DOI: 10.18372/2410-7840.23.16766
УДК [004(056.53+413.4)::001.51]::303.732

МЕТОДОЛОГІЯ ПОБУДОВИ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Володимир Мохор, Василь Цуркан

Досліджено побудову систем управління інформаційною безпекою як проактивний захід збереження конфіденційності, цілісності та доступності інформації. Показано, що передумовою його реалізування в організаціях є визначення зовнішніх і внутрішніх обставин. Насамперед це стосується встановлення меж побудови систем управління інформаційною безпекою, взаємодій з іншими системами та/або організаціями. Крім того визначаються зовнішні і внутрішні зацікавлені сторони, їхні потреби, очікування, обмеження. Цим підтверджується актуальність і необхідність розроблення методології побудови систем управління інформаційною безпекою. За результатами аналізу останніх досліджень і публікацій встановлено характерні для них обмеження. Їх подолання досягнуто завдяки врахуванню технічних процесів життєвого циклу систем управління інформаційною безпекою. Тому побудову систем управління інформаційною безпекою зведено до аналізування вимог, аналізування функцій, синтезування архітектури. Її відповідність потребам, очікуванням, обмеженням зацікавлених сторін запропоновано встановлювати синтезуванням поведінки. З огляду на це запропоновано оцінювати якість синтезованої архітектури за функційною придатністю. Такий вибір обумовлено перш за все її відповідністю настановам міжнародних стандартів серії ISO/IEC 27k і, як наслідок, можливістю оцінювання ступеня задоволеності потреб, очікувань, обмежень зацікавлених сторін реалізуванням функцій систем управління інформаційною безпекою за синтезованим варіантом архітектури в організаціях. Сформульовані завдання виконуються на основі використання розвинутого системного підходу моделе-орієнтованим. Тож розроблена методологія побудови систем управління інформаційною безпекою реалізується за п'ять етапів: аналізу вимог, аналізу функцій, синтезу архітектури, синтезу поведінки та оцінювання функційної придатності синтезованої архітектури. Це дозволить гарантувати зацікавленим сторонам задоволеність їхніх потреб, очікувань, обмежень стосовно збереження конфіденційності, цілісності та доступності інформації в організаціях. Крім того, стане можливим синтезування альтернативних варіантів архітектури і обирання серед них найкращого при проєктуванні систем управління інформаційною безпекою.

Ключові слова: *система управління інформаційною безпекою, методологія побудови, якість систем управління інформаційною безпекою, функційна придатність архітектури, системний підхід, моделе-орієнтований підхід, мова моделювання систем.*

ПОСТАНОВКА ПРОБЛЕМИ

Одним з проактивних заходів збереження конфіденційності, цілісності та доступності інформації є побудова систем управління інформаційною безпекою [1, 2]. За її основу взято оцінювання ризиків, належністю поводження з якими гарантується зацікавленим сторонам безпечність як діяльності, так і надання послуг організаціями [1, 3]. Зокрема, банківської системи [4], кваліфікованими надавачами електронних довірчих послуг та їхніми відокремленими пунктами реєстрації [5], операторами системи передачі електричної енергії [6], об'єктами критичної інфраструктури загалом [7].

Побудові систем управління інформаційною безпекою в організаціях передує визначення зовнішніх і внутрішніх обставин впливу на даний процес. Насамперед це стосується встановлення меж побудови, взаємодій з іншими системами та/або організаціями. З одного боку, така обумовленість пов'язана з необхідністю включення систем управління інформаційною безпекою у загальну структуру управління організацією [1]. Тоді як з іншого, побудовою на їх основі, наприклад, систем управління кібербезпекою [2] або приватною інформацією [8]. Крім того, визначаються внутрішні та зовнішні зацікавлені сторони [1]. Для кожної з них встановлюються потреби, пов'язані з ними очікування, обмеження стосовно збереженості конфіденційності, цілісності та доступності інформації.

До того ж враховуються вимоги нормативно-правових і настанови нормативних документів. Прикладом такого врахування є збереженість властивостей державних інформаційних ресурсів в окремих випадках застосовністю систем управління інформаційною безпекою з підтвердженою відповідністю [9].

Зважаючи на отримані при цьому результати їхню побудову необхідно здійснювати, по-перше, у встановлених межах і з урахуванням внутрішніх і зовнішніх обставин діяльності організацій, зокрема, і взаємодій з іншими системами та/або організаціями; по-друге, на основі визначених потреб, очікувань, обмежень внутрішніх і зовнішніх зацікавлених сторін.

Тож розроблення методології побудови систем управління інформаційною безпекою в організаціях є актуальним.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Методологічні основи побудови систем управління інформаційною безпекою встановлюються гармонізованими в Україні міжнародними стандартами серії ISO/IEC 27k [1, 10, 11]. Відповідно до настанов цих документів виокремлюються такі їхні основні елементи як політики, працівники, управління (побудова, впровадження, функціонування, вдосконалення), документована інформація, а також додаткові – оцінювання, оброблення ризиків [11]. Тому побудова систем управління інформаційною безпекою здебільшого зводиться до створення і документування встановлених елементів у межах циклу «Плануй – Виконуй – Перевіряй – Дій» (англ. Plan – Do – Check – Act, PDCA). Водночас це призводить до складнощів їх реалізування у зв'язку з узагальненістю формулювань настанов, різноманітністю потреб, очікувань, обмежень зацікавлених сторін, специфікою діяльностей організацій. Подолання даних обмежень запропоновано в [12] завдяки забезпеченню підтримки формування документації на етапі планування відповідно до [1]. Характерною особливістю такого підходу є моделювання і аналіз правових аспектів. Таку підтримку розширено в [13] розробленням відповідного інженерного середовища. Його використання дозволило реалізовувати основні та додаткові елементи систем управління інформаційною безпекою на всіх етапах циклу PDCA. Це досягнуто завдяки їх документальному супроводженню на основі простежуваності документів з урахуванням відношень між ними. До того ж встановлено їхні шаблони та визначено наповненість відповідно до настанов міжнародних стандартів серії ISO/IEC 27k. Серед елементів виокремлено документи політик та процедур (наприклад, ідентифікування інформаційних активів, ідентифікування загроз). Представленню систем управління інформаційною безпекою через процеси (побудови, впровадження, функціонування) приділено увагу в [14]. Це обумовлено зосередженістю нормативних документів насамперед на їх наявності, а не змістовності. Дане обмеження подолано введенням критерія належності процесів, як основних елементів, системам управління інформаційною безпекою. Його використання взято за основу розроблення відповідного фреймворку. Це дозволило розмежовувати процеси на основні, допоміжні, управління і пов'язані з ними заходи забезпечення безпеки. Для кожного з них запропоновано визначати рівень зрілості та, як наслідок, забезпечувати ефективне використання наявних ресурсів організації. Описання процесів побудови систем управління інформаційною безпекою організаціями енергетичного сектору деталізовано в [15]. Зокрема виокремлено десять основних етапів – від їх обирання до подання заявки для проведення сертифікаційного аудиту – та визначено заходи в межах кожного з них. Окрему увагу приділено документуванню побудови систем управління інформаційною безпекою. Наведено перелік, шаблони та зміст відповідних документів. Побудову систем управління інформаційною безпекою центрів оброблення даних адаптовано в [16]. Для цього розроблено фреймворк з орієнтованістю на збереження конфіденційності, цілісності та доступності інформації. За його основу взято реалізування трьох елементів: люди, процеси, технології. Їх впровадження досягнуто в межах застосування циклу PDCA. Насамперед виокремлено основні процеси – від створення політик до покращення систем управління інформаційною безпекою. Для кожного з них обрано заходи відповідно до додатку А [1]. Застосування систем управління інформаційною безпекою у державних організаціях викладено в [18]. Передумовою цьому стала необхідність протидії загрозам безпеці інформаційно-комунікаційних систем. Забезпечення протидії досягнуто реалізуванням процесів за циклом PDCA з урахуванням настанов [1]. При цьому

зосереджено увагу на заданні меж побудови систем управління інформаційною безпекою шляхом реалізування відповідних заходів додатку А. Серед них виділено політики інформаційної безпеки, А.5; забезпечення безпеки експлуатації, А.12; забезпечення безпеки комунікацій, А.13; управління інцидентами, А.16. Це дозволило перейти від уявлень про рівень інформаційної безпеки до об'єктивного розуміння потреб, що пов'язані з її забезпеченням. Оцінювати необхідність побудови систем управління інформаційною безпекою за математичним підходом запропоновано в [18]. Його використанням передбачено оцінювання наслідків з урахуванням впроваджень настанов [1] в організаціях. За результатами зіставлення отриманих оцінок приймається рішення стосовно необхідності їх реалізування як елементів і побудови систем управління інформаційною безпекою загалом. Визначення поточного стану збереження властивостей інформації шляхом узгодженого використання їх моделі з настановами [1] представлено в [19]. Запропонованою моделлю відображено три фази: початкове діагностування, підготовлення і планування систем управління інформаційною безпекою. Її використання орієнтоване на задання як початкового, так і досягнення очікуваного стану збереження властивостей інформації відповідно до настанов [1].

За результатами аналізування останніх досліджень і публікацій встановлено, по-перше, узагальненість формулювань настанов міжнародних стандартів серії ISO/IEC 27k, і, як наслідок, відсутність методології побудови систем управління інформаційною безпекою. По-друге, орієнтованість на реалізування процесів укладання і виконання угод, організаційного забезпечення, технічного управління їх життєвого циклу [1, 20]. Насамперед це обумовлено тим, що у міжнародних стандартах серії ISO/IEC 27k викладення настанов обмежується тільки запровадженням зазначених процесів у організації. Кожен з них здебільшого виконується у межах циклу PDCA. По-третє, відображеність елементів систем управління інформаційною безпекою як політик, процесів побудови, впровадження, підтримання, вдосконалення, документованої інформації. По-четверте, застосовність документо-орієнтованого підходу як основи побудови систем управління інформаційною безпекою на всіх етапах циклу PDCA. Незважаючи на те, що документована інформація визначається як необхідний елемент [1], це призводить до їх тлумачення як «систем документів». По-п'яте, забезпеченість підтримання систем управління інформаційною безпекою як на окремих, так і всіх етапах циклу PDCA стосовно використання настанов міжнародних стандартів серії ISO/IEC 27k. Насамперед реалізування процесів побудови, впровадження, підтримання, вдосконалення. Як наслідок, по-шосте, складність гарантування зацікавленим сторонам придатності систем управління інформаційною безпекою відповідно до їхніх потреб, очікувань і обмежень. Наявністю встановлених обмежень обумовлюється об'єктивне протиріччя між придатністю методів побудови систем управління інформаційною безпекою, з одного боку, та їх методологічною сумісністю, з іншого.

Для подолання встановленого протиріччя окрім типового переліку процесів життєвого циклу систем управління інформаційною безпекою враховано технічні [1, 20]. Вони направлені на перетворення потреб, очікувань, обмежень зацікавлених сторін у системи управління інформаційною безпекою. Це досягається виконанням технічних дій у межах аналізу діяльності організацій (внутрішніх, зовнішніх обставин), визначення вимог, визначення архітектури, проєктування, системного аналізу, імплементації, інтеграції, верифікації [20]. Водночас враховано те, що системи загалом [21] і, системи управління інформаційною безпекою, зокрема [22], повністю визначаються архітектурою, а також поведінкою. Тому серед технічних зосереджено увагу на процесах, виконання яких дозволяє синтезувати їхню архітектуру [23–26] шляхом виконання завдань аналізу вимог [24] і функцій [25].

Архітектурою систем управління інформаційною безпекою виражаються їх основні поняття і властивості з огляду на навколишнє середовище [23, 27]. Дані поняття і властивості втілюються у елементах, відношеннях між ними. Тоді як під навколишнім середовищем розуміється організація незалежно від типу, розміру та природи [1]. Зва-

жаючи на це, системи управління інформаційною безпекою визначаються елементами, відношеннями між ними для досягнення сформульованих зацікавленими сторонами цілей.

Насамперед збереження конфіденційності, цілісності та доступності інформації в організаціях [1, 26].

Тому побудова систем управління інформаційною безпекою зводиться до виконання таких завдань: проаналізувати вимоги, проаналізувати функції, синтезувати архітектуру.

Її відповідність потребам, очікуванням, обмеженням зацікавлених сторін встановлюється синтезуванням поведінки [28]. Завдяки цьому створюються передумови оцінювання якості отриманого варіанту архітектури систем управління інформаційною безпекою. Як характеристику обрано функційну придатність [29].

Такий вибір обумовлено перш за все її відповідністю настановам [1] і, як наслідок можливістю оцінювання ступеня задоволення потреб, очікувань, обмежень зацікавлених сторін реалізуванням функцій систем управління інформаційною безпекою за синтезованим варіантом архітектури в конкретному навколишньому середовищі (організації).

Виконання сформульованих завдань досягається використанням системного підходу [22]. Однак, його застосування характеризується багатоаспектністю. Це пов'язано з існуванням різноманітних точок зору тлумачення його сутності, прийомів реалізування, складнощів ототожнення проблематики кожного з них [21, 22].

Їх подолання досягається орієнтованістю на виділення окремого аспекту дослідження, зокрема, архітектури систем управління інформаційною безпекою.

Тоді як уніфікованість представлення отриманих результатів забезпечується доповненням системного підходу моделе-орієнтованим (англ. Model Based Systems Engineering, MBSE) [23–26, 28], зокрема, використанням мови моделювання систем.

Тож метою даної роботи є підвищення функційної придатності архітектури систем управління інформаційною безпекою.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Методологія побудови систем управління інформаційною безпекою реалізується за п'ять етапів: аналізу вимог, аналізу функцій, синтезу архітектури, синтезу поведінки та оцінювання функційної придатності синтезованої архітектури (рис. 1) [22–26, 28]. Розглянемо кожен з виокремлених етапів.

Етап 1. Аналіз вимог до систем управління інформаційною безпекою [24]. Вимоги аналізуються на основі вхідних даних про потреби зацікавлених сторін. Вони відображаються частково впорядкованою множиною за їхньою важливістю:

$$ND = \{ND_i\},$$

$$ND_1 \geq ND_2 \geq ... \geq ND_i \geq ... \geq ND_N,\ i=\overline{1,N}.$$

Для представлення потреб зацікавлених сторін вимогами використовується така синтаксична форма:

[Умова] [Суб'єкт] [Дія] [Об'єкт] [Обмеження дії].

Це дозволяє кожну потребу ND_i взаємно однозначно відобразити вимогою RQ_i до систем управління інформаційною безпекою

$$f_{RQ} : ND \to RQ,$$

де f_{RQ} – взаємно однозначне відображення (1) у (2); RQ – частково впорядкована множина вимог зацікавлених сторін за їхньою важливістю

$$RQ = \{RQ_i\},$$

$$RQ_1 \geq RQ_2 \geq ... \geq RQ_i \geq ... \geq RQ_N.$$

Інформація про вимогу до систем управління інформаційною безпекою формалізується з урахуванням встановлених атрибутів.

Серед атрибутів використовуються ідентифікатор, формулювання, тип, пріоритет, зацікавлена сторона. Цей перелік уточнюється залежно від конкретної організації. Тоді представлення вимоги до систем управління інформаційною безпекою матиме вид:

$$RQ_i = \{id_i, Text_i, Type_i, Priority_i, Stakeholder_i\},$$

де RQ_i – вимога, що задовольняє потребу ND_i; id_i – ідентифікатор *i*-ї вимоги; $Text_i$ – формулю-

вання i-ї вимоги; $Type_i$ – тип i-ї вимоги (функційна або не функційна); $Priority_i$ – пріоритет i-ї вимоги (низький, середній, високий); $Stakeholder_i$ – зацікавлена сторона у виконанні i-ї вимоги.

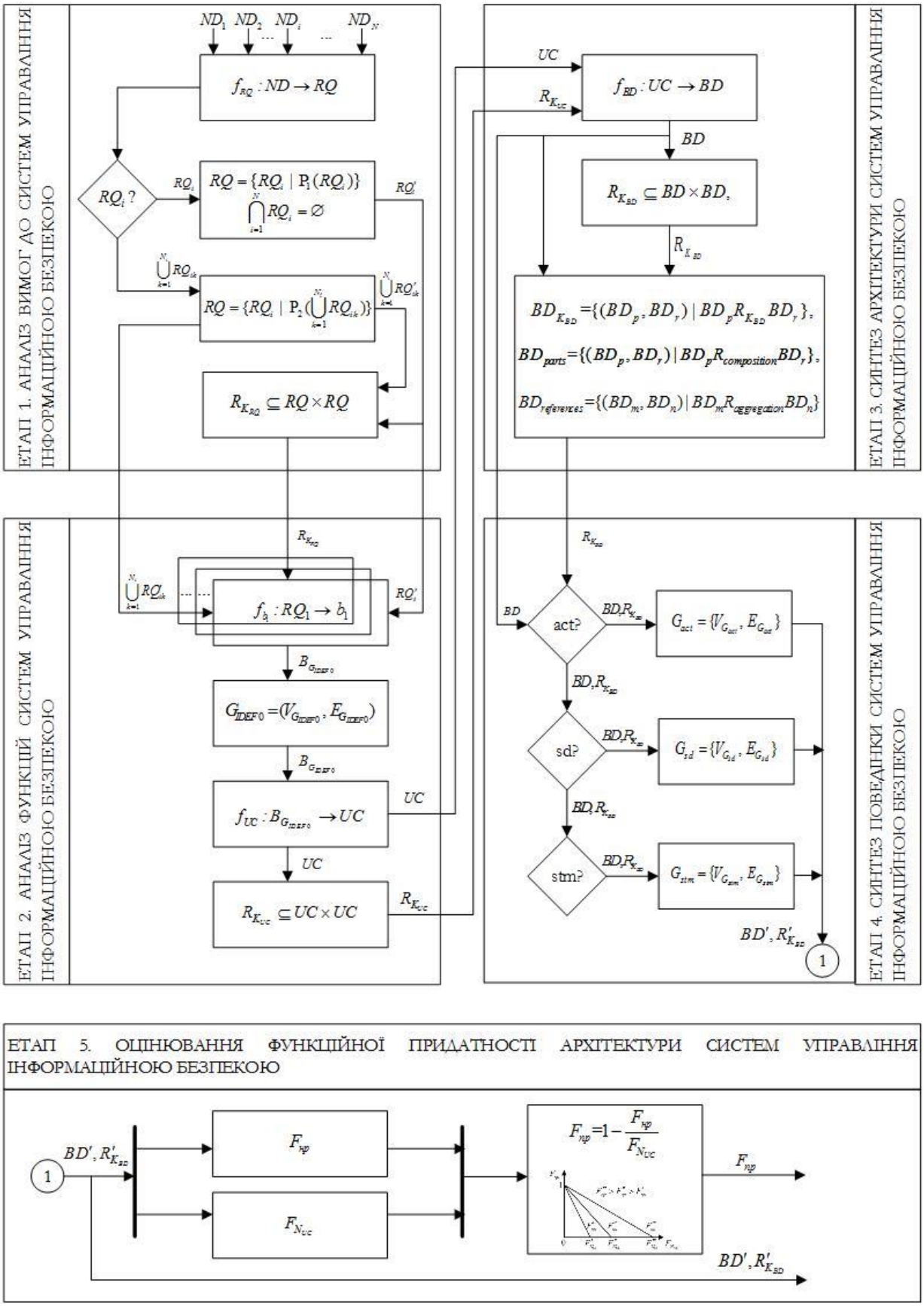

Рис. 1 Структурно-аналітичне відображення методології побудови систем управління інформаційною безпекою

Після того як сформульовано вимоги до систем управління інформаційною безпекою перевіряється відповідність індивідуальним:

$$RQ = \{RQ_i \mid \mathrm{P}_1(RQ_i)\},$$

$\bigcap_{i=1}^{N} RQ_i = \varnothing$ і груповим характеристикам $RQ =$

$\{RQ_i \mid \mathrm{P}_2(\bigcup_{k=1}^{N_i} RQ_{ik})\}$,

де $\mathrm{P}_1(RQ_i)$ – RQ_i задовольняє індивідуальним характеристикам; $\mathrm{P}_2\left(\bigcup_{k=1}^{N_i} RQ_{ik}\right) - \bigcup_{k=1}^{N_i} RQ_{ik}$ задовольняє груповим характеристикам.

Взаємозв'язок між вимогами до систем управління інформаційною безпекою встановлюється за допомогою відношень $R_{K_{RQ}}$

$$(RQ_i, RQ_j) \in R_{K_{RQ}},$$

$$R_{K_{RQ}} \subseteq RQ \times RQ,$$

де (RQ_i, RQ_j) – пара вимог з відношенням $R_{K_{RQ}}$, $j=\overline{1,N}$; K_{RQ} – множина різновидів відношень між вимогами,

$K_{RQ} = \{derive, copy, containment, satisfy, verify, refine, trace\}$.

Отже, на основі потреб, очікувань, обмежень зацікавлених сторін отримуємо множину вимог до систем управління інформаційною безпекою і відношень між ним. Для їх специфікування використовується відповідна діаграма мовою моделювання SysML, $D_{req}=\{RQ, R_{K_{RQ}}\}$.

Етап 2. Аналіз функцій систем управління інформаційною безпекою [25].

Функції аналізуються на основі вхідних даних про вимоги до систем управління інформаційною безпекою шляхом використання графу IDEF0. Цьому передує формулювання мети та точки зору.

Метою визначаються очікування зацікавлених сторін від побудови систем управління інформаційною безпекою в організаціях, зокрема, забезпечення конфіденційності, цілісності, доступності інформації; гарантування надання послуг організацією з прийнятним рівнем ризиків інформаційної безпеки.

Тоді як точкою зору задається в інтересах кого або чого вони будуються, наприклад: зацікавлених сторін (внутрішніх, зовнішніх), окремого підрозділу або організації загалом. З огляду на це, вимога найвищого пріоритету RQ_1 відображається функцією верхнього рівня

$$f_{b_1} : RQ_1 \to b_1,$$

а саме, діяльністю з управління інформаційною безпекою. Для неї визначаються вхідні дані, обмеження, вихідні дані і механізми

$$I_{G_{IDEF0}} \subset S_{G_{IDEF0}} \times B_{G_{IDEF0}},\ (s, b_1) \in I_{G_{IDEF0}},$$

$$C_{G_{IDEF0}} \subset S_{G_{IDEF0}} \times B_{G_{IDEF0}},\ (s, b_1) \in C_{G_{IDEF0}},$$

$$O_{G_{IDEF0}} \subset B_{G_{IDEF0}} \times S_{G_{IDEF0}},\ (b_1, s) \in O_{G_{IDEF0}},$$

$$M_{G_{IDEF0}} \subset S_{G_{IDEF0}} \times B_{G_{IDEF0}},\ (s, b_1) \in M_{G_{IDEF0}}.$$

Це дозволяє задати граф IDEF0

$$G_{IDEF0} = (V_{G_{IDEF0}}, E_{G_{IDEF0}}),$$

де $V_{G_{IDEF0}}$ – множина блоків, сегментів стрілок, $V_{G_{IDEF0}} = \bigcup(B_{G_{IDEF0}}, S_{G_{IDEF0}})$; $B_{G_{IDEF0}}$ – підмножина множини блоків B, $B_{G_{IDEF0}} \subseteq B$; $S_{G_{IDEF0}}$ – підмножина множини стрілок S, $S_{G_{IDEF0}} \subseteq S$; $E_{G_{IDEF0}}$ – множина дуг,

$$E_{G_{IDEF0}} = \bigcup(I_{G_{IDEF0}}, C_{G_{IDEF0}}, O_{G_{IDEF0}}, M_{G_{IDEF0}}).$$

За аналогією з цим, визначаються функції нижніх рівнів шляхом декомпозиції діяльності управління інформаційною безпекою як функції верхнього рівня. Ними відображаються або процеси (оцінювання ризиків), або операції (визначення оцінок ризиків), або дії (визначення вірогідності реалізації загрози).

На основі визначених функцій формалізується представлення варіантів використання систем управління інформаційною безпекою

$$f_{UC} : B_{G_{IDEF0}} \to UC,$$

де f_{UC} – взаємно однозначне відображення функцій систем управління інформаційною безпекою варіантами використання; UC – множина варіантів використання систем управління інфо-

рмаційною безпекою, $UC=\{UC_l\}$; l – номер варіанту використання, $l = \overline{1, N_{UC}}$.

Варіантами використання описуються функційні можливості з точки зору зацікавлених сторін. Вони тлумачаться як ектори і ними відображаються ролі стосовно використання систем управління інформаційною безпекою. При цьому виокремлюються такі взаємозв'язки: «Зацікавлена сторона – зацікавлена сторона», «Зацікавлена сторона – варіант використання», «Варіант використання – варіант використання»

$$(UC_l, UC_m) \in R_{K_{UC}},$$

$$R_{K_{UC}} \subseteq UC \times UC,$$

де (UC_l, UC_m) – пара варіантів використання з відношенням $R_{K_{UC}}$; K_{UC} – множина різновидів відношень між варіантами використання, $K_{UC} = \{association, include, extend, generalization\}$.

Отже, за результатами аналізу функцій отримуємо множину варіантів використання систем управління інформаційною безпекою і відношень між ним. Для їх специфікування використовується відповідна діаграма мовою моделювання SysML, $D_{uc}=\{UC, R_{K_{UC}}\}$.

Етап 3. Синтез архітектури систем управління інформаційною безпекою [26].

Архітектура систем управління інформаційною безпекою синтезується на основі вхідних даних про їх варіанти використання.

Для відображення кожного з них використовуються блоки. Вони тлумачиться як елементи архітектури систем управління інформаційною безпекою (підсистеми, комплекси, компоненти):

$$f_{BD} : UC \to BD,$$

де f_{BD} – взаємно однозначне відображення варіантів використання систем управління інформаційною безпекою блоками; BD – множина блоків, $BD = \{BD_p\}$; m – номер блоку, $m = \overline{1, N_{BD}}$.

Взаємозв'язок між елементами архітектури систем управління інформаційною безпекою визначається за допомогою відношень «Association», «Generalization», «Aggregation», «Composition»:

$$(BD_p, BD_r) \in R_{K_{BD}},$$

$$R_{K_{BD}} \subseteq BD \times BD,$$

де (BD_p, BD_r) – пара елементів з відношенням $R_{K_{BD}}$ між ними; K_{BD} – множина різновидів відношень між елементами,

$$K_{BD} = \{association, generalization, aggregation, composition\}.$$

Структурні ознаки елементів архітектури систем управління інформаційною безпекою представляються такими властивостями як порти, обмеження, частина, посилання, значення. Портами відображаються прийнятні типи відношень. Зокрема, деталізуються місця підключення зовнішніх сутностей до елементів та способи взаємодії між ними. Межі використання властивостей встановлюються обмеженнями. Тоді як частиною характеризується розкладання елементу на окремі складники. Взаємозв'язки між ними встановлюються за допомогою відношення «Composition»:

$$BD_{parts} = \{(BD_p, BD_r) \mid BD_p R_{composition} BD_r\},$$

$$BD_{parts} \subseteq BD.$$

Його використання орієнтоване на встановлення основних і додаткових властивостей елементу-частини в межах елементу-цілого. Наприклад, елемент «Ідентифікування вірогідності реалізацій загроз інформаційній безпеці» є частиною елементу «Ідентифікування ризиків інформаційної безпеки». Тоді як останній є складником для цілого «Оцінювання ризиків інформаційної безпеки». Посилання – характеризує включення до елементу інших елементів як його складників. Особливістю використання цієї властивості є можливість існування елементів-частин при знищенні цілого. Крім того, воно застосовується для описання логічної ієрархії елементів архітектури систем управління інформаційною безпекою, що визначається елементами інших ієрархічних частин. Відношення між ними задається різновидом «Aggregation»:

$$BD_{references} = \{(BD_m, BD_n) \mid BD_m R_{aggregation} BD_n\},$$

$$BD_{references} \subseteq BD.$$

Наприклад, якщо розглядати як елемент-ціле «Визначення оцінок ризиків інформаційної безпеки», то до нього можуть включатися елементи «Визначення якісних оцінок ризиків інформаційної безпеки», «Визначення кількісних оцінок ризику інформаційної безпеки», «Визначення якісно-кількісних оцінок ризиків інформаційної безпеки». З огляду на характеризування взаємозв'язку між ними різновиду «Aggregation», кожна з цих частин може реалізовуватися як окремий елемент, так і агрегуватися у межах елементу-цілого.

Для визначення характеристик елементів архітектури систем управління інформаційною безпекою використовується властивість «Значення».

До таких характеристик належать, наприклад: вірогідність (імовірність) реалізації загрози, наслідки реалізації загрози, оцінка ризиків інформаційної безпеки.

Основою використання цієї властивості є встановлення діапазону прийнятних значень при описанні блоку (наприклад, оцінка низька (0–2), середня (3–5) або висока (6–8)).

Тому при синтезі архітектури систем управління інформаційною безпекою важливо забезпечувати узгодженість типів значень характеристик її елементів.

Отже, за результатами синтезу архітектури систем управління інформаційною безпекою отримуємо множину елементів (блоків) і відношень між ним. Для їх специфікування використовується відповідна діаграма мовою моделювання SysML, $D_{bdd}=\{BD, R_{K_{BD}}\}$.

Етап 4. Синтез поведінки систем управління інформаційною безпекою [28].

Поведінка синтезується на основі вхідних даних про архітектуру систем управління інформаційною безпекою. Даний етап орієнтований на підтвердження виконання проаналізованих функцій відповідно до потреб, очікувань і обмежень зацікавлених сторін.

Це досягається за такими аспектами як діяльність – послідовність дій з боку елементів архітектури, умов їхнього виконання, потоку даних; взаємодія – часові особливості передавання і приймання даних між елементами архітектури; скінченний автомат – змінення станів елементами архітектури при настанні визначених умов.

Діяльністю зі збереження конфіденційності, цілісності та доступності інформації в організаціях синтезується поведінка систем управління інформаційною безпекою через контрольовану послідовність дій елементів. Характерною особливістю такого представлення є орієнтованість на встановлення умов їх виконання.

Водночас відображення об'єктів як вхідних і вихідних даних кожної дії. Тому діяльність як один з основних аспектів синтезу поведінки систем управління інформаційною безпекою синтезується графом діяльності:

$$V_{G_{act}} = \bigcup (A_{G_{act}}, CN_{G_{act}}, ON_{G_{act}}),$$

$$G_{act} = \{V_{G_{act}}, E_{G_{act}}\},$$

де G_{act} – граф діяльності; $V_{G_{act}}$ – множина вузлів діяльності; $A_{G_{act}}$ – підмножина дій, $A_{G_{act}} \subset V_{G_{act}}$; $CN_{G_{act}}$ – підмножина вузлів управління, $CN_{G_{act}} \subset V_{G_{act}}$; $ON_{G_{act}}$ – підмножина вузлів об'єктів, $ON_{G_{act}} \subset V_{G_{act}}$; $E_{G_{act}}$ – множина дуг діяльності.

Часові особливості передавання і приймання об'єктів між елементами архітектури систем управління інформаційною безпекою відображаються через їхнє взаємодіяння. Основою такої взаємодії є встановлення послідовності обміну повідомленнями. Це можливе або між системами управління інформаційною безпекою і навколишнім середовищем (організацією), або між елементами їхньої архітектури. У цьому випадку як елементи, так і системи управління інформаційною безпекою тлумачаться окремими сутностями – лініями життя. Взаємодіяння між ними здійснюється обміном повідомленнями.

Тому воно представляється як окремий аспект синтезування поведінки систем управління інформаційною безпекою графом взаємодії:

$$G_{sd} = \{V_{G_{sd}}, E_{G_{sd}}\},$$

де G_{sd} – граф взаємодії; $V_{G_{sd}}$ – множина вузлів взаємодії (ліній життя); $E_{G_{sd}}$ – множина дуг взаємодії.

Змінення станів елементами архітектури відображається скінченним автоматом. Його використання орієнтоване на описання поведінки систем управління інформаційною безпекою станами та переходами між ними. Це супроводжується встановленням умов настання таких змін.

Тож поведінка як елементів архітектури, так і систем управління інформаційною безпекою загалом визначається переходами між вершинами графу скінченного автомату. Направленість таких переходів задається дугами. Тому змінення станів як окремий аспект синтезування поведінки елементів архітектури систем управління інформаційною безпекою представляється графом скінченного автомату:

$$G_{stm} = \{V_{G_{stm}}, E_{G_{stm}}\},$$

де G_{stm} – граф скінченного автомату; $V_{G_{stm}}$ – множина станів елементів (блоків) архітектури систем управління інформаційною безпекою:

$$V_{G_{stm}} = \bigcup (ST_{G_{stm}}, PST_{G_{stm}});$$

де $ST_{G_{stm}}$ – підмножина станів, $ST_{G_{stm}} \subset V_{G_{stm}}$; $PST_{G_{stm}}$ – підмножина псевдостанів, $PST_{G_{stm}} \subset V_{G_{stm}}$; $E_{G_{stm}}$ – множина переходів між станами елементів архітектури систем управління інформаційною безпекою.

Отже, за результатами синтезу поведінки систем управління інформаційною безпекою отримуємо множини вузлів і дуг діяльності; вузлів і дуг взаємодії; станів і переходів між станами елементів. Для їх специфікування використовуються відповідні діаграми мовою моделювання SysML, $D_{act}=\{V_{G_{act}} \cup \mathrm{E}_{G_{act}}\}$, $D_{sd}=\{V_{sd}, E_{sd}\}$, $D_{stm}=\{V_{stm} \cup E_{stm}\}$.

Етап 5. Оцінювання функційної придатності архітектури систем управління інформаційною безпекою.

Функційна придатність архітектури оцінюється на основі вхідних даних про реалізованість функцій систем управління інформаційною безпекою відповідно до синтезованих варіантів їх архітектури та поведінки [29]. Це дозволяє встановити ступінь задоволення потреб, очікувань, обмежень зацікавлених сторін:

$$F_{пр} = 1 - \frac{F_{нр}}{F_{N_{UC}}},$$

де $F_{пр}$ – функцій придатність; $F_{N_{UC}}$ – загальна кількість варіантів використання (функцій) систем управління інформаційною безпекою; $F_{\text{нр}}$ – кількість не реалізованих варіантів використання (функцій) систем управління інформаційною безпекою. При $F_{\text{нр}} = 0$ функційна придатність максимальна. Тоді як при $F_{пр} = F_{N_{UC}}$ – мінімальна.

ВИСНОВКИ

Отже, розроблено методологію побудови систем управління інформаційною безпекою, яка завдяки придатності і водночас методологічній сумісності запропонованих методів аналізу вимог, аналізу функцій, синтезу архітектури, синтезу поведінки дозволяє формалізувати процес побудови систем управління інформаційною безпекою за їх функційно придатною архітектурою. Це дозволяє гарантувати зацікавленим сторонам задоволеність їхніх потреб, очікувань, обмежень стосовно збереження конфіденційності, цілісності та доступності інформації в організаціях. Крім того, можливе синтезування альтернативних варіантів архітектури і обирання серед них найкращого при проєктуванні систем управління інформаційною безпекою.

ЛІТЕРАТУРА

[1] *ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements*. [Valid from 2013-09-25; revised 2018-12-04]. URL: https://www.iso.org/standard/54534.html.

[2] *ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity*. [Valid from 2012-07-16; revised 2018-12-13]. URL: https://www.iso.org/ standard/44375.html.

[3] *ISO/IEC/IEEE 15026-1:2019. Systems and software engineering. Systems and software assurance. Part1: Concepts and vocabulary*. [Valid from 2019-03-08]. URL: https://www.iso.org/ standard/73567.html.

[4] *Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України: Постанова правління Національного банку України від 28.09.2017. № 95*. URL: https://zakon.rada.gov.ua/laws/show/v0095500-7#Text.

[5] *Про встановлення вимог з безпеки та захисту інфор-*

мації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 14.05.2020 № 269. URL: https:// zakon. rada. gov.ua/laws/show/z0668-20#Text.

[6] *Про прийняття попереднього рішення про сертифікацію оператора системи передачі електричної енергії: Постанова Національної комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг від 07.10.2019 № 2094*. URL: https://www.nerc.gov. ua/index.php?id=44925.

[7] *Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.2019 № 518*. URL: https://zakon.rada.gov.ua/laws/show/518 -2019-%D0%BF/print.

[8] *ISO/IEC 27701:2019. Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Requirements and guidelines*. [Valid from 2019-08-05]. URL: https://www.iso. org/standard/71670.html.

[9] *Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Дата оновлення: 04.07.2020*. URL: https://zakon.rada.gov.ua/ laws/show/80/94-%D0%B2%D1%80#Text.

[10] *ISO/IEC 27000:2018. Information technology. Security techniques. Information security management systems. Overview and vocabulary*. URL: https://www.iso. org/standard/73906. html.

[11] *ISO/IEC 27003:2017. Information technology. Security techniques. Information security management systems. Guidance*. [Valid from 2017-04-12]. URL: https:// www.iso.org/standard/63417. html.

[12] Beckers K., Heisel M., Solhaug B., Stolen K. ISMS-CORAS: A Structured Method for Establishing an ISO 27001 Compliant Information Security Management System / M. Heisel, W. Joosen, J. Lopez, F. Martinelli (eds). *Engineering Secure Future Internet Services and Systems*. Vol. 8431. Cham: Springer, 2014. pp. 315–344.

[13] Suhaimi A. I. H., Bao D., Goto Y., Cheng J. Development of ISMEE: An Information Security Management Engineering Environment. / J. Park, I. Stojmenovic, H. Jeong, G. Yi (eds). *Computer Science and its Applications*. Vol. 330. Berlin: Springer, 2015. pp. 1325–1330.

[14] Haufe K., Colomo-Palacios R., Dzombeta S., Brandis K., Stantchev V. ISMS core processes: A study. *Procedia Computer Science*. 2016. Vol. 100. pp. 339–346.

[15] Комаров М., Гончар С. Методика побудови системи управління інформаційною безпекою на об'єктах критичної інфраструктури. *Моделювання та інформаційні технології*. 2017. Вип. 81. С. 12–19. URL: http://nbuv.gov.ua/UJRN/ Mtit_2017_81_4.

[16] Achmadi D., Suryanto Y., Ramli K. On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center. *Big Data and Information Security:* International Workshop (Jakarta, 12–13 May 2018). Piscataway, 2018. - pp. 149–157.

[17] Carvalho C., Marques E. Adapting ISO 27001 to a Public Institution. *Information Systems and Technologies:* Iberian Conference (Coimbra, 19-22 June 2019). Piscataway, 2019. - pp. 1–6.

[18] Stoica L. A., Candoi-Savu R. A. Math approach of implementing ISO 27001. *Proceedings of the International Conference on Business Excellence*. 2020. Vol. 14, No. 1. pp. 521–530.

[19] Fonseca-Herrera O. A., Rojas A. E., Florez H. A Model of an Information Security Management System Based on NTC-ISO/*IEC 27001 Standard. International Journal of Computer Science*. 2021. Vol. 48, Iss. 2. pp. 213–222. URL: http://www.iaeng. org/IJCS/issues_v48/issue_2/IJCS_48_2_01.pdf.

[20] *ISO/IEC 15288:2015. Systems and software engineering. System life cycle processes*. [Valid from 2015-05-21; revised 2020-09-03]. URL: https://www. iso.org/ standard/63711.html.

[21] *Проблемы методологии системного исследования* / ред. коллегия И. В. Блауберг и др. Москва: «Мысль», 1970. - 455 с.

[22] Мохор В., Цуркан В. Системний аспект дослідження системи управління інформаційною безпекою. *Global Cyber Security Forum*: матеріали першого міжнародного науково-практичного форуму (Харків, 14–16 листопада 2019 р.). Харків, 2020. С. 74–75.

[23] Мохор В., Цуркан В. Концептуальні основи описання архітектури системи управління інформаційною безпекою. *Information Technology and Security*. July – December 2019. Vol. 7, Iss. 2 (13). pp. 197–207.

[24] Цуркан В. В. Метод аналізування вимог до систем управління інформаційною безпекою. *Кібербезпека: освіта, наука, техніка*. 2020. Том 1, № 9. С. 149–158.

[25] Цуркан В. В. Метод функціонального аналізування систем управління інформаційною безпекою. *Кібербезпека: освіта, наука, техніка*. 2020. Том 4, № 8. С. 192–201.

[26] Цуркан В. Метод синтезування структури систем управління інформаційною безпекою. *Безпека інформації*. 2020. Том 26, № 2. С. 116–122.

[27] *ISO/IEC/IEEE 42010:2011. Systems and software engineering. Architecture description. [Valid from 2011-11-24; revised 2017-08-16]*. URL: https://www. iso.org/ standard/50508.html.

[28] Цуркан В. Метод синтезування поведінки систем управління інформаційною безпекою. *Захист інформації*. Липень – Вересень 2020. Том 22, № 3. С. 189–199.

[29] *ISO/IEC 25010:2011. Systems and software engineering. Systems and software Quality Requirements*

and Evaluation (SQuaRE). System and software quality models. [Valid from 2011-03-01; revised 2017-08-16]. URL: https://www.iso.org/standard/35733.html.

МЕТОДОЛОГИЯ ПОСТРОЕНИЯ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Исследовано построение систем управления информационной безопасностью как проактивное мероприятие сохранения конфиденциальности, целостности и доступности информации. Показано, что предпосылкой его реализации в организациях является определение внешних и внутренних обстоятельств. Прежде всего это касается установления границ построения систем управления информационной безопасностью, взаимодействия с другими системами и/или организациями. Кроме этого, определяются внешние и внутренние заинтересованные стороны, их потребности, ожидания, ограничения. Этим подтверждается актуальность и необходимость разработки методологии построения систем управления информационной безопасностью. По результатам анализа последних исследований и публикаций установлено характерные для них ограничения. Их преодоление достигнуто благодаря учету технических процессов жизненного цикла систем управления информационной безопасностью. Поэтому построение систем управления информационной безопасностью сведено к анализу требований, анализу функций, синтезу архитектуры. Их соответствие потребностям, ожиданиям, ограничениям заинтересованных лиц предложено устанавливать путем синтеза поведения. Учитывая это, качество синтезированной архитектуры оценивается с помощью функциональной пригодности. Такой выбор обусловлен прежде всего ее соответствием наставлениям международных стандартов серии ISO/IEC 27k и, как следствие, возможностью оценивания степени удовлетворенности потребностей, ожиданий, ограничений заинтересованных лиц реализацией функций систем управления информационной безопасностью по синтезированному варианту архитектуры в организациях. Сформулированные задания выполняются на основе использования развитого системного подхода моделе-ориентированным. Таким образом, разработанная методология построения систем управления информационной безопасностью реализуется за пять этапов: анализа требований, анализа функций, синтеза архитектуры, синтеза поведения и оценивания функциональной пригодности синтезированной архитектуры. Это позволит гарантировать заинтересованным лицам удовлетворённость их потребностей, ожиданий, ограничений относительно сохранения конфиденциальности, целостности, доступности информации в организациях. Кроме того, станет возможным синтез альтернативных вариантов архитектуры и выбор среди них наилучшего при проектировании систем управления информационной безопасностью.

Ключевые слова: система управления информационной безопасностью, методология построения, качество систем управления информационной безопасности, функциональная пригодность архитектуры, системный подход, моделе-ориентированный подход, язык моделирования систем.

METHODOLOGY FOR DEVELOPMENT INFORMATION SECURITY MANAGEMENT SYSTEMS

The construction of information security management systems as a proactive measure of preserving confidentiality, integrity, and availability of information is investigated. It is shown that a precondition for its implementation in organizations is the definition of external and internal conditions. Primarily, this concerns the establishment of boundaries for the construction of information security management systems, interactions with other systems and/or organizations. In addition, external and internal stakeholders, their needs, expectations, and constraints are identified. This confirms the relevance and necessity of developing a methodology for development information security management systems. According to the analysis of recent studies and publications, characteristic limitations for them have been established. They have been overcome by considering the technical processes of the information security management systems lifecycle. Therefore, the development of information security management systems is reduced to requirements analysis, function analysis, architecture synthesis. It is proposed to establish its compliance with the needs, expectations, and constraints of stakeholders by synthesizing behavior. Given this, it is proposed to evaluate the quality of the synthesized architecture by functional suitability. This choice is primarily due to its compliance with the ISO/IEC 27k series of international standards and, as a result, the ability to assess the degree of needs satisfaction, expectations, stakeholder's restrictions by implementing information security management systems functions on a synthesized version of the architecture in organizations. The formulated tasks are performed based on the use of a developed model-oriented system approach. Therefore, the developed methodology for development information security management systems is implemented in five stages: requirements analysis, function analysis, architecture synthesis, behavior synthesis, and evaluation of the synthesized architecture functional suitability. This will ensure that stakeholders fulfill their needs, expectations, restrictions on maintaining the confidentiality, integrity, and accessibility of information in organizations. In addition, it will be possible to synthesize alternative architecture options and choose among them the best in the design of information security management systems.

Keywords: information security management system, development methodology, information security man-

agement system quality, architecture functional suitability, system approach, model-based systems engineering, systems modeling language.

Мохор Володимир Володимирович, член-кореспондент Національної академії наук України, доктор технічних наук, професор, директор, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України.
Orcid ID: 0000-0001-5419-9332.
E-mail: v.mokhor@gmail.com.
Мохор Владимир Владимирович, член-корреспондент Национальной академии наук Украины, доктор технических наук, профессор, директор, Институт проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины.
Mokhor Volodymyr, corresponding member of the National Academy of Sciences of Ukraine, doctor of technical sciences, professor, director, Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine.

Цуркан Василь Васильович, кандидат технічних наук, доцент, старший науковий співробітник, Інститут проблем моделювання в енергетиці імені Г.Є. Пухова Національної академії наук України.
E-mail: v.v.tsurkan@gmail.com.
Orcid ID: 0000-0003-1352-042X.
Цуркан Василий Васильевич, кандидат технических наук, доцент, старший научный сотрудник, Институт проблем моделирования в энергетике имени Г.Е. Пухова Национальной академии наук Украины.
Tsurkan Vasyl, candidate of technical sciences, associate professor, senior researcher, Pukhov Institute for Modeling in Energy Engineering of National Academy of Sciences of Ukraine.