INFORMATION SECURITY RISK MANAGEMENT

DOI 10.20535/2411-1031.2020.8.1.218012
УДК [004(056.53+413.4)::001.51]::303.732

ВОЛОДИМИР МОХОР,
ВАСИЛЬ ЦУРКАН,
ОЛЕКСАНДР БАКАЛИНСЬКИЙ,
ЯРОСЛАВ ДОРОГИЙ

МЕТОД КОНЦЕПТУАЛІЗУВАННЯ СИСТЕМНИХ ДОСЛІДЖЕНЬ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Запропоновано метод концептуалізування комплексних досліджень систем управління інформаційною безпекою. За основу його розроблення взято розвинений системний підхід шляхом доповнення моделеорієнтованим. Таке розширення дозволило уніфікувати онтологічне представлення комплексних досліджень систем управління інформаційною безпекою. Насамперед виокремити завдання як основні поняття і встановити відношення між ними. Серед них виділено чотири класи: аналізування вимог, аналізування функцій, синтезування архітектури, синтезування поведінки. Вхідними даними для аналізування вимог є потреби як внутрішніх, так і зовнішніх зацікавлених сторін. За ними встановлюється правильність формулювання вимог, відповідність індивідуальним і груповим характеристикам. Після цього визначаються відношення між вимогами до систем управління інформаційною безпекою. Специфікація вимог використовується як вхідні дані при аналізуванні функцій систем управління інформаційною безпекою. Для кожної з них встановлюються вхідні, вихідні дані, обмеження і ресурси. Таке представлення дозволяє обґрунтувати визначення варіантів використання систем управління інформаційною безпекою. Їх реалізування досягається синтезуванням архітектури. Для цього обираються блоки, кожним з яких відображаються відповідні елементи архітектури та встановлюються відношення між ними. Її функціональна придатність визначається синтезуванням поведінки систем управління інформаційною безпекою. Вхідними даними для розв’язання цього завдання є їхня архітектура. При цьому може синтезуватися поведінка як окремого елементу (блоку), так і системи управління інформаційною безпекою загалом. Це виконується через діяльність, взаємодію і змінення станів. Завдяки цьому знаходиться функціональна придатність/непридатність синтезованої архітектури відповідно до вимог зацікавлених сторін. Уніфікованість представлень виокремлених завдань комплексних досліджень систем управління інформаційною безпекою досягається використанням мови моделювання систем. На основі отриманих результатів можливе визначення альтернативних варіантів архітектури та обирання серед них найкращого за її функціональною придатністю.

Ключові слова: система управління інформаційною безпекою, комплексні дослідження, онтологія завдань, системний підхід.

Постановка проблеми. Архітектура систем управління інформаційною безпекою визначається на етапі розроблення їх життєвого циклу. Характерною особливістю даного процесу є орієнтованість перш за все на задоволення потреб зацікавлених сторін. Тож процесу архітектуризації передує встановлення сфери та меж розроблення систем управління інформаційною безпекою [1], [2]. На основі потреб, очікувань і пов’язаних з ними обмежень аналізуються вимоги – від загальних (управляти інформаційною безпекою) до часткових (ідентифіковувати наяні засоби забезпечення інформаційної безпекою). При цьому встановлюються правильність їх формулювань, відповідність індивідуальним і груповим характеристикам, а також відношень між ними. Задоволеність вимог забезпечується завдяки

© В. Мохор, В. Цуркан, О. Бакалинський, Я. Дорогий, 2020

аналізуванню функцій. Залежно від цього синтезується архітектура систем управління інформаційною безпекою в організаціях, елементами якої реалізуються проаналізовані функції. Тому забезпеченістю їх виконання системами управління інформаційною безпекою у конкретному навколишньому середовищі (організації) відповідно до вимог зацікавлених сторін визначається функціональна придатність архітектури [3]. Її підвищення досягається завдяки урахуванню потреб, очікувань і пов'язаних з ними обмежень зацікавлених сторін. Тоді як для визначення функціональної придатності архітектури синтезується поведінка систем управління інформаційною безпекою.

Такою послідовністю демонструється включення кожним з наступних прийомів попередніх, наприклад: аналіз вимог → аналіз функцій, аналіз вимог → аналіз функцій → синтез архітектури, аналіз вимог → аналіз функцій → синтез архітектури → синтез поведінки. До того ж переходом від одного прийому до іншого обумовлюється вирішення нових часткових завдань, наприклад, проаналізувати вимоги → проаналізувати функції → синтезувати архітектуру. Цим визначається комплексний характер досліджень систем управління інформаційною безпекою. Тоді як сукупність зазначених прийомів, що застосовуються до систем управління інформаційною безпекою, тлумачитиметься як комплексні дослідження [4], [5]. Отже, розроблення методу концептуалізування комплексних досліджень систем управління інформаційною безпекою є актуальним завданням.

Аналіз останніх досліджень і публікацій. Дослідженню систем управління інформаційною безпекою приділено увагу в [6] - [17]. Особливості розроблення і впровадження систем управління інформаційною безпекою в організаціях енергетичного сектору досліджено в [6]. Насамперед встановлюється можливість їх інтегрування з комплексними системами захисту інформації. Окрема увага приділяється документуванню процесу розроблення систем управління інформаційною безпекою на основі серії міжнародних стандартів ISO/IEC 27x. Це досягається його реалізованістю у межах циклу заходів «Плануй – Виконуй – Перевіряй – Дій». Розроблення систем управління інформаційною безпекою автоматизовано в [7]. Для цього на основі ризиків розробляється відповідний фреймворк. Ним реалізуються вимоги міжнародного стандарту ISO/IEC 27001 до процесу розроблення систем управління інформаційною безпекою. З огляду на це забезпечується узгодженість між виконанням завдань та засобами оброблення ризиків. Це досягається формуванням списків інформаційних активів, уразливостей, загроз і ризиків. Як наслідок, оперативним відслідковуванням змін у даних списках. Моделі управління інформаційною безпекою кіберфізичних систем проаналізовано в [8]. Для цього використано міжнародні стандарти ISO/IEC TR 13335 та ISO/IEC 27001. Їх розглянуто як основу управління комплексною системою безпеки кіберфізичних систем. Даний процес узгоджується з циклом «Плануй – Виконуй – Перевіряй – Дій». Структуру такого управління розширено на рівні життєвого циклу інформації та багаторівневої моделі «кібернетичний простір – комунікаційне середовище – фізичне середовище». Досліджується Обирання засобів забезпечення безпеки за міжнародним стандартом ISO/IEC 27002 досліджено в [9]. Зокрема, формалізується їх описання і забезпечення підтримання прийняття відповідних рішень. Формалізоване представлення засобів забезпечення безпеки використовується для оброблення ризиків. Величина ризику оцінюється за допомогою запропонованої системи підтримки прийняття рішення. Воно приймається зі залученням експертів і розпорядників інформаційних активів. Отримані при цьому результати використовуються як вхідні дані при прийнятті рішень про вибір заходів забезпечення безпеки на етапі оброблення ризиків. Систему управління інформаційною безпекою за вимогами міжнародного стандарту ISO/IEC 27001 проаналізовано в [10]. Висвітлюється складність її розроблення без існування детального плану. Ним визначається модель зрілості організації до впровадження системи управління інформаційною безпекою. За потреби приймається рішення про необхідність досягнення нею заданого рівня і, як наслідок, готовності до розроблення даної системи в

організації. Імітаційну модель функціонування системи управління інформаційною безпекою розроблено в [11]. Нею враховуються особливості об'єкта інформаційної діяльності, зокрема, судна. Пропонується схема функціонування системи управління інформаційною безпекою. Вона визначається блоками дестабілізуючих факторів, моделі захищеної системи, первинних і вторинних наслідків, засобів контролювання і управління, надійності і відновлення, оцінювання функціонування системи і прийняття рішень. За основу дослідження розробленої схеми взято наявність (або можливість накопичення) статистичних даних. Однак, на практиці їх накопичення ускладнене, зокрема, для сфери інформаційної безпеки. Крім того, таким представленням залишаються поза увагою вимоги до функціонування систем управління інформаційною безпекою за міжнародним стандартом ISO/IEC 27001. Нормативний аспект розроблення і впровадження таких систем на об'єктах критичної інфраструктури описано в [12]. Для цього використано сімейство міжнародних стандартів ISO/IEC 27x та процесний підхід. Окрему увагу приділено аналізуванню основних нормативних документів даного сімейства. Це дозволило виокремити серед них найбільш пріоритетні для розроблення і впровадження систем управління інформаційною безпекою на об'єктах критичної інфраструктури. Насамперед міжнародний стандарт ISO/IEC 27001. З огляду на це викладено стадії його використання, а саме: «Плануй – Виконуй – Перевіряй – Дій». Системи аудиту та контролю стану інформаційної безпеки на об'єктах критичної інфраструктури досліджено в [13]. Серед них аналізується модель системи управління інформаційної безпекою. Її побудова орієнтована на впровадження взаємонезалежних процесів управління насамперед інформаційними активами, ризиками, їх документального забезпечення. Тому таке впровадження зводиться до створення необхідної документації, якою регламентуються зазначені процеси. Зокрема, для них встановлюються відповідальні особи та, як наслідок, розробляються посадові інструкції. Моделі оцінювання зрілості забезпечення інформаційної безпеки проаналізовано в [14]. Розглянута аналогія їхніх елементів з елементами міжнародного стандарту ISO/IEC 27001. Як основу моделей зрілості процесів забезпечення інформаційної безпеки взято оцінювання ризиків. З огляду на це визначаються метрики для встановлення їх реалізованості в організаціях. Зокрема пропонуються такі моделі зрілості як SSE-CMM, C2M2, NICE і O-ISM3. Серед них обираються C2M2 і O-ISM3 з огляду на застосовність до систем управління інформаційною безпекою. Цим гарантується ефективність діяльності організацій [6] - [17].

Метою статті є уніфікування представлень комплексних досліджень систем управління інформаційною безпекою шляхом виокремлення завдань як основних понять і встановлення відношень між ними.

Виклад основного матеріалу дослідження. Комплексні дослідження систем управління інформаційною безпекою концептуалізовано виокремленням чотирьох класів завдань

$$TS = \{TS_1, TS_2, TS_3, TS_4\},$$

де TS_1 – проаналізувати вимоги до систем управління інформаційною безпекою (рис. 1). Вхідними даними для розв'язання цього завдання є вимоги як внутрішніх, так і зовнішніх зацікавлених сторін. Вони визначаються на основі потреб, очікувань і обмежень. На їх основі аналізується правильність формулювання вимог як обов'язкових тверджень, а також відповідність індивідуальним і груповим характеристикам. Завдяки цьому встановлюються відношення між вимогами до систем управління інформаційною безпекою. Вихідними даними є їх специфікація діаграмою мовою моделювання SysML.

TS_2 – проаналізувати функції систем управління інформаційною безпекою (рис. 1). Вхідними даними для розв'язання цього завдання є діаграма вимог до систем управління інформаційною безпекою мовою моделювання SysML. Вони задовольняються визначенням функцій. Для кожної з них встановлюються вхідні, вихідні дані, обмеження і

ресурси. Як діяльність (функція верхнього рівня) розглядається управління інформаційною безпекою в організації. Завдяки цьому визначаються варіанти використання систем управління інформаційною безпекою. Вихідними даними є їх специфікація діаграмою мовою моделювання SysML.

TS_3 – синтезувати архітектуру систем управління інформаційною безпекою (рис. 2). Вхідними даними для розв'язання цього завдання є діаграма варіантів використання систем управління інформаційною безпекою мовою моделювання SysML. Для їх реалізування обираються блоки, кожним з них моделюється відповідний елемент архітектури (наприклад, діяльність – система (підсистема), процес – комплекс, функція – компонент). Завдяки цьому визначаються відношення між блоками та, як наслідок, синтезується архітектура систем управління інформаційною безпекою. Вихідними даними є їх архітектура, що специфікується діаграмою блоків мовою моделювання SysML.

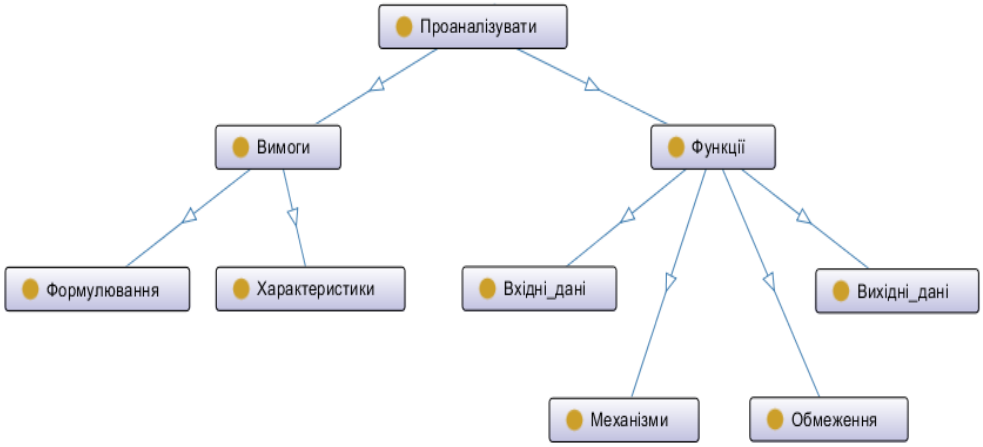

Рисунок 1 – Онтологія завдань аналізу вимог і функцій систем управління інформаційною безпекою

TS_4 – синтезувати поведінку систем управління інформаційною безпекою (рис. 2). Вхідними даними для розв'язання цього завдання є архітектура систем управління інформаційною безпекою, зокрема, діаграма блоків мовою моделювання SysML. При цьому може синтезуватися поведінка як окремого елементу (блоку), так і системи загалом. Це досягається через діяльність, взаємодію і змінення станів. Кожне з даних часткових завдань розв'язується окремо. Характерною особливістю такого представлення поведінки діяльністю є орієнтованість на встановлення умов виконання дій елементами (блоками) або системою загалом. Часові особливості передавання і приймання об'єктів відображаються через їхнє взаємодіяння. Основою такої взаємодії є встановлення послідовності обміну повідомленнями. Змінення станів елементами (блоками) або системами управління інформаційною безпекою при настанні визначених умов орієнтоване на описання поведінки за схемою «стан – перехід». Вихідними даними є визначення функціональної придатності архітектури систем управління інформаційною безпекою відповідно до вимог зацікавлених сторін.

Комплексні дослідження систем управління інформаційною безпекою концептуалізуються за системним підходом, що доповнюється моделеорієнтованим. Його використання дозволяє досліджувати дані системи як цілісні об'єкти. Кожен з них складаються з структурно та функціонально взаємопов'язаних відношеннями елементів. Цілісність об'єкта забезпечується сукупністю стійких зв'язків між елементами. Тому виокремлення класів завдань і орієнтоване на синтез архітектури систем управління інформаційною безпекою.

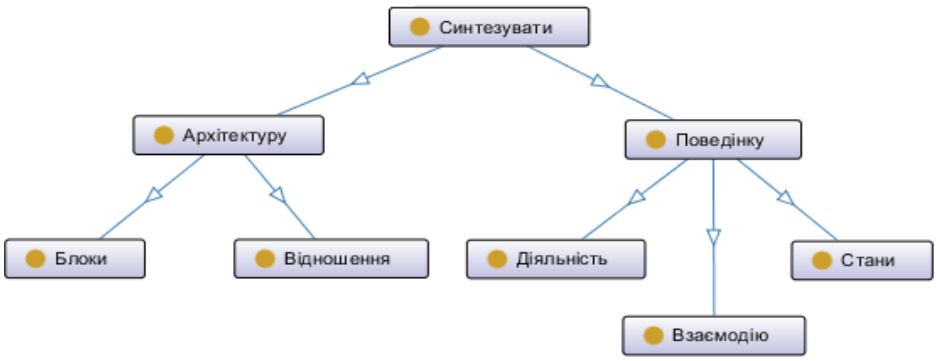

Рисунок 2 – Онтологія завдань синтезу архітектури та поведінки систем управління інформаційною безпекою

Тож

$$O_{TS} = \{TS, R_{TS}\},$$

де O_{TS} – онтологія завдань комплексних досліджень систем управління інформаційною безпекою (рис. 3);

TS – множина завдань комплексних досліджень систем управління інформаційною безпекою;

R_{TS} – відношення між окремими завданнями комплексних досліджень систем управління інформаційною безпекою.

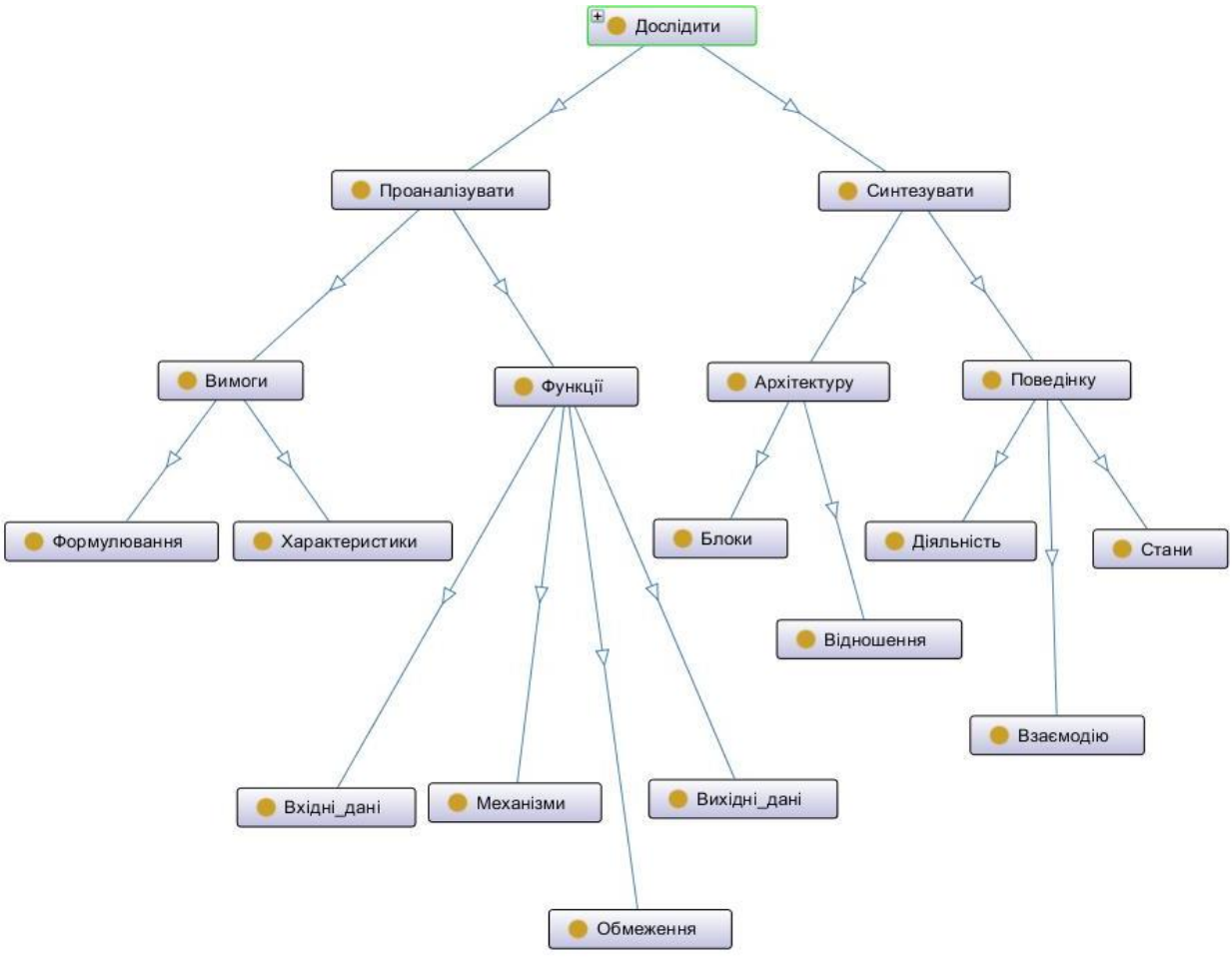

Рисунок 3 – Онтологія завдань комплексних досліджень систем управління інформаційною безпекою

Висновки. Виокремлені завдання можуть формулюватися з огляду на специфіку організацій. Тож однозначність їх тлумачень забезпечується концептуалізуванням комплексних досліджень систем управління інформаційною безпекою завдяки онтологічному представленню. До того ж це обумовлено тим, що відомі напрями досліджень орієнтовані, наприклад, на: класифікування онтологій забезпечення інформаційної безпеки за специфічними та загальними категоріями. Серед специфічних виокремлено [15] - [17] онтології забезпечення безпеки вебслужб, мереж на основі ризиків; онтології стандартів оцінювання ризиків інформаційної безпеки стосовно визначення вартості втрат унаслідок реалізації загроз; перевіряння відповідності настановам міжнародного стандарту ISO/IEC 27002 представленням його онтологічною структурою забезпечення безпеки; формалізування відношень між національними та міжнародними стандартами забезпечення інформаційної безпеки створенням онтології відповідної предметної області; формалізування опису заходів забезпечення інформаційної безпеки за міжнародним стандартом ISO/IEC 27002 та системи підтримки прийняття рішень про їх обирання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] В. В. Мохор, О. О. Бакалинський, та В. В. Цуркан, "Архітектура системи управління інформаційною безпекою", на *XX ювілейній міжнародній науково-практичній конференції Безпека інформації в інформаційно-телекомунікаційних системах*, Київ, 2018, с. 38.

[2] В. В. Мохор, В. В. Цуркан, Я. Ю. Дорогий, та Ю. М. Штифурак, "Архітектуризування системи управління інформаційною безпекою", *на VI міжнародній науково-практичній конференції Актуальні питання забезпечення кібербезпеки та захисту інформації*. Київ, 2020. С. 82-84.

[3] International Organization for Standardization. (2011, March 01). *ISO/IEC 25010, Systems and software engineering. Systems and software Quality Requirements and Evaluation (SQuaRE). System and software quality models*. [Online]. Available: https://www.iso.org/standard/35733.html. Accessed on: Okt. 30, 2019.

[4] И. В. Блауберг и др., *Проблемы методологии системного исследования*. Москва : «Мысль», 1970.

[5] Академічний тлумачний словник української мови (1970–1980 рр.). [Електронний ресурс]. Доступно: http://sum.in.ua/. Дата звернення: Жовт. 30, 2019.

[6] М. Комаров, та С. Гончар, "Методика побудови системи управління інформаційною безпекою на об'єктах критичної інфраструктури", *Моделювання та інформаційні технології*, Iss. 81, pp. 12-19, 2017. [Електронний ресурс]. Доступно: http://nbuv.gov.ua/UJRNMtit_2017_81_4. Дата звернення: Жовт. 30, 2019.

[7] M. Brunner, C. Sillaber, and R.Breu, "Towards Automation in Information Security Management Systems", in *Proc. IEEE International ConferenceSoftware Quality, Reliability and Security (QRS)*, Prague, 2017. pp. 160-167, doi: https://doi.org/10.1109/QRS. 2017.26.

[8] В. Б. Дудикевич, Г. В. Микитин, та А. І. Ребець, "До проблеми управління комплексною системою безпеки кіберфізичних систем", *Вісник Національного університету «Львівська політехніка» «Інформаційні системи та мережі»*, Вип. 901, 2018, с. 10-21. [Електронний ресурс]. Доступно: http://ena.lp.edu.ua:8080/handle/ntb/44544. Дата звернення: Жовт. 30, 2019.

[9] S. Fenz, and T. Neubauer, "Ontology-based information security compliance determination and control selection on the example of ISO 27002". *Information and Computer Security*, vol. 26, iss. 5, pp. 551-567, 2018, doi: http://dx.doi.org/10.1108/ ICS-02-2018-0020.

[10] D. Proença, and J. Borbinha, "Information Security Management Systems – A Maturity Model Based on ISO/IEC 27001", in *Business Information Systems. Vol. 320*. W. Abramowicz, A. Paschke (eds). Cham: Springer, 2018. pp. 102-114, 2018, doi: https://doi.org/10.1007/978-3-319-93931-5_8.

[11] Д. Бабійчук, та М. Турти, "Дослідження системи управління інформаційною безпекою судна на мережі Петрі", на *7-й Міжнародній науково-технічної конференції Інформаційні системи та технології*, Харків, 2018. с. 392-395. [Електронний ресурс]. Доступно: http://istconf.nure.ua/archive/ist_ 2018.pdf. Дата звернення: Жовт. 30, 2019.

[12] М. Ю. Комаров, С. Ф. Гончар, та А. В. Ониськова, "Нормативний аспект побудови та впровадження системи управління інформаційною безпекою на об'єктах критичної інфраструктури", *Моделювання та інформаційні технології*, Вип. 82, с. 40-48, 2018. [Електронний ресурс]. Доступно: http://nbuv.gov.ua/UJRN/Mtit_2018_82_8 Жовт. 30, 2019.

[13] О. Юдін, Р. Зюбіна, та О.Матвійчук-Юдіна, "Сучасні практики впровадження системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури", *Наукоємні технології*, т. 41, № 1, с. 36-43, 2019, doi: http://dx.doi.org/10.18372/ 2310-5461.41.13527.

[14] М. Коломыцев, С. Носок, и Р. Тоцкий, "Сравнительный анализ моделей оценки зрелости информационной безопасности", *Захист інформації*, т. 21, no. 4, с. 224-232, doi: http://dx.doi.org/10.18372/2410-7840. 21.14337.

[15] V. Casola, R. Catelli, and A. D. Benedictis, "A First Step Towards an ISO-Based Information Security Domain Ontology", in *Proc. IEEE International Conference Enabling Technologies: Infrastructure for Collaborative Enterprises*, Napoli, 2019. pp. 334-339, doi: https://doi.org/ 10.1109/WETICE.2019.00075.

[16] I. Meriah, and L. B. A., "Rabai Comparative Study of Ontologies Based ISO 27000 Series Security Standards", *Procedia Computer Science*, vol. 160, pp. 85-92, 2019, doi: https://doi.org/ 10.1016/j.procs.2019.09.447.

[17] V. Diamantopoulou, A. Tsohou, and M. Karyda, "General Data Protection Regulation and ISO/IEC 27001:2013: Synergies of Activities Towards Organisations' Compliance", in *Trust and Privacy in Digital Business*. Vol. 11711, S.Gritzalis, E. Weippl, S. Katsikas, G. Anderst-Kotsis, A. Tjoa, I. Khalil (eds), Cham : Springer, 2019, pp. 94-109, doi: https://doi.org/10.1007/978-3-030-27813-7_7.

Стаття надійшла до редакції 17.02.2020.

REFERENCE

[1] V. V. Mokhor, V. V. Tsurkan, and O. O. Bakalynskyi, "Information security management system architecture", in *Proc. XX Anniversary International Scientific Conference on Information Security in Information and Telecommunication Systems*. Kyiv, 2018, pp. 38.

[2] V. V. Mokhor, V. V. Tsurkan, Ya. Yu. Dorohyi, and Yu. M. Shtyfurak, "Information security management system architecturing", in *Proc. International Scientific Conference on Current issues of cybersecurity and information security*, Kyiv, 2020. pp. 82-84.

[3] International Organization for Standardization. (2011, March 01). *ISO/IEC 25010, Systems and software engineering. Systems and software Quality Requirements and Evaluation (SQuaRE). System and software quality models*. [Online]. Available: https://www.iso.org/ standard/35733.html. Accessed on: Okt. 30, 2019.

[4] I. V. Blauberg et al. (eds), *Methodological problems of system research*, Moskow : "Mysl", 1970.

[5] Academic explanatory dictionary of the Ukrainian language (1970-1980). [Online]. Available: http://sum.in.ua/. Accessed on: Okt. 30, 2019.

[6] M. Komarov, and S. Gonchar, "Method of constructing information security management system for critical infrastructure", *Modeling and Information Technology*, no. 81, pp. 12-19, 2017, [Online]. Available: http://nbuv.gov.ua/UJRN/ Mtit_2017_81_4 Accessed on: Okt. 30, 2019.

[7] M. Brunner, C. Sillaber, and R.Breu, "Towards Automation in Information Security Management Systems", in *Proc. IEEE International ConferenceSoftware Quality, Reliability and Security (QRS)*, Prague, 2017. pp. 160-167, doi: https://doi.org/10.1109/QRS. 2017.26.

[8] V. Dudykevych, G. Mykytyn, and A. Rebets, "On the Problem of Complex Security System Management of Cyber-physical Systems", *The Journal of Lviv Polytechnic National University "Information Systems and Networks"*, no. 901, pp. 10-21. 2018. [Online]. Available: http://ena.lp.edu.ua:8080/handle/ntb/44544. Accessed on: Okt. 30, 2019.

[9] S. Fenz, and T. Neubauer, "Ontology-based information security compliance determination and control selection on the example of ISO 27002", *Information and Computer Security*, vol. 26, iss. 5, pp. 551-567, 2018, doi: http://dx.doi.org/10.1108/ ICS-02-2018-0020.

[10] D. Proença, and J. Borbinha, "Information Security Management Systems – A Maturity Model Based on ISO/IEC 27001", in *Business Information Systems. Vol. 320*. W. Abramowicz, A. Paschke (eds). Cham: Springer, 2018. pp. 102-114, 2018, doi: https://doi.org/ 10.1007/978-3-319-93931-5_8.

[11] D. Babiichuk, and M. Turty "Investigation of the ship's information security management system on the Petri net", in *Proc. International Scientific Conference on Information systems and technologies*. Kharkiv, 2018. pp. 392-395. [Online]. Available: http://istconf.nure.ua/archive/ist_2018.pdf. Accessed on: Okt. 30, 2019.

[12] M. Komarov, S. Gonchar, and A. Onyskova, "Legal aspects of construction and implementation of information security management system for critical infrastructure", *Modeling and Information Technology*, no. 82, pp. 40–48, 2018. [Online]. Available: http://nbuv.gov.ua/UJRN/Mtit_2018_82_8. Accessed on: Okt. 30, 2019.

[13] O. Yudin, R. Ziubina, and O. Matviichuk-Yudina, "The modern practices of implementation of the information security audit system on the critical infrastructure objects", *Science-Based Technologies*, vol. 41, no. 1, pp. 36-43, 2019, doi: http://dx.doi.org/10.18372/ 2310-5461.41.13527.

[14] M. Kolomytsev, S. Nosok, and R. Totskyi, "Comparative analysis of maturity models to evaluate information security", *Ukrainian information security research journal*, vol. 21, no. 4, pp. 224-232, 2019, doi: 10.18372/ 2410-7840.21.14337.

[15] V. Casola, R. Catelli, and A. D. Benedictis, "A First Step Towards an ISO-Based Information Security Domain Ontology", in *Proc. IEEE International Conference Enabling Technologies: Infrastructure for Collaborative Enterprises*, Napoli, 2019. pp. 334-339, doi: https://doi.org/10.1109/WETICE.2019.00075.

[16] I. Meriah, and L. B. A., "Rabai Comparative Study of Ontologies Based ISO 27000 Series Security Standards", *Procedia Computer Science*, vol. 160, pp. 85-92, 2019, doi: https://doi.org/10.1016/j.procs.2019.09.447.

[17] V. Diamantopoulou, A. Tsohou, and M. Karyda, "General Data Protection Regulation and ISO/IEC 27001:2013: Synergies of Activities Towards Organisations' Compliance", in *Trust and Privacy in Digital Business*. Vol. 11711, S.Gritzalis, E. Weippl, S. Katsikas, G. Anderst-Kotsis, A. Tjoa, I. Khalil (eds), Cham : Springer, 2019, pp. 94-109, doi: https://doi.org/10.1007/978-3-030-27813-7_7.

VOLODYMYR MOKHOR,
VASYL TSURKAN,
OLEKSANDR BAKALYNSKYI,
YAROSLAV DOROHYI

METHOD FOR CONCEPTUALIZING SYSTEM STUDIES OF INFORMATION SECURITY MANAGEMENT SYSTEMS

A method for conceptualizing system studies of information security management systems is proposed. Its development is based on a developed system approach by supplementing it with a model-oriented. This extension allowed to unify the ontological representation of system studies of information security management systems. First, identify the tasks as basic concepts and establish relations between

them. Among them, four classes are defined: requirements analysis, function analysis, architecture synthesis, behavior synthesis. The inputs for requirements analysis are the needs of both internal and external stakeholders. They are followed by the correctness of requirements formulation, compliance with personal and group features. The relationships between the requirements for information security management systems are then determined. The requirements specification is used as input data when analyzing the functions of information security management systems. For each of them the inputs, outputs, constraints, and resources are established. Such a representation allowed to justify the definition of options for the use of information security management systems. The implementation of options for using information security management systems is achieved by synthesizing the architecture. For this purpose, blocks are selected, each of which maps the corresponding elements of the architecture and establishes the relationships between them. Its functional usability is determined by synthesizing the behavior of information security management systems. The input data for solving this problem is their architecture. In this case, the behavior of an individual element (block) or the information security management system can be synthesized. This is achieved through activities, interactions, and state changes. Due to this, the functional suitability/unsuitability of the synthesized architecture is found following the requirements of stakeholders. Unified views of separate tasks of system research of information security management systems are achieved using the system modeling language. Based on the results obtained, it is possible to determine alternative architecture options and select the best among them in terms of their functional suitability.

Keywords: information security management system, system studies, task ontology, system approach.

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, Київ, Україна.

ORCID: 0000-0001-5419-9332.

E-mail: v.mokhor@gmail.com.

Цуркан Василь Васильович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0003-1352-042X.

E-mail: v.v.tsurkan@gmail.com.

Бакалинський Олександр Олегович, заступник директора, департамент кіберзахисту, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Київ, Україна.

ORCID: 0000-0001-9712-2036.

E-mail: baov@meta.ua.

Ярослав Юрійович Дорогий, кандидат технічних наук, доцент, доцент кафедри автоматики і управління в технічних системах, Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0003-3848-9852.

E-mail: argusyk@gmail.com.

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, Kyiv, Ukraine.

Tsurkan Vasyl, candidate of technical sciences, associate professor, associate professor at the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection National technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Bakalynskyi Oleksandr, deputy director, department of cyber protection, Administration of State serves of special communication and information protection of Ukraine, Kyiv, Ukraine.

Dorohyi Yaroslav, candidate of technical sciences, associate professor, associate professor at the automation and control in technical systems academic department, National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.