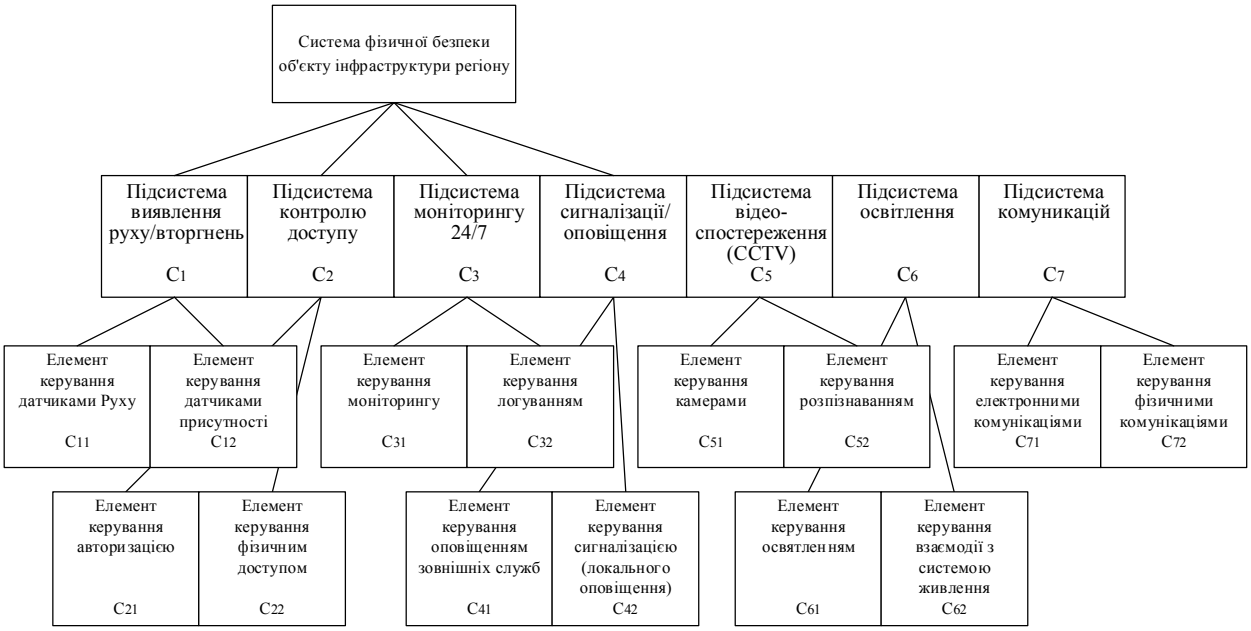

Рис. 2. Приклад прикладного застосування структурно-ієрархічної схеми системи фізичної безпеки інфраструктури регіону

Рис. 3. Функціональна діаграма пристрою «Відеоспостереження»

З точки зору забезпечення безпеки під час реалізації прототипу, основним джерелом загроз може бути канал передачі даних через RFID, що може дозволити зловмиснику отримати доступ до серверу та/або сенсорів. В якості криптокомпоненту пропонується використовувати алгоритм DESL, який є полегшеною версією алгоритму DES [14]. Через те, що розмір ключа шифрування має розмір 56 біт, існує загроза, що цей алгоритм буде зламано через декілька місяців. Тому його необхідно використовувати лише на етапі проектування, щоб перевірити функціональні можливості розробленої системи.

Поєднання можливостей Raspberry Pi і Arduino в одному прототипі дозволяє в найкоротший час за невелику вартість компонентів, енергоресурси і розроблення створити продукт, який спрямований на виконання певної функції в певному місці, перевірити спроможність системи забезпечити функціональну безпеку, надати перелік рекомендацій та процедур запланованих дій з створення дійсно повнофункціонального пристрою на основі більш захищених (дорогих) програмних та/або апаратних компонентів.

Для формального опису сценаріїв атаки (вторгнення) або каскадного відмови підсистем / елементів може бути застосовані CASE-засоби з можливістю опису процесів, що відбуваються в системі.

Для забезпечення наочності, сценарій відключення електричного живлення (випадкового або навмисного) у зв'язку підсистем освітлення і відеоспостереження, представлено на рис. 4.

Проведене дослідження і аналіз передбачає етап формалізації системи, що дозволить ідентифікувати і проаналізувати такі характеристики системи:

– всі потенційно можливі типи відмов компонентів (підсистем) системи;

– вплив цих відмов на функціонування системи;

– можливості (способи) запобігання відмов і / або усунення впливу відмов на функціонування системи.

З точки зору існуючих методологій, що дозволяють ефективно вирішувати подібні завдання і пов'язані з ними, необхідно виділити аналіз режимів, наслідків та критичності відмов (англ. Failure, Modes, Effects, and Criticality Analysis, FMECA). В даній роботі необхідно ввести для провадження аналізу режимів, наслідків та критичності фізичної безпеки термін PSMECA [15]. Тобто, наступним етапом є проведення PSMECA аналізу .

Прототипом об'єкта дослідження і аналізу є система фізичної безпеки студентського містечку одного з університетів м. Багдад, Ірак.

Моделі системи фізичної безпеки

Процес дослідження та розроблення моделей і методів аналізу ризиків систем фізичної безпеки проводиться по схемі, що представлена на рис. 5, де HW – апаратне забезпечення, SW – програмне забезпечення, HF – людський фактор, PIMECA – аналіз режимів, наслідків та критичності фізичних вторгнень (англ. Physical Intrusion Modes, Effects and Criticality Analysis), IIMECA – аналіз режимів, наслідків та критичності інформаційних вторгнень (англ. Information Intrusion Modes, Effects and Criticality Analysis). PIMECA та IIMECA є модифікаціями FMECA. Більш детальна інформація о можливих варіаціях FMECA-методів, які предназначені

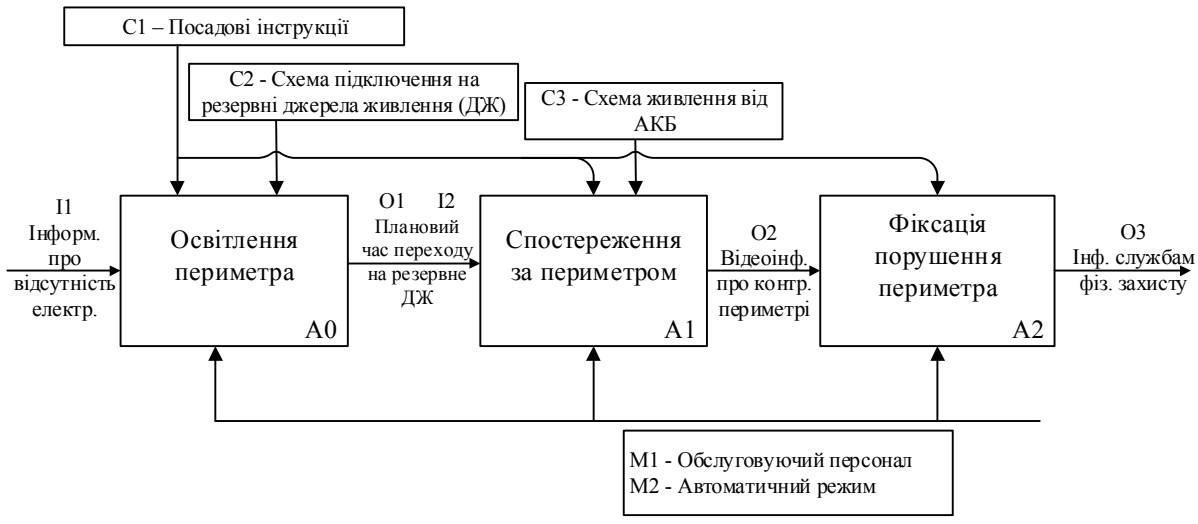

Рис. 4. IDEF0 діаграма впливу на PSMECA компоненти

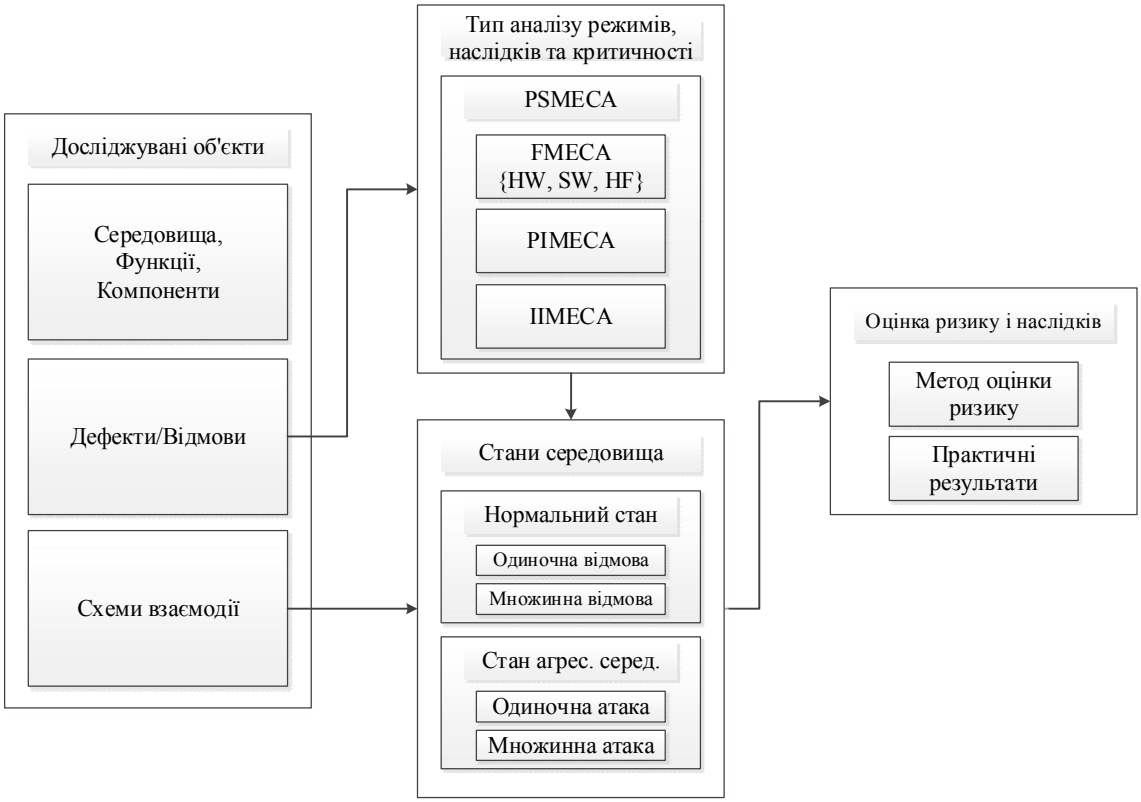

Рис. 5. Схема дослідження та розроблення моделей і методів аналізу ризиків систем фізичної безпеки

саме для виявлення проблем інформаційної та кібербезпеки у формі вторгнень у складні системи, представлена в роботах [10, 16, 17]. Питання вибору FMECA-методів та засобів для аналізу стану фізичної безпеки критичних систем наведено в [19].

Моделі функцій і компонентів системи фізичного захисту. Система фізичної безпеки (PSS) є частиною метасистеми (MS), яка в свою чергу включає в себе середовище системи (ES):

$$\mathrm{MS} = \{\mathrm{PSS}, \mathrm{ES}\}. \tag{1}$$

Система фізичної безпеки розроблюється для виконання функцій:

$$\mathrm{SFPSS} = \{\mathrm{FVis}, \mathrm{FVDet}, \mathrm{Finf}\}, \tag{2}$$

і складається з множини непересічних компонентів:

$$\mathrm{SCPSS} = \mathrm{CHF} \cup \mathrm{CHW} \cup \mathrm{CSW}, \tag{3}$$

де CHF – декілька компонентів (операторів) людського фактору, які важко формалізувати, CHW – декілька компонентів апаратного забезпечення, CSW – декілька компонентів програмного забезпечення. Для того, щоб виявити первинні причини відмов, перетин програмних і апаратних компонентів, людський фактор і апаратні компоненти, людський фактор і програмний компоненти визначаються як нуль:

$$\begin{aligned} \mathrm{CHF} \cap \mathrm{CHW} &= \varnothing, \\ \mathrm{CSW} \cap \mathrm{CHF} &= \varnothing, \\ \mathrm{CHW} \cap \mathrm{CSW} &= \varnothing. \end{aligned} \tag{4}$$

У свою чергу

$$\begin{aligned} \mathrm{CHW} &= \mathrm{CHWS} \cup \mathrm{CHWH}, \\ \mathrm{CHWS} \cap \mathrm{CHWH} &= \varnothing, \end{aligned} \tag{5}$$

де CHWS – підмножина апаратних (первинних) компонентів - медіа програмного забезпечення (пристрої зберігання, зберігання даних), CHWH - підмножина апаратних (вторинних) компонентів - відеокамери, датчики руху, присутності і т. д.

У свою чергу, залежність між програмним забезпеченням системи і застосунками може бути представлена як:

$$\begin{aligned} \mathrm{CSW} &= \mathrm{CSWS} \cup \mathrm{CSWA}, \\ \mathrm{CSWS} \cap \mathrm{CHWA} &= \varnothing, \end{aligned} \tag{6}$$

де CSWS – підмножина програмного забезпечення системи (операційних систем), CSWA - підмножина застосунків (спеціалізованого програмного забезпечення).

Середовище системи включає в себе фізичні компоненти (EPS) та інформаційні компоненти або підсистеми о (EIS). Підсистеми EPS та EIS розділено на природні (пасивні) підсистеми (EPNS та EINS) і штучні (активні або агресивні у відношенні до системи) – EPAS та EIAS.

З однієї сторони, середовище системи складається з фізичних і інформаційних компонентів

$$ES = \{EPS, EIS\}. \quad (7)$$

З другого боку, це можна представити у формі їх станів середовища – нормальний (ENS) або агресивний (EAS)

$$ES = \{ENS, EAS\}. \quad (8)$$

Іншими словами, середовище може бути описано як декартів добуток

$$ES = \{EPS, EIS\} \times \{ENS, EAS\} = \\ = \{EPNS, EINS, EPAS, EINS\}. \quad (9)$$

Відображення ΩEC множин підсистем функцій середовища (2) на множині компонентів (3), яка може бути представлена у вигляді

$$\Omega EC : SFPSS \to SCPSS, \quad (10)$$

що описується булевою матрицею BEC, з наступними значеннями – 0, якщо немає впливу (залежності); 1, якщо є вплив; Ø, якщо природа показників різна.

Відображення ΩEF множин підсистем функцій середовища (2) на множині компонентів (3), яка може бути представлена у вигляді

$$\Omega FC : SFPSS \to SCPSS, \quad (11)$$

що описується булевою матрицею BFC з наступними значеннями:

0 – якщо немає впливу (залежності);

1 – якщо є вплив;

Ø – якщо природа показників різна.

Моделі відмов системи фізичної безпеки. У відповідності до [4, 6], відмови можна класифікувати як фізичні (pf), проектні (df), операторні (hf) і взаємодії (if).

Відповідно, кількість відмов SDPSS системи фізичної безпеки складається з непересічних підпросторів

$$SDPSS = SDpf \cup SDdf \cup SDhf \cup SDif, \quad (12)$$

і

$$SDpf \cap SDdf = \varnothing,\ SDdf \cap SDif = \varnothing, \\ SDpf \cap SDif = \varnothing, ... \quad (13)$$

Неперетинання підмножин відмов означає, що вони стосуються різних причин виникнення, але не наслідків.

Беручи до уваги (7),

$$SDPSS = SDpf \cup SDdf \cup SDhpf \cup \\ \cup SDhf \cup SDif \cup SDiif. \quad (14)$$

Помилки, зв'язані з діями операторів, також можуть бути поділені на ті, які приводять до фізичного дефекту (hpf) або інформаційного порушення (hif).

В цьому випадку

$$SDPSS = SDpf \cup SDdf \cup SDhpf \cup \\ \cup SDhif \cup SDipf \cup SDiif. \quad (15)$$

Відображення ΩDC множини системних відмов SDPSS на множині компонентів SCPSS:

$$\Omega DC : SDPSS \to SCPSS, \quad (16)$$

що описується булевою матрицею BDC, з наступними значеннями: 0 – якщо немає впливу (залежності); 1 – якщо є вплив; Ø – якщо природа показників різна.

Дослідження і аналіз виникнення відмов систем фізичної безпеки. На даному етапі необхідно визначити унікальність відповідності відмов, що виникають у системі фізичної безпеки (фактично – порушення в реалізації функцій, які зазначені у проекті системи) і компонентів цієї системи (необхідних для виконання функцій). Таким чином, беручи до уваги існування відмов різного типу (апаратних, програмних, людського фактору, тощо), шукані відповідності представлено як проекцію ієрархічної структури в таблиці основних структурних елементів системи фізичної безпеки (табл. 1).

Побудова таблиці обумовлена необхідністю обґрунтування формального підтвердження (доказу) причини включення різних типів компонентів у сформовану матрицю відмов. PSMECA таблиця містить в собі інформацію з двох таблиць FMECA і

Таблиця 1

Проекція ієрархічної структури відмов в таблиці основних структурних елементів системи фізичної безпеки

	PSMECA							
	FMECA				IMECA			
	pf	df	hf		if			
			hpf	hif	ipf		iif	
					ip(nf)	ip(a)f	ii(n)f	ii(a)f
HW	1	1	1	1	1	1	0	1
SW	0	1	0	1	0	1	1	1
OP	Ø	Ø	1	1	1	1	1	1

IMECA. Це розписано у формулах (1) – (16) і дозволяє формалізувати різні типи появи відмов. Реалізацію такого підходу представлено в табл. 2 і 3.

З огляду на динамічний характер відмов у системі фізичної безпеки існує необхідність визначення множини сценаріїв. Множина сценаріїв (SScen) складається з різних послідовностей подій, які ведуть до відмови. Таким чином, беручи до уваги сценарії динамічної появи відмов в досліджуваній системі фізичної безпеки:

$$SScen = \sum SSceni,\ i = 1,...,n, \qquad (17)$$

з урахуванням показнику часу (t).

Таким чином, розроблена формалізація ієрархічної структури відмов у зв'язці з джерелом появи відмов, дозволяє створювати PSMECA таблиці на базі теоретико-множинної моделі компонентів системи фізичної безпеки.

Побудова PSMECA таблиці

Приклад PSMECA таблиці для CCTV підсистеми, що функціонує в нормальному режимі. Процес створення PSMECA таблиць починається з розроблення подібних (базових або початкових) FMECA таблиць, які модифікуються відповідно до розробленої теоретико-множинної моделі компонентів системи фізичної безпеки. Основною метою такої модифікації є поглиблення структури аналізованих джерел відмов системи, щоб забезпечити більш строго формалізований підхід, заснований на додаткових елементах структури та рівнях ієрархії, як показано у табл. 1. Таким чином, для даного прикладу, першим шагом буде розроблення FMECA таблиці підсистеми відеоспостереження. Таблиця 2 представляє собою FMECA таблицю, де P – ймовірність, S – тяжкість, M – ремонтопридатність, C – критичність. Показники ймовірності, тяжкості і

Таблиця 2

FMECA таблиця для CCTV підсистеми, що функціонує в нормальному режимі

Підсистема	**Тип відмови**	**Режим відмови**	**Причина відмови**	**Наслідок відмови**	**P**	**S**	**M**	**C**
Елемент керування камерами	HW	Не запускається	Помилка установки або аварійне припинення (переривання)	Моніторинг руху в межах контрольованого периметру вимкнено	L	H	L	H
		Неправильне функціонування			M	M	M	M
	SW	Не працює	Помилка персоналу або проектна помилка		L	H	M	H
		Немає відгуку			L	M	M	M
Елемент керування розпізнаванням	HW	Не запускається	Помилка установки або аварійне припинення (переривання)	Несанкціонований доступ до захищеної зони	L	H	L	H
		Неправильне функціонування			M	M	M	M
	SW	Неправильне функціонування	Помилка персоналу або проектна помилка		L	M	M	M

Таблиця 3

PSMECA таблиця для CCTV підсистеми, що функціонує в нормальному режимі

Підсистема	Тип відмови				Режим відмови	Причина відмови	Наслідок відмови	P	S	M	C
Елемент керування камерами	HW	pf			Не запускається	Помилка установки або аварійне припинення (переривання)	Моніторинг руху в межах контрольованого периметру вимкнено	L	H	L	H
		df						L	H	L	H
		hf	hpf		Неправильне функціонування			M	H	L	H
			hif					M	M	M	M
		if	ipf	ip(n)f				L	L	L	L
				ip(a)f				L/M	L	M	M
			iif	ii(a)f				L/M	H	H	H
	SW	df			Не працює	Помилка персоналу або проектна помилка		L	H	M	H
		hf	hif		Немає відгуку			L	M	M	M
		if	ipf	ip(a)f				L/M	H	M	H
			iif	ii(n)f				L	L	M	M
				ii(a)f				L/M	H	H	H
Елемент керування розпізнаванням	HW	pf			Не запускається	Помилка установки або аварійне припинення (переривання)	Несанкціонований доступ до захищеної зони	L	H	L	H
		df						L	H	L	H
		hf	hpf		Неправильне функціонування			M	H	L	H
			hif					M	M	M	M
		if	ipf	ip(n)f				L	L	L	L
				ip(a)f				L/M	L	M	M
			iif	ii(a)f				L/M	H	H	H
	SW	df			Неправильне функціонування	Помилка персоналу або проектна помилка		L	H	M	H
		hf	hif					L	M	M	M
		if	ipf	ip(a)f				L/M	H	M	H
			iif	ii(n)f				L	L	M	M
				ii(a)f				L/M	H	H	H

ремонтопридатності коливаються від низького (L) через середнє (M) до високого (H) і оцінювання здійснюється експертами. Результуючий рівень критичності (C) вказується максимальним діапазоном ймовірності, ступеня тяжкості та ремонтопридатності для відповідного режиму аварії. Такі нечіткі значення (низьке (L), середнє (M), високе (H) обираються лише для демонстрації можливостей реалізації розробленого підходу без зайвого ускладнення обчислень.

FMECA таблиця для підсистеми відеоспостереження, що функціонує в нормальному режимі повинна бути модифікована у схожу PSMECA таблицю у відповідності до теоретико-множинної моделі компонентів системи фізичної безпеки (табл. 3). Показники ймовірності, тяжкості і ремонтопридатності оцінюються експертами. Ймовірність для PSMECA встановлюється як низька (L), низька у середню (L/M), середня (M) і висока (H). Для тяжкості і ремонтопридатності використовується такі ж самі значення (низьке, середнє, високе) як і у попередньому випадку.

Розроблена PSMECA таблиця може використовуватися для встановлення більш детальних причинних зв'язків між підсистемами, їх типами відмов та ризиками безпеки PSS.

Графічне представлення PSMECA таблиці у вигляді кубу критичності для розглянутого випадку представлено на рис. 6, де P – вісь зі значеннями ймовірності відмови, S – вісь зі значеннями тяжкості відмови і M – вісь зі значеннями ремонтопридатності. На рис. 7 представлено значення показників та їх графічне представлення у відповідності до кубу критичності.

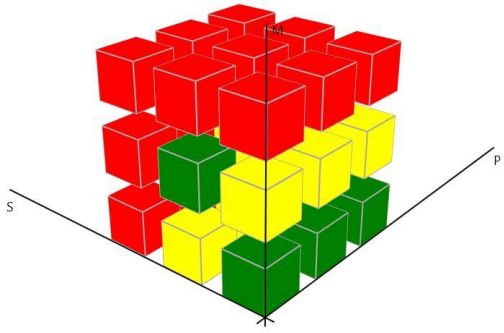

Рис. 6. Представлення PSMECA таблиці у вигляді кубу критичності

Таким чином, на основі результатів табл. 3, отриманої із табл. 2, можна більш точно визначити причину виникнення відмови в системі фізичної безпеки та значення критичності відмови.

Результати PSMECA аналізу. Запропонована методика оцінювання поєднує в собі дві відомі методики (FMECA і IMECA), беручи до уваги особливості систем фізичної безпеки.

Ймовірність відмови	Тяжкість відмови		
	Низька	Середня	Висока
Низька	L	M	H
Середня	M	M	H
Висока	H	H	H

Рис. 7. Значення показників та їх графічне представлення у PSMECA таблиці

Особливостями PSMECA методики є:

– методика заснована на аналізі компонентів і відмов системи у відповідності до множини SDPSS, враховуючи, що SDipf і SDiif декомпозовані на підмножини відмов, викликаними пасивними причинами (n) і агресивним середовищем (f), тобто ip(n)f та ip(a)f, ii(n)f та ii(a)f. Таблиця 1 ілюструє відмови для різних компонентів (апаратні, програмні і людський фактор);

– результати аналізу представлені множиною рядків, що описується вектором <компонент, тип відмови, режим, причина і наслідки відмови з точки зору безпеки PSS, ймовірність P, тяжкість S та складність (час та кошти) на відновлення Crec>:

$$\text{PSS security Risk} = \text{Prob} * \text{Sev} * \text{Crec}. \qquad (18)$$

– з урахуванням запропонованої структури PSS та платформи (рис. 2, 4), ієрархічна PSMECA може бути застосована, яка складається з FMECA / IMECA (HF/IME(C)A), що показано в табл. 2-3.

Висновки

Отже, на підставі дослідження систем фізичної безпеки були отримані наступні результати:

– розроблена структурна та функціональна декомпозиція системи фізичної безпеки;

– запропоновані прикладні рішення для реалізації стандартних функцій підсистем у об'єкті дослідження, а деякі з них були розглянуті в роботі;

– проаналізовано теоретико-множинну модель компонентів, середовища і відмов системи фізичної безпеки, а також основні результати методики PSMECA оцінювання.

Слід зауважити, що стаття описує лише статичну систему. Перш ніж проводити оцінку в динаміці, необхідно розглянути сценарії атаки. У випадку динамічного процесу слід провести апостеріорний аналіз, тобто, якщо є певна подія (режим відмови), необхідно переглянути критичність наслідку відмови на підсистему та систему та провести PSMECA аналіз ще раз.

Майбутні дослідження можуть бути направленні на розроблення сценаріїв фізичних та кібератак, включаючи багатоступінчасті втручання та множинні відмови, враховуючи ці обставини під час реалізації PSMECA в динаміці.

Література

1. Павлов, Д. М. Забезпечення фізичної безпеки ядерних об'єктів в Україні в умовах зростання військово-терористичної загрози: організаційно-правовий аспект [Текст] / Д. М. Павлов // Юридична наука. – 2015. – № 2. – С. 21–27.

2. Niles, S. Physical Security in Mission Critical Facilities [Text] / Suzanne Niles // Schneider Electric. – 2004. – 22 p.

3. Physical Security Systems [Text] // Hitachi Review. – 2004. – Vol. 53, № 2. – P. 73–78.

4. Basic concepts and taxonomy of dependable and secure computing [Text] / A. Avizienis, J. Laprie, B. Randell, C. Landwehr // IEEE Transactions on Dependable and Secure Computing. – 2004. – №1. – P. 11–33.

5. Yastrebenetsky, V. Nuclear Power Plants Instrumentation and Control Systems for Safety and Security [Text] / V. Yastrebenetsky, V. Kharchenko. – Hershey PA, USA, 2014. – 470 p. – (IGI Global).

6. Qahtan Abdulmunem, M. Availability and Security Assessment of Smart Building Automation Systems: Combining of Attack Tree Analysis and Markov Models [Text] / M. A.-S. Qahtan Abdulmunem, V. Kharchenko // Proceedings of Third International Conference on Mathematics and Computers in Sciences and in Industry. – 2016. – P. 302–307.

7. Charlie, F. Physical Protection Principles [Text] / F. Charlie, M. Brayon // Nuclear Installation Dept. AELB. – 2014. – 10 p.

8. Harris, S. Physical and Environmental Security. [Text] / S. Harris // CISSP Exam Guide. – 2013. – P. 457–502.

9. Conrath, J. Structural Design for Physical Security: State of the Practice [Text] / J. Conrath. – ASCE Reston: Task Committee, Structural Engineering Institute, 1999. – 264 p.

10. Security Informed Safety Assessment of NPP I&C Systems: GAP-IMECA Technique [Text] / V. S. Kharchenko, O. A. Illiashenko, A. A. Kovalenko, V. V. Sklyar // International Conference on Nuclear Engineering. – 2014. – 9 p.

11. Monk, S. Programming the Raspberry Pi: Getting Started with Python [Text] / S. Monk. – McGraw Hill Professional, 2015. – 192 p.

12. Blum, J. Exploring Arduino: Tools and Techniques for Engineering Wizardry [Text] / J. Blum. – Jonh Willey & Sons, 2013. – 384 p.

13. Wireless Sensor Node with Passive RFID for Indoor Monitoring System [Text] / N. M. Nadzir, M. Rahim, F. Zubir et al. // International Journal of Electrical & Computer Engineering. – 2017. – P. 1459–1466.

14. New Light-Weight Crypto Algorithms for RFID [Text] / A. Poschmann, G. Leander, K. Schramm, C. Paar // IEEE International Symposium on Circuits and Systems. – 2007. – P. 1843–1846.

15. IoT-based physical security systems: Structures and PSMECA analysis [Text] / A. K. A. Waleed, V. Kharchenko, D. Uzun, O. Solovyov // IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). – 2017. – P. 870–873.

16. F(I)MEA-technique of Web Services Analysis and Dependability Ensuring [Text] / A. Gorbenko, V. Kharchenko, O. Tarasyuk, A. Furmanov // Lecture Notes in Computer Science. – 2006. – Vol. 4157. – P. 153–167.

17. Babeshko, E. Applying F(I)MEA-technique for SCADA-based Industrial Control Systems Dependability Assess-ment and Ensuring [Text] / E. Babeshko, V. Kharchenko, A. Gorbenko // Third International Conference on Dependability of Computer Systems DEPCOS-RELCOMEX – 2008. – P. 309–315.

18. Illiashenko, O. Choosing FMECA-based techniques and tools for safety analysis of critical systems [Text] / O. Illiashenko, E. Babeshko // Information & Security: An International Journal. – 2012. – No. 28(2). – P. 275–285.

References

1. Pavlov, D. M. Zabezpechennya fizychnoyi bezpeky yadernykh ob"yektiv v Ukrayini v umovakh zrostannya viyskovo-terorystychnoyi zahrozy: orhanizatsiyno-pravovyy aspect [Physical security of nuclear facilities in Ukraine in terms of growth of military-theoretical threat, organizational and legal aspects]. *Yurydychna nauka – Jurisprudence*, 2015, no. 2, pp. 21–27. (in Ukrainian).

2. Niles, S. Physical Security in Mission Critical Facilities. *Schneider Electric*, 2004. 12 p.

3. Physical Security Systems. *Hitachi Review*, 2004, vol. 53, no. 2, pp. 73–78.

4. Avizienis, A., Laprie, J., Randell, B., Landwehr, C. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 2004, no. 1, pp. 11–33.

5. Yastrebenetsky, V., Kharchenko, V. *Nuclear Power Plants Instrumentation and Control Systems for Safety and Security*. Hershey PA, USA, 2014. 470 p.

6. Qahtan Abdulmunem, M. A.-S., Kharchenko, V. Availability and Security Assessment of Smart Building Automation Systems: Combining of Attack Tree Analysis and Markov Models. *Proceedings of Third International Conference on Mathematics and Computers in Sciences and in Industry*, 2016, pp. 302–307.

7. Charlie, F., Brayon, M. *Physical Protection Principles*. Nuclear Installation Dept. AELB, 2014. 10 p.

8. Harris, S. *Physical and Environmental Security*. CISSP Exam Guide, 2013, pp. 457–502.

9. Conrath, J. *Structural Design for Physical Security: State of the Practice*. ASCE Reston: Task Committee, Structural Engineering Institute, 1999. 264 p.

10. Kharchenko, V. S., OIlliashenko, O. A., Kovalenko, A. A., Sklyar, V. V. Security Informed Safety Assessment of NPP I&C Systems: GAP-IMECA Technique. *International Conference on Nuclear Engineering*, 2014. 9 p.

11. Monk, S. *Programming the Raspberry Pi: Getting Started with Python*. McGraw Hill Professional, 2015. 192 p.

12. Blum, J. Exploring Arduino: *Tools and Techniques for Engineering Wizardry*. Jonh Willey & Sons, 2013. 384 p.

13. Nadzir, N. M., Rahim, M. K. A., Zubir, F., Zabri, A., Majid, H. A. Wireless Sensor Node with Passive RFID for Indoor Monitoring System. *International Journal of Electrical & Computer Engineering*, 2017, pp. 1459–1466.

14. Poschmann, A., Leander, G., Schramm, K., Paar, C. New Light-Weight Crypto Algorithms for RFID. *IEEE International Symposium on Circuits and Systems*, 2007, pp. 1843–1846.

15. Walled, A. K. A., Kharchenko, V., Uzun. D., Solovyov, O. IoT-based physical security systems: Structures and PSMECA analysis. *IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, 2017, pp. 870–873.

16. Gorbenko, A., Kharchenko, V., Tarasyuk, O., Furmanov, A. F(I)MEA-technique of Web Services Analysis and Dependability Ensuring. *Lecture Notes in Computer Science*, 2006, vol. 4157, pp. 153–167.

17. Babeshko, E., Kharchenko, V., Gorbenko, A. Applying F(I)MEA-technique for SCADA-based Industrial Control Systems Dependability Assessment and Ensuring. *Third International Conference on Dependability of Computer Systems DEPCOS-RELCOMEX,* 2008, pp. 309–315.

18. Illiashenko, O. Babeshko, E. Choosing FMECA-based techniques and tools for safety analysis of critical systems. *Information & Security: An International Journal*, 2012, no. 28(2), pp. 275–285.

Поступила до редакції 1.09.2018, розглянута на редколегії 12.09.2018

РАЗРАБОТКА МЕТОДИКИ PSMECA АНАЛИЗА ПРИ ИСПОЛЬЗОВАНИИ IoT КОМПОНЕНТОВ В СИСТЕМАХ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

Аль-Хафаджи Ахмед Валид

Системы физической безопасности используются для того, чтобы заблаговременно предупредить известный вектор атак. В данной статье представлен анализ исследования и оценки систем физической без-

опасности используя методику PSMECA (анализ режимов, последствий и критичности физической безопасности). *Объектом исследования* и анализа является система физической безопасности Министерства образования и науки Ираке (как инфраструктура объектов региона), а также территория компактного проживания студентов и сотрудников. В данной работе рассматриваются вопросы организации систем физической защиты, которые используют устройства с низким энергопотреблением и функционируют в среде Интернета вещей. *Целью исследования* является описание и разработка системы физической безопасности, которая функционирует в среде Интернета вещей, а также разработка схемы исследований и разработок моделей и методов анализа рисков, моделей функций и компонентов, моделей отказов систем и проведения исследования и анализа возникновения отказов систем физической безопасности. Представлена общая структурно-иерархическая схема системы физической безопасности инфраструктуры региона, а также показано прикладное применение схемы на примере система физической безопасности студенческого городка одного из университетов г. Багдад. Функциональная схема моделирования объекта представлена и базируется на использовании микрокомпьютера Raspberry Pi и микроконтроллера Arduino. Представленные теоретико-множественные модели функций, компонентов и отказов исследуемой системы, а также построена проекция иерархической структуры отказов в таблице основных структурных элементов системы физической безопасности. Представлена IDEF0 диаграмма, показывающая сценарий отключения электропитания (случайного или преднамеренного) в связи подсистем освещения и видеонаблюдения, Схема процесса исследования и разработки моделей и методов анализа рисков систем физической безопасности проводится в работе. Построена PSMECA таблица для системы видеонаблюдения, благодаря которой можно более точно определить причину возникновения отказа в системе физической безопасности и значение критичности отказа.

Ключевые слова: PSMECA, FMECA, Raspberry Pi, атака, Интернет вещей, куб критичности, региональная инфраструктура, система физической безопасности.

DEVELOPMENT OF PSMECA ANALYSIS TECHNIQUE APPLYING IoT COMPONENTS IN PHYSICAL SECURITY SYSTEMS

Al-Khafaji Ahmed Waleed

Physical security systems are applied to alert in advance a well-known vector of attacks. This paper presents an analysis of the research and assessment of physical security systems applying the PSMECA technique (analysis of modes, efforts, and criticality of physical security). The object of research and analysis is the physical security system of the Ministry of Education and Science of Iraq (as the infrastructure of the region's objects), as well as the area of the compact living of students and co-workers (campus). This paper discusses the organization of physical security systems, which are based on devices with low power consumption and function in the Internet of things environment. The main aim is to describe and develop a physical security system that functions in the Internet of things environment, as well as the development of a scheme for the research and development of models and methods for risk analysis, models of functions and components, models of failures and conducting research and analysis of occurrence failures of PSS. The generalized structural and hierarchical scheme of the physical security system of the infrastructure of the region is presented, as well as the applied application of the scheme is illustrated by the example of the physical security system of a student campus of one of the universities of Baghdad. The functional modeling scheme of the object is provided and is based on the use of the Raspberry Pi microcomputer and the Arduino microcontroller. The set-theoretical models of functions, components, and failures of the system under study, as well as the projection of a hierarchical failure structure in the table of the basic structural elements of the system, are presented. The IDEF0 diagram, showing a power outage scenario (accidental or intentional) in connection with lighting and video subsystems, is presented. The scheme of research and development of models and methods of analysis of risks of PSS is carried out in the paper. A PSMECA table for the CCTV system has been created, which allows you to more precisely determine the cause of the failure in the physical security system and the importance of failure criticality.

Keywords: PSMECA, FMECA, Raspberry Pi, attack, Internet of Things, criticality cube, the infrastructure of the region, physical security system.

Аль-Хафаджі Ахмед Валід – здобувач кафедри комп'ютерних систем, мереж та кібербезпеки, Національний аерокосмічний університет «ХАІ», Харків, Україна, e-mail: eng_ahmed.waleed@yahoo.com.

Al-Khafaji Ahmed Waleed – PhD Candidate, Computer Systems, Networks and Cybersecurity of department, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine, e-mail: eng_ahmed.waleed@yahoo.com.