КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№4 (8), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.8.192201
УДК 004[056.53::413.4]

Цуркан Василь Васильович
к.т.н., доцент, старший науковий співробітник
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, Україна
ORCID: 0000-0003-1352-042X
v.v.tsurkan@gmail.com

МЕТОД ФУНКЦІОНАЛЬНОГО АНАЛІЗУВАННЯ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Анотація. Розглянуто процес функціонального аналізування стосовно систем управління інформаційною безпекою. Показано актуальність їх представлення множиною взаємопов'язаних функцій з внутрішніми та зовнішніми інтерфейсами. З огляду на це проаналізовано способи функціонального аналізування систем управління інформаційною безпекою. Серед них виокремлено графічну нотацію IDEF0. Такий вибір обумовлено можливістю відображення як інтерфейсів функцій, так й умов і ресурсів їх виконання. При цьому встановлено орієнтованість застосування графічної нотації IDEF0 здебільшого для представлення міжнародних стандартів серії ISO/IEC 27k, відображення основних стадій життєвого циклу систем управління інформаційною безпекою, розроблення окремих елементів систем управління інформаційною безпекою, зокрема, управління ризиком. Ці обмеження подолано завдяки методу функціонального аналізування систем управління інформаційною безпекою. Цьому передувало визначення теоретичних основ даного методу. Його використання дозволяє виокремлювати їх функції як на рівні системи, так і рівнях її структурних елементів (підсистем, комплексів, компонентів). Для цього визначається мета, точка зору та встановлюється управління інформаційною безпекою як основна діяльність. Вона відображається множиною ієрархічно взаємопов'язаних функцій, що представляються родинним деревом. Кожній функції цього дерева визначаються вхідні, вихідні дані, управління і механізми. Це дозволяє встановити їх відповідність організаційно технічній структурі на рівнях "діяльність-система", "процес-підсистема", "операція-модуль (комплекс)" і "дія-блок (компонент)". У перспективах подальших досліджень планується на основі запропонованого методу функціонального аналізування визначити ієрархію функцій та розробити логічну структуру систем управління інформаційною безпекою.

Ключові слова: функція; ієрархія функцій; функціональне аналізування, система управління інформаційною безпекою, IDEF0.

1. ВСТУП

Функціональне аналізування орієнтоване на представлення систем управління інформаційною безпекою множинною взаємопов'язаних функцій. Кожна з них характеризується наявністю внутрішніх і зовнішніх інтерфейсів, що виникають при їх взаємодії. Вони можуть розкладатися на функції нижчих рівнів відповідно до структурних елементів систем управління інформаційною безпекою, наприклад: підсистем, комплексів, компонентів. Для кожної функції визначається реакція на подразник стосовно задоволення потреб з боку зацікавлених сторін. У даному випадку подразник тлумачиться як внутрішній інтерфейс (вхід або вхідні дані), а реакція – зовнішній інтерфейс (вихід або вихідні дані) функції структурного елементу. При цьому враховуються умови та ресурси реакції на подразник. Це дозволяє встановити

послідовність виконання функцій системами управління інформаційною безпекою на рівні структурних елементів [1], [2].

Постановка проблеми. Серед способів функціонального аналізування виокремлюються такі представлення [2] - [5]: функцій, IDEF0; робіт IDEF3, BPMN, ARIS; даних, DFD. Результати їх зіставлення стосовно можливості відображення функції, її інтерфейсів, умов і ресурсів зведено в табл. 1. З огляду на неї, для функціонального аналізування систем управління інформаційною безпекою доцільно обрати спосіб представлення функцій у графічній нотації IDEF0.

Таблиця 1

Способи функціонального аналізування систем управління інформаційною безпекою

№ з/с	Спосіб функціонального аналізування	Функція	Інтерфейс функції		Умови виконання функції	Ресурси виконання функції
			Внутрішній	Зовнішній		
1.	IDEF0	+	+	+	+	+
2.	IDEF3	–	+	+	–	–
3.	ARIS	+	+	+	–	–
4.	BPMN	–	+	+	–	–
5.	DFD	+	+	+	–	–

Однак, застосовність графічної нотації IDEF0 на практиці зводиться до, по-перше, формалізованого представлення настанов міжнародних стандартів серії ISO/IEC 27k [6] - [13]; по-друге, відображення основних стадій життєвого циклу систем управління інформаційною безпекою [7] - [9]; розроблення окремих елементів систем управління інформаційною безпекою, наприклад [14], [15], управління ризиком. Поза увагою залишається аспект виокремлення їх функцій як на рівні системи, так і рівнях її структурних елементів (підсистем, комплексів, компонентів) [2].

Аналіз останніх досліджень і публікацій. Використання графічної нотації IDEF0 для представлення організаційно-технічних систем набором функцій запропоновано в [1], [5]. Таке представлення використовуються як підґрунтя для прийняття рішень про їх вдосконалення або розроблення нових [5]. Окремі аспекти дослідження систем управління інформаційною безпекою викладено в [6] - [15]. Зокрема, представлення базових положень міжнародних стандартів, залежностей між ними єдиною структурною формою у графічній нотації IDEF0 розкрито в [7] - [9]. Цією формою відображено основні стадії життєвого циклу систем управління інформаційною безпекою за моделлю PDCA (англ. “Plan – Do – Check – Act”). Насамперед розроблення, впровадження, функціонування, контролювання, удосконалювання. Тоді як у [10] розглядається розроблена система через обирання засобів захисту та місць їх впровадження. Дослідження захищеності побудовою функціональної моделі на основі багатоагентного підходу розкривається у [11]. Дане завдання вирішено з огляду на такі аспекти як відображення процесу впровадження і використання нормативних документів зі забезпечення інформаційної безпеки, зокрема, ISO/IEC 27001, та аналізування захищеності тестами на проникнення. Розробленню системи управління ризиком як одного з основних елементів систем управління інформаційною безпекою приділено увагу в [14], [15]. Графічною нотацією IDEF0 формалізовано субдіяльність зі управління ризиком завдяки визначенню мети, точки зору, набору функцій даної системи. Для кожної функції встановлено вхідні, вихідні дані; умови виконання і ресурси. Методику побудови систем управління інформаційною безпекою відповідно до настанов міжнародних стандартів серії ISO/IEC 27k розкрито в [12]. При цьому

ISSN 2663 - 4023

виокремлено аспект їх інтегрування з впровадженими комплексними системами захисту інформації. Функціональну модель системи забезпечення інформаційної безпеки в аспекті документування викладено в [13]. Її представлено набором документів і залежностей між ними. За основу такого викладення взято додаток А міжнародного стандарту ISO/IEC 27002.

Мета статті. визначення функцій систем управління інформаційною безпекою методом їх функціонального аналізування.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Теоретичною основою методу функціонального аналізування систем управління інформаційною безпекою є такі компоненти графічної нотації IDEF0 [5], [16]: лексика та граматика. Це обумовлено тим, що представленнями в даній нотації відображається інформація за аналогією з природньою мовою. Лексикою визначаються основні її елементи, а граматикою – правила використання.

Лексика мови IDEF0, L, визначається тріадою попарно неперетинних зліченних множин

$$L = (B, S, J) \tag{1}$$

де B – множина блоків, S – множина сегментів стрілок, J – множина стиків.

Основним поняттям при визначенні граматики з урахуванням (1) є граф IDEF0. Він тлумачиться як орієнтований граф

$$G = (V_G, E_G), \tag{2}$$
$$V_G = \bigcup\{B_G, S_G, J_G),$$
$$E_G = \bigcup\{I_G, C_G, O_G, M_G, L_G, R_G),$$

де V_G – множина вершин (блоків, сегментів стрілок, стиків), E_G – множина дуг, B_G – підмножина множини B ($B_G \subseteq B$), S_G – підмножина множини S ($S_G \subseteq S$), J_G – підмножина множини J ($J_G \subseteq J$), I_G, C_G, M_G – попарно неперетинні підмножини множини $S_G \times B_G$ способів з'єднань сегменту вхідної стрілки з блоком, O_G – підмножина множини $B_G \times S_G$ способів з'єднань блоку зі сегментом вихідної стрілки ($O_G \subseteq B_G \times S_G$), L_G – підмножина множини $S_G \times J_G$ з'єднань сегменту стрілки зі стиком ліворуч ($L_G \subseteq S_G \times J_G$), R_G – підмножина множини $J_G \times S_G$ з'єднань стику зі сегментом стрілки праворуч ($R_G \subseteq J_G \times S_G$).

Використання (2) орієнтоване на задоволення трьох умов [16]:

1) E_G функціональна на $\bigcup\{I_G, C_G, M_G, L_G)$ якщо $(x, y) \in E_G$ і $(x, z) \in E_G$, то будь-який $y = z$ або обидві $(x, y), (x, z) \in \bigcup\{O_G, R_G\}$;

2) E_G^{-1} функціональна на $\bigcup\{O_G, R_G)$ якщо $(y, x) \in E_G$ і $(z, x) \in E_G$, то будь-який $y = z$ або обидві $(y, x) \in \bigcup\{I_G, C_G, M_G, L_G\}$ і $(z, x) \in \bigcup\{I_G, C_G, M_G, L_G\}$;

3) $\forall j \in J$ існують різні сегменти стрілок s, s', s'' такі, що $L_G sj, L_G s'j$ і $R_G s''j$ або $R_G sj, L_G s'j$ і $R_G s''j$;

з урахуванням двох обмежень на [16]:

1) з'єднання пар вершин кожним типом ребра: входом I_G (англ. "**I**nput"), управлінням C_G (англ. "**C**ontrol"), механізмом M_G (англ. "**M**echanism") приєднуються сегменти стрілок до блоків; виходом O_G (англ. "**O**utput") приєднується блок до сегментів стрілок; краями стиків з'єднуються сегменти стрілок між собою;

2) застосовність сегментів стрілок. Насамперед сегмент вхідної стрілки даного блоку не може бути сегментом вхідної стрілки (або управління, або механізм) для іншого (умова 1). Тоді як сегмент вихідної стрілки даного блоку не може бути сегментом вихідної стрілки для іншого (умова 2). Водночас з будь-яким стиком повинні пов'язуватися або декілька сегментів стрілок, що входять у нього, або декілька сегментів стрілок що виходять з нього (умова 3). Цим встановлюються особливості їх використання при відображенні з'єднань і розгалужень.

Шлях графу G визначається послідовністю вершин $(y_1, y_2, .., y_i, .., y_n)$ таких, що (y_i, y_{i+1}) для всіх i за умови $0 < i < n$. Довжина шляху $(y_1, y_2, .., y_i, .., y_n)$ дорівнює $n-1$.

Вузол наступник (попередник) x вузла y графу G якщо існує шлях від y до x (від x до y). Вузол x є безпосереднім наступником (попередником) вузла y графу G якщо (x, y) $((y, x))$.

Шлях стрілки графу G визначається послідовністю вершин $(y_1, y_2, .., y_i, .., y_n)$ таких, що $y_i \in S_G \cup J_G$ за умови $0 \le i \le n$ і $y_1, y_n \in S_G$. Цей шлях проходить лише сегменти стрілок і стики.

Сегмент стрілки s графу G є вхідним (вихідним) стосовно блоку або стику e якщо s його безпосередній попередник (безпосередній наступник). Водночас сегмент стрілки s пов'язаний зі стиком e якщо він або вхідний, або вихідний стосовно e. Стрілка $(s_1, s_2, .., s_n)$ графу G є вхідною (вихідною) для блоку якщо s_n вхідний (s_1 вихідний) до нього сегмент.

Номер вузла визначається числами від 0 до 9 та нескінченним порядковим числом ω, $0 < n < \omega$. Тоді отримаємо

$$m(10^i) + n,$$

де $1 \le m \le 9$, i – найменше число $10^i \le n$.

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для функціонального аналізування систем управління інформаційною безпекою визначається мета та точку зору. Метою встановлюються причини розроблення даних систем, наприклад: забезпечення конфіденційності, цілісності, доступності інформації; гарантування надання послуг організацією з прийнятним ризиком інформаційної безпеки. Тоді як точкою зору задається в інтересах кого або чого розробляються системи управління інформаційною безпеко, наприклад: зацікавлені сторони (внутрішні, зовнішні), підрозділ організації, організація загалом [2], [3], [14].

Після визначення мети та точки зору встановлюються вхідні I_G, вихідні дані O_G, а також управління C_G і механізми M_G. У цьому випадку як діяльність розглядається управління інформаційною безпекою, b_1 [2], [16]. З огляду на це отримаємо:

1) функцією верхнього рівня є діяльність з управління інформаційною безпекою. Для її представляється використовується один блок, $B_G = \{b_1\}$;

2) кожен сегмент стрілки $s \in S_G$ відображається стрілкою;

3) для блоку $b_1 \in B_G$ існує щонайменше одна вхідна стрілка $s \in S_G$ така, що $(s, b_1) \in I_G$;

4) для блоку $b_1 \in B_G$ існує щонайменше одна вихідна стрілка $s \in S_G$ така, що $(b_1, s) \in O_G$;

5) для блоку $b_1 \in B_G$ існує щонайменше одна стрілка управління $s \in S_G$ така, що $(s, b_1) \in C_G$;

6) для блоку $b_1 \in B_G$ існує щонайменше одна стрілка механізму $s \in S_G$ така, що $(s, b_1) \in M_G$;

7) блок $b_1 \in B_G$ має унікальний номер $\#_1(b) = \#(b) = 0$ та номер вузла $\#_n(G) = \omega$ графу G.

Якщо виконуються встановлені умови та $D = \{G, \#_n, \#\}$ є преструктурою, то D представляється як структура контекстної діаграми [16]. Нею відображається функція верхнього рівня систем управління інформаційною безпекою діяльністю [2]. Для позначення контекстної діаграми використовується код А0.

Детальне представлення діяльності з управління інформаційною безпекою здійснюється завдяки її поділу на функції нижніх рівнів. Ними відображаються процеси, операції і дії. При цьому на кожному з рівнів поділу рекомендується представляти від 3 до 6 блоків [5]. Тому за аналогією з діяльністю управління інформаційною безпекою для кожного з рівнів відображення отримаємо [16]:

1) функціями нижнього рівня є або процеси, або операції, або дії. Вони представляється блоками $b' \in B_{G'}$;

2) для блоку $b' \in B_{G'}$ існує щонайменше один вхідний сегмент стрілки $s' \in S_{G'}$ така, що $(s', b') \in I_{G'}$;

3) для блоку $b' \in B_{G'}$ існує щонайменше один вихідний сегмент стрілки $s' \in S_{G'}$ така, що $(b', s') \in O_{G'}$;

4) для блоку $b' \in B_{G'}$ існує щонайменше один сегмент стрілки управління $s' \in S_{G'}$ така, що $(s', b') \in C_{G'}$;

5) для блоку $b \in B_{G'}$ існує щонайменше однин сегмент стрілки механізму $s' \in S_{G'}$ така, що $(s', b') \in M_{G'}$;

6) потужність множини $B_{G'}$ визначається у таких межах $2 \le card(B_{G'}) \le 9$;

7) блоки $b' \in B_{G'}$ мають унікальний номер $\#(b') \in \{1, ..., card(B_{G'})\}$ та номер вузла $\#_n(b') = 10(\#_n(G')) + \#(b')$.

Якщо виконуються встановлені умови та $D' = \{G', \#_n, \#\}$ є преструктурою, то D' представляється як структура не контекстної діаграми [16]. Дана діаграма є дочірньою стосовно контекстної. Це обумовлено виконанням такої рівності

$$\#_n(b_1) = \#(D')$$

і розробляється окремо для кожного з рівнів поділу. З огляду на це, для позначення не контекстних діаграм використовуються коди, наприклад, A1, A2 (рівень процесу), A11, A12 (рівень операції), A111, A112 (рівень дії). Такий поділ дозволяє представити ієрархію функцій систем управління інформаційною безпекою родовідним деревом [2], [14], [16].

Під родовідним деревом розумітиметься дерево (див., наприклад [5], [14], рис. 1)

$$\Delta = (\delta, P),$$

$$D, D' \in \delta, \#_n(D) \neq \#_n(D'),$$

де δ – множина попарно неперетинних діаграм, P – батьківське відношення "предок-нащадок".

Тоді при виконанні таких умов

1) D_{root} – контекстна діаграм;
2) $\forall D \in \Delta - D_{root}$, D – не контекстна діаграма

отримаємо закодоване родовідне дерево

$$\Delta_c = (\Delta, c)$$

де c – загальна функція ICOM кодування, якою визначається сегмент стрілки.

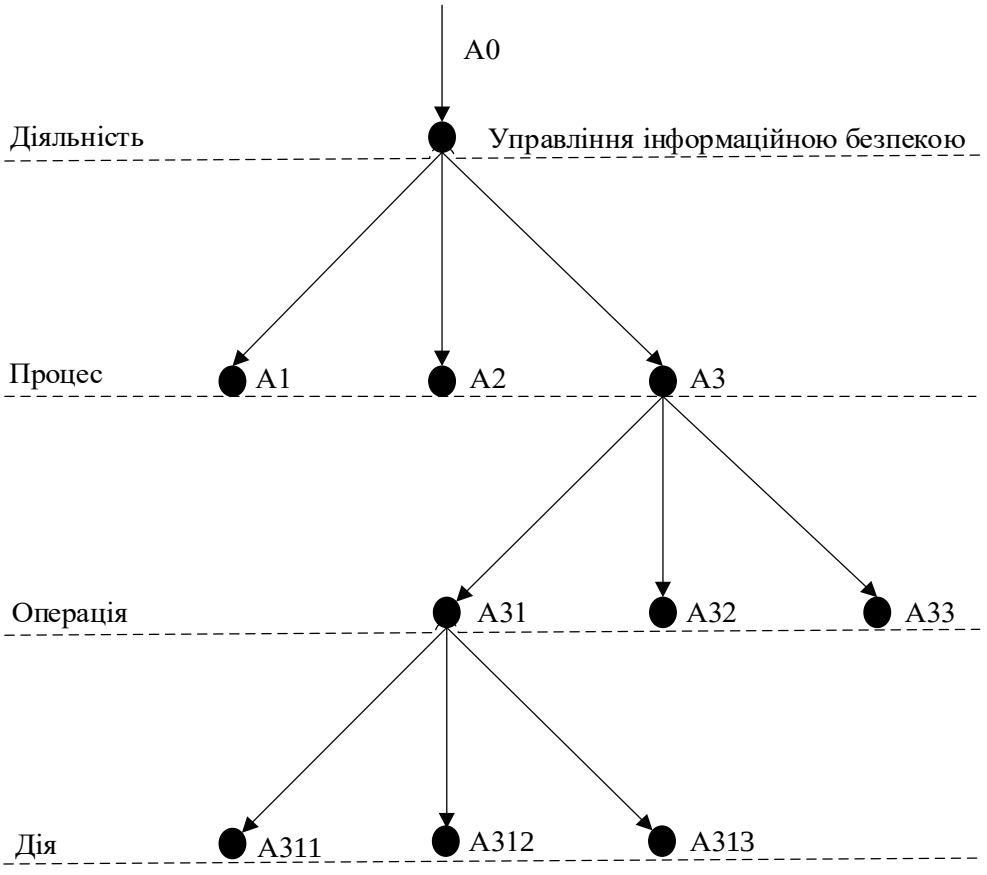

Рис. 1. Представлення ієрархії функцій систем управління інформаційною безпекою родовідним деревом

Оскільки завдяки функціональному аналізуванню визначається ієрархія функцій систем управління інформаційною безпекою, то, як наслідок, можливе встановлення їх відповідності організаційно-технічній структурі [2], [3], [14]. При цьому доцільно

враховувати один з основних принципів такого підходу, зокрема, «відокремленість» організації від функцій систем [5]. Однак, незважаючи на це, між ієрархією функцій та організаційно-технічною структурою існує відповідність (див., наприклад, рис. 2).

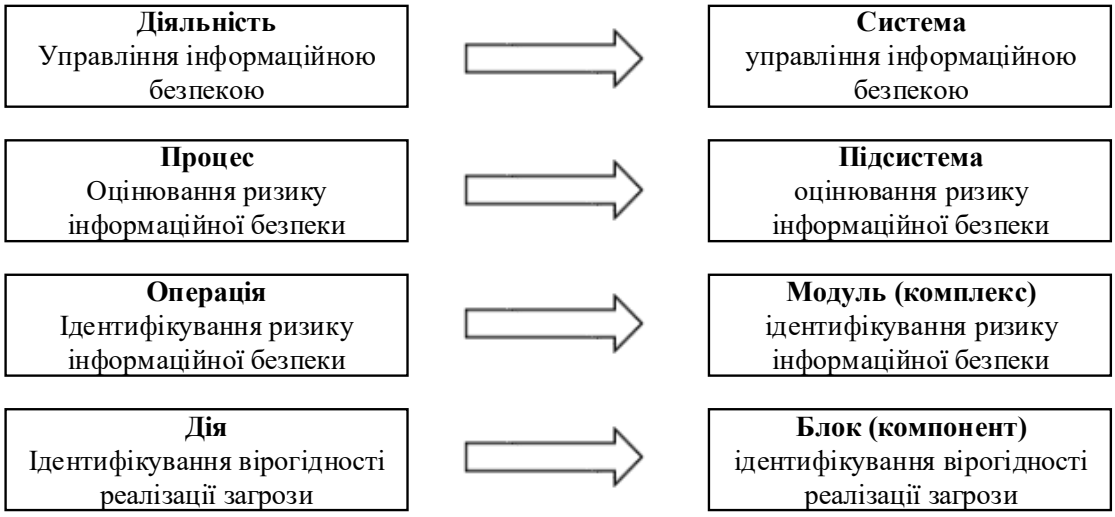

Рис. 2. Відповідність між функціями та організаційно-технічними структурами

4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отже, розроблення методу функціонального аналізування систем управління інформаційною безпекою дозволить визначати їх функції як на рівні системи, так і рінях її структурних елементів (підсистем, комплексів, компонентів). Завдяки цьому встановлюється відповідність між ієрархією функцій і організаційно-технічною структурою. Для кожної функції ієрархії визначаються вхідні, вихідні дані, управління і механізми. Як наслідок, можливе подолання обмежень типових способів функціонального аналізування, зокрема, орієнтованості на представлення міжнародних стандартів серії ISO/IEC 27k, відображення основних стадій життєвого циклу систем управління інформаційною безпекою, розроблення окремих елементів систем управління інформаційною безпекою, зокрема, управління ризиком.

У перспективах подальших досліджень планується на основі запропонованого методу функціонального аналізування визначити ієрархію функцій та розробити логічну структуру систем управління інформаційною безпекою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] International Organization for Standardization. (2016, May 27). *ISO/IEC/IEEE 24748-4:2016. Systems and software engineering. Life cycle management. Part 4: Systems engineering planning*. Geneva, 2016, 62 p.

[2] В. В. Мохор, та В. В. Цуркан, “Функції системи управління інформаційною безпекою”, на *X міжнародній науково-технічній конференції ITSec: Безпека інформаційних технологій*, Київ, 2020, с. 53.

[3] В. В. Цуркан, “Функціональний підхід до моделювання процесу менеджування ризику безпеки інформації”, на *XIII международной научной конференции Информационные технологии и безопасность. Оценка состояния*, Киев, 2013, с. 193-194.

[4] В. В. Репин, и В. Г. Елиферов, *Процессный подход к управлению. Моделирование бизнес-процессов.* Москва, Россия: Манн, Иванов и Фербер, 2013.

[5] Госстандарт России. (2001, Февр. 02). *РД 50.1.028:2001. Методология функционального моделирования IDEF0*. Москва, 2001. 75 с.

[6] Н. В. Андреева, "Функциональная модель системы управления информационной безопасностью как средство внедрения стандартов линейки ISO/IEC 2700X (BS 7799)", *Научно-технический вестник информационных технологий, механики и оптики*, № 5 (39), с. 40-44, 2007.

[7] А. В. Любимов, Н. В. Андреева, и С. В. Шустиков, "Базовые параметры полуформальных моделей систем управления информационной безопасностью", *Научно-технический вестник информационных технологий, механики и оптики*, № 7 (52), с. 219-226, 2008.

[8] А. В. Любимов, С. В. Шустиков, и Н. В. Андреева, "Функциональное моделирование системы управления информационной безопасности организации по семейству стандартов ISO/IEC 2700x", *Научно-технический вестник информационных технологий, механики и оптики*, № 7 (52), с. 251-257, 2008.

[9] А. Н. Гупаленко, "Применение методов функционального моделирования для исследования защищенности предприятия", *Информационное противодействие угрозам терроризма*, № 14, с. 27-30, 2010.

[10] И. В. Машкина, М. Б. Гузаиров, "Методы разработки функциональной модели управления защитой информации", *Безопасность информационных технологий*, том 15, № 2, с. 105-110, 2008.

[11] А. М. Цыбулин, "Многоагентный подход к построению автоматизированной системы управления информационной безопасностью предприятия", *Известия ЮФУ. Технические науки. Информационная безопасность*, № 12, с. 111-116, 2012.

[12] М. Ю. Комаров, та С. Ф. Гончар, "Методика побудови системи управління інформаційною безпекою на об'єктах критичної інфраструктури", *Моделювання та інформаційні технології*, вип. 81, с. 12-19, 2017.

[13] Ю. Кожедуб, "Функціональна модель системи забезпечення інформаційної безпеки", *Information Technology and Security*, vol. 6, iss. 2 (11), pp. 29-42, July-December 2018. doi: 10.20535/2411-1031.2018.6.2.153488.

[14] В. В. Мохор, В. В. Цуркан, Я. Ю. Дорогий, та О. М. Крук, "Функціональне моделювання системи керування ризиком безпеки інформації", *Захист інформації*, том 18, № 1, с. 74-80, 2016, doi: 10.18372/2410-7840.18.10115.

[15] В. В. Мохор, В. В. Цуркан, Я. Ю. Дорогий, та О. М. Крук, "Дерево вузлів функціональної моделі системи керування ризиком безпеки інформації", на *XVIII міжнародній науково-практичній конференції Безпека інформації в інформаційно-телекомунікаційних системах*, Київ, 2016, с. 36.

[16 International Organization for Standardization. (2012, Sept. 15). *ISO/IEC/IEEE 31320-1:2012. Information technology. Modeling Languages. Part 1: Syntax and Semantics for IDEF0*. Geneva, 2012, 120 p.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (8), 2020
ISSN 2663 - 4023

Vasyl V. Tsurkan
Candidate of Technical Sciences, Associate Professor, Senior Researcher
Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID: 0000-0003-1352-042X
v.v.tsurkan@gmail.com

METHOD OF INFORMATION SECURITY MANAGEMENT SYSTEMS FUNCTIONAL ANALYSIS

Abstract. The process of functional analysis of information security management systems was considered. The relevance of their presentation with many interrelated functions with internal and external interfaces is shown. Taking this into account, the methods of functional analysis of information security management systems are analyzed. Among them, graphic notation IDEF0 is highlighted. This choice is based on the ability to display both interfaces of functions and the conditions and resources of their execution. The orientation of the graphic notation IDEF0 use is established mainly for the presentation of the international standards ISO/IEC 27k series, the display of the main stages of the information security management systems life cycle, the development of individual elements of information security management systems, in particular, risk management. These limitations have been overcome by the method of information security management systems in functional analysis. This was preceded by the definition of the theoretical foundations of this method. Its use allows to allocate their functions at both levels of the system, and levels of its structural elements (subsystems, complexes, components). To do this, define the purpose, viewpoint and establishes information security management as the main activity. It is represented by a set of hierarchically related functions that are represented by a family tree. Each function of this tree defines incoming, outgoing data, management, and mechanisms. This makes it possible to establish their consistency with the organizational structure at the "activity-system", "process-subsystem", "operation-module (complex)" and "action-block (component)" levels. In future studies, it is planned to define a hierarchy of functions and develop a logical structure of information security management systems based on the proposed method of functional analysis.

Keywords: function; functions hierarchy; functional analysis, information security management system, IDEF0.

REFERENCES

[1] International Organization for Standardization. (2016, May 27). *ISO/IEC/IEEE 24748-4:2016. Systems and software engineering. Life cycle management. Part 4: Systems engineering planning*. Geneva, 2016, 62 p.

[2] V. V. Mokhor, and V. V. Tsurkan, "Functions of information security management system", in *Proc. X International Scientific and Technical Conference ITSec: Information Technology Security*, Kyiv, 2020, pp. 53.

[3] V. V. Tsurkan, "The functional approach to the information security risk management process modeling", in *Proc. XIII International Scientific Conference Information Technology and Security. Condition assessment*, Kyiv, 2013, pp. 193-194.

[4] V. V. Repin, and V. G. Eliferov, *The process approach to management. Business Process Modeling*. Moscow, Russia: Mann, Ivanov i Ferber, 2013.

[5] Gosstandart of Russia. (2001, Febr. 02). *RD 50.1.028:2001. Functional Modeling Methodology IDEF0*. Moscow, 2001. 75 p.

[6] N. V. Andreeva, "Functional model of information security management system as a means of implementing ISO/IEC 2700X (BS 7799) standards", *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, no. 5 (39), pp. 40-44, 2007.

[7] A. V. Ljubimov, N. V. Andreeva, and S. V. Shustikov, "Basic parameters of semi-formal models of information security management systems", *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, no. 7 (52), pp. 219-226, 2008.

[8] A. V. Ljubimov, S. V. Shustikov, and N. V. Andreeva, "Functional modeling of information security management system of the organization over the ISO/IEC 2700x standards", *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, no. 7 (52), pp. 251-257, 2008.

[9] A. N. Gupalenko, "The use of functional modeling methods to study enterprise security", *Information counteraction to threats of terrorism*, no. 14, pp. 27-30, 2010.

[10] I. V. Mashkina, and M. B. Guzairov, "Methods for developing a managing information security functional model", *IT Security*, vol. 15, no. 2, pp. 105-110, 2008.

[11] A. M. Cybulin, "Multi-agent approach to the construction of an automated enterprise information security management system", *Izvestiya SFedU: engineering sciences. Information Security*, no. 12, pp. 111-116, 2012.

[12] M. Yu. Komarov, and S. F. Gonchar, "Methods of building an information security management system at critical infrastructure facilities", *Modeling and Information Technology*, iss. 81, pp. 12-19, 2017.

[13] Yu. Kozhedub, "Functional model of information security systems", *Information Technology and Security*, vol. 6, iss. 2 (11), pp. 29-42, July-December 2018. doi: 10.20535/2411-1031.2018.6.2.153488.

[14] V. V. Mokhor, V. V. Tsurkan, Ya. Yu. Dorohyi, and O. M. Kruk, "Functional modeling of information security risk management system", *Zahist ìnformacìï*, vol. 18, no. 1, pp. 74-80, 2016, doi: 10.18372/2410-7840.18.10115.

[15] V. V. Mokhor, V. V. Tsurkan, Ya. Yu. Dorohyi, and O. M. Kruk, "Node tree of information security risk management system functional model", in *Proc. XVIII International Scientific and Practical Conference Information Security in Information and Telecommunication Systems*, Kyiv, 2016, pp. 36.

[16] International Organization for Standardization. (2012, Sept. 15). *ISO/IEC/IEEE 31320-1:2012. Information technology. Modeling Languages. Part 1: Syntax and Semantics for IDEF0*. Geneva, 2012, 120 p.