КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№1 (9), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.9.149158
УДК 004[056.53+413.4]::303.732.4

Цуркан Василь Васильович
кандидат технічних наук, 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 АНАЛІЗУВАННЯ ВИМОГ ДО СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Анотація. Розглянуто процес аналізування вимог до систем управління інформаційною безпекою. Показано обов'язковість дотримання їхнього переліку настановам міжнародного стандарту ISO/IEC 27001. Завдяки цьому надається впевненість зацікавленим сторонам належного управління ризиками інформаційної безпеки з прийнятним рівнем. Це обумовлюється врахуванням внутрішніх і зовнішніх обставин впливання на мету та досягнення очікуваного результату діяльності організацій. До того ж визначенням зацікавлених сторін, їхніх потреб та очікувань від розроблення систем управління інформаційною безпекою. При цьому встановлено, що нині здебільшого зосереджується увага на врахуванні вимог до процесу розроблення даних систем або до забезпечення інформаційної безпеки в організаціях. При цьому поза увагою залишено перетворення потреб, очікувань і пов'язаних з ними обмежень зацікавлених сторін у відповідне системне рішення. Ці обмеження подолано завдяки методу аналізування вимог до систем управління інформаційною безпекою. Його використання дозволяє на основі потреб, очікувань і пов'язаних з ними обмежень зацікавлених сторін визначити відповідні твердження за встановленими синтаксичними формами. Кожне з них перевіряється стосовно правильності формулювання і відповідності характеристикам як індивідуальної вимоги, так і набору вимог. Для їх систематизування, встановлення відношень використано графічну нотацію SysML. З огляду на це вимогу розглянуто як стереотип класу з властивостями та обмеженнями. Для встановлення взаємозв'язків між вимогами використано відношення. Їхнє поєднання відображається діаграмою у графічній нотації SysML і, як наслідок, дозволяє специфікувати вимоги до систем управління інформаційною безпекою. У перспективах подальших досліджень планується на основі запропонованого методу розробити її логічну структуру.

Ключові слова: система управління інформаційною безпекою, вимога, характеристика вимоги, аналізування вимог, діаграма вимог, SysML.

1. ВСТУП

Системи управління інформаційною безпекою розробляються, впроваджуються, використовуються, контролюються, переглядаються, підтримуються і вдосконалюються завдяки визначенню вимог до них [1]. На це впливають потреби, мета, процеси і структура організацій. Перелік вимог узагальнюється і наводиться у міжнародному стандарті ISO/IEC 27001:2013 (з 2015 року ДСТУ ISO/IEC 27001 [2]) незалежно від їх типу, величини та природи [1], [3]. Дотримання цього переліку є обов'язковим при розробленні систем управління інформаційною безпекою. Завдяки цьому можливе встановлення відповідності міжнародному стандарту ISO/IEC 27001:2013. Як наслідок, задоволення потреб і очікувань зацікавлених сторін від впровадження зазначених систем в організаціях. Насамперед збереження таких властивостей інформації як конфіденційність, цілісність та доступність шляхом

оцінювання ризиків інформаційної безпеки. Це сприяє наданню впевненості зацікавленим сторонам належного управління ними з прийнятним рівнем [1], [4].

Тож визначення вимог до систем управління інформаційною безпекою для їх розроблення в організаціях є актуальним.

Постановка проблеми. Передумовою розроблення систем управління інформаційною безпекою є визначення сфери їх застосування в організаціях. Для цього встановлюються відповідні межі та, власне, існування такої можливості [1], [5]. Ця можливість обумовлюється, по-перше, врахуванням внутрішніх і зовнішніх обставин впливання на мету та досягнення очікуваного результату діяльності організацій. Наприклад [6], [7], надання послуг у галузях енергетики [8], інформаційно-комунікаційних технологій [9], електронних комунікацій [10], у банківському та фінансовому секторах [11].

По-друге, визначенням зацікавлених сторін, їхніх потреб та очікувань від розроблення систем управління інформаційною безпекою. Стосовно організацій вони розглядаються як внутрішні (наприклад [5], керівництво, працівники, фахівці з інформаційної безпеки), так і зовнішні (наприклад [5], інвестори, постачальники, конкуренти, споживачі). Це означає, що кожна з них або може впливати, або перебувати під впливом. Тому потреби, очікування зацікавлених сторін і пов’язані з ними обмеженням тлумачаться як вимоги до систем управління інформаційною безпекою. Вони специфікуються завдяки дослідженню, наприклад [12], стосовно зрозумілості, повноти, однозначності. Ці завдання вирішуються у межах аналізування вимог [2], [12], [13].

Водночас нині здебільшого зосереджується увага на врахуванні вимог до процесу розроблення систем управління інформаційною безпекою, з одного боку. Тоді як з іншого – до забезпечення збереженості конфіденційності, цілісності та доступності інформації в організаціях. При цьому поза увагою залишається перетворення потреб і очікувань зацікавлених сторін у відповідне системне рішення. Як наслідок, це призводить до складнощів гарантування досягненості системами управління інформаційною безпекою запланованих результатів впровадження [2].

Аналіз останніх досліджень і публікацій. Розробленню і впровадженню систем управління інформаційною безпекою в організаціях приділено увагу в [1], [3], [5], [14] - [20]. Так, актуальні питання розроблення даних систем розглянуто в [14]. Серед них виокремлено та розкрито процесну модель. Її застосовність зведено до відповідності вимогам [1]. Дану модель взято за основу при створенні інженерного середовища системи управління інформаційною безпекою [15]. Його використання орієнтоване на документальне забезпечення впровадженості настанов міжнародних стандартів серії ISO/IEC 27k. Вимоги та засоби забезпечення інформаційної безпеки розглядаються у [16]. Для їх переглядання і вдосконалювання пропонується п’ять фаз: підготовлення, перевіряння, класифікування, вдосконалення і переглядання. Вирішення завдань розроблення ефективної системи управління інформаційною безпекою на прикладі патентного відомства викладено в [17]. Запропоновано формалізовані моделі та методи аналізування предметної області, оцінювання і оброблення ризиків. Водночас як окремий етап описано формування специфікацій інформаційних потреб користувачів для побудови об’єктної канонічної структури патентної бази даних. Напрями подолання складнощів розроблення і впровадження систем управління інформаційною безпекою пропонуються у [18]. Зокрема, вони долаються завдяки оцінюванню поточного рівня зрілості. За його результатами встановлюється необхідність розроблення плану вдосконалення як багатокрокової перспективи. Застосовність вимог Регламенту зі захисту персональних даних і міжнародного стандарту ISO/IEC 27001 при розробленні систем управління інформаційною безпекою розглянуто в [19]. Їх

узгодженість досягається шляхом використання запропонованого фреймворку. Завдання формування прийнятних варіантів організаційної структури автоматизованої системи управління інформаційною безпекою вирішено в [20]. При цьому організаційну структуру розглянуто як сукупність пунктів управління з відношеннями підпорядкованості між ними.

Мета статті. Специфікування вимог до систем управління інформаційною безпекою методом їх аналізування.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Аналізування вимог до систем управління інформаційною безпекою в організаціях орієнтоване на встановлення відповідності індивідуальним, груповим характеристикам, систематизування, виявлення відношень між ними і, як наслідок, специфікування. Вхідними даними для цього процесу є потреби, очікування і пов'язані з ними обмеження з боку зацікавлених сторін [1], [21]. Крім того встановлені внутрішні та зовнішні обставини, що впливають або можуть впливати на діяльність організацій і функціонування систем управління інформаційною безпекою (див., наприклад [1], [22], рис. 1), зокрема.

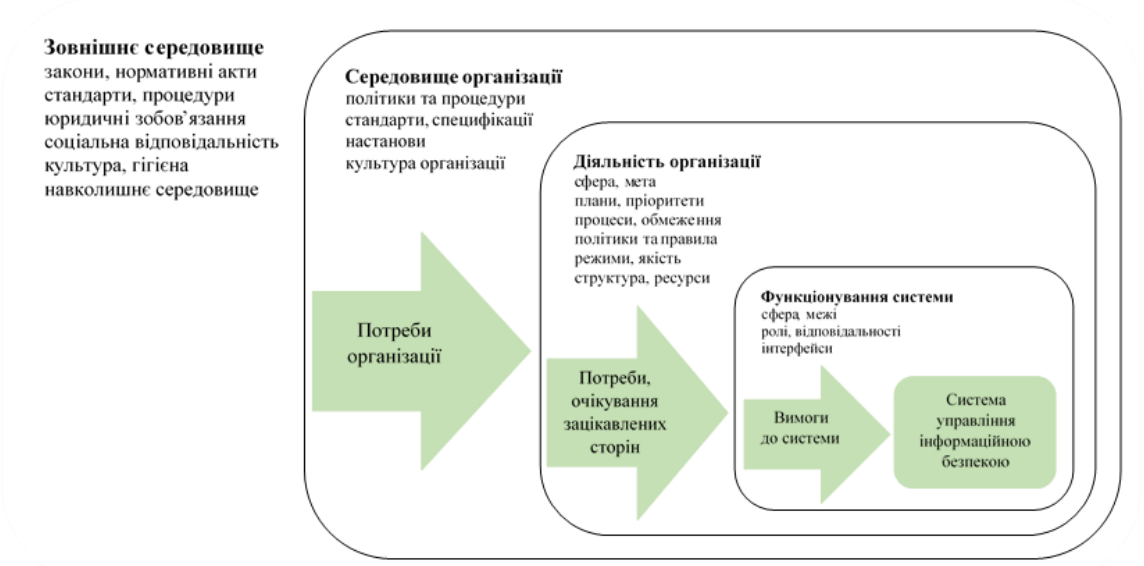

Рис. 1. Представлення сфери застосування і вимог до систем управління інформаційної безпекою в організаціях

На основі потреб, очікувань і пов'язаних з ними обмежень зацікавлених сторін визначаються вимоги. Кожна з них формулюється як твердження, яким розкривається дія суб'єкта над об'єктом, умови такої діяльності. Наприклад: коли оцінка ризику більша за рівень прийнятності, то система управління інформаційною безпекою повинна обробити неприйнятний ризик за варіантом зменшення; система управління інформаційною безпекою повинна оцінити ризик методом дерева рішень. Для відображення вимог використовується одна зі встановлених синтаксичних форм [22]:

[Умова] [Суб'єкт] [Дія] [Об'єкт] [Обмеження дії]
[Оцінка ризику більша за рівень прийнятності] [Система управління інформаційною безпекою] [Обробити] [Неприйнятний ризик] [Зменшення неприйнятного ризику]

або

[Суб'єкт] [Дія] [Обмеження дії]

[Система управління інформаційною безпекою] [Оцінити ризик] [Дерево рішень]

При визначенні вимог до систем управління інформаційною безпекою перевіряється відповідність їх формулювань насамперед як обов'язкових тверджень з використанням слова "повинна". Це дозволяє виокремити серед потреб і очікувань описовий текст, що використовується для їх пояснення і може помилково тлумачитися як вимога. Тоді як аспект їх необов'язковості враховується уживанням слова "доцільно". Крім цього звертається увага на позитивну ("повинна") або негативну ("не повинна") тональність формулювань вимог. Зокрема, необхідно уникати використання таких тверджень: система управління інформаційною безпекою не повинна обробляти прийнятні ризики.

Після того як проаналізовано правильність формулювання вимог до систем управління інформаційною безпекою необхідно перевірити наявність у них індивідуальних і групових характеристик. Індивідуальні характеристики насамперед властиві окремо взятій вимозі, а саме [1], [13], [22]:

Необхідність. Вимогою відображається важлива потреба, очікування або обмеження зацікавлених сторін. Її відсутність серед набору вимог призведе до складнощів реалізування інших. Наприклад, система управління інформаційною безпекою повинна ідентифікувати ризик. Ця індивідуальна вимога характеризується необхідністю, оскільки залишення її поза увагою призведе до ускладнення визначення оцінок величин вірогідності та наслідків реалізації загроз інформаційній безпеці.

Коректність. Вимогою відображається точність описання реалізованості потреби, очікування або обмеження зацікавлених сторін на певному рівні абстрагування. Наприклад, на рівні підсистем, – підсистема аналізування ризику інформаційної безпеки повинна визначати оцінки величин вірогідності та наслідків реалізації загроз. Це сприяє уникненню обмежень на розроблення архітектури системи управління інформаційною безпекою і, як наслідок, незалежність від конкретної реалізації.

Однозначність. Вимогою відображається одноманітність (простота, легкість) реалізування потреб, очікувань або обмежень зацікавлених сторін. Наприклад, система управління інформаційною безпекою повинна визначати оцінки ризику методом матриця "Наслідки-Вірогідність" за трьохзначною шкалою: "Низька", "Середня", "Висока". Це дозволяє уникати розбіжностей думок при розробленні систем управління інформаційною безпекою.

Повнота. Вимогою відображається уся необхідна інформація про потреби, очікування або обмеження зацікавлених сторін. Це вказує на відсутність необхідності в додатковому їх поясненні. Наприклад, система управління інформаційною безпекою повинна обробляти ризики з оцінками наслідків "Середні", "Високі" та вірогідності "Висока" за варіантом зменшення.

Здійсненність. Вимогою відображається реалізованість потреб та очікувань зацікавлених сторін з урахуванням обмежень на людські, фінансові ресурси. Наприклад, при обиранні методів оцінювання ризику необхідно серед них віддавати перевагу простим. Це дозволить уникнути залучення експертів і, як наслідок, фінансових витрат. Тому з урахуванням простоти використання вимога визначається: система управління інформаційною безпекою повинна оцінювати ризик методом матриця "Наслідки-Вірогідність".

Верифікованість. Вимогою відображається потреба, очікування або обмеження зацікавлених сторін з можливістю перевірки їх реалізування. Наприклад, система

ISSN 2663 - 4023

управління інформаційною безпекою повинна визначати оцінки ризику методом за умови відтворюваності його результатів. Це означає, що оцінки ризику можуть знаходитися одним і тим самим методом, але різними фахівцями. Задоволеність даної умови сприяє порівнюваності отриманих значень і, як наслідок, зменшенню впливу фактору суб'єктивності.

Пріоритетність. Для кожної з вимог необхідно встановити пріоритет їхнього реалізування. При цьому враховується важливість потреб, очікувань і обмежень зацікавлених сторін. До того ж можливий більш раціональний розподіл наявних ресурсів між важливими та неважливими вимогами. Пріоритет встановлюється або за значенням оцінок ризиків, або порядковою шкалою "Низький", "Середній", "Високий".

Індивідуальність. Вимогою визначається єдині потреба, очікування або обмеження зацікавлених сторін. Наприклад, система управління інформаційною безпекою повинна атестувати (зіставляти) ризик. Тоді як вимога оцінювання його величини є прикладом групи вимог – ідентифікування, визначення оцінок і атестування (зіставлення).

Вимога визначається як стереотип класу у графічній нотації SysML. Це дозволяє їх специфікувати поєднанням з відношеннями (див., наприклад, рис. 2) [23], [24]. Таке представлення розширюється завдяки використанню атрибутів. Ними описуються особливості представлення вимог та характерні для них обмеження. При їхньому аналізуванні розглядаються описові атрибути класу. Атрибутом позначається окрема характеристика, яка є спільною для об'єктів даного класу. На їхній основі та зважаючи на індивідуальні характеристики аналізуються вимоги до систем управління інформаційною безпекою. Серед описових атрибутів найбільш важливими є [22]:

Ідентифікатор. Вказує на однозначність ідентифікування вимог за визначеним номером. Наявністю унікальних ідентифікаторів забезпечується відстежуваність вимог.

Номер версії. Вказує на версію вимог. Це дозволяє при аналізуванні переконатися у правильності їхнього використання. Водночас виявити проблеми та ризики реалізування потреб, очікувань і обмежень зацікавлених сторін.

Розпорядник. Особа чи елемент організації, який підтримує реалізування вимог до систем управління інформаційною безпекою. Крім цього може їх змінювати, затверджувати зміни та повідомляти про стан вимоги.

Пріоритет зацікавлених сторін. Вказує на черговість реалізування кожної з вимог. Визначається через домовленості між зацікавленими сторонами за шкалою, наприклад, від 1 до 5 або "Низький", "Середній", "Високий".

Ризик. Визначається на основі факторів ризику з огляду на невідповідність характеристикам формулювань вимог. Насамперед неточність, неоднозначність.

Обґрунтування. Вказує на необхідність встановлення вимоги з огляду на потреби, очікування і обмеження зацікавлених сторін. Цим атрибутом визначається причина їхньої реалізованості.

Складність. Вказує на орієнтовну затратність реалізування кожної з вимог, наприклад: проста, середня, висока. Забезпечується додаткова інформація стосовно доступності вимог.

Тип. Виокремлює вимоги за орієнтованістю, типом властивостей, які ними відображаються. Водночас дозволяє їх класифікувати та аналізувати за групами.

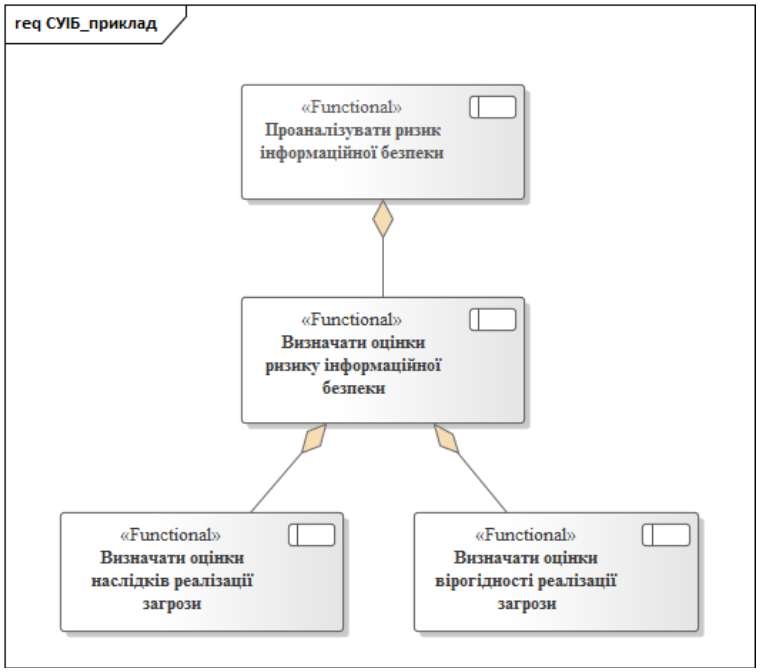

Рис. 2. Приклад специфікування вимог до систем управління інформаційної безпекою в організаціях з відношенням агрегування між ними

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отже, розроблення методу аналізування вимог до систем управління інформаційною безпекою дозволить визначити їх індивідуальні, групові характеристики, систематизувати, встановлювати відношення між ними. Завдяки цьому можливе перетворення потреб, очікувань і обмежень зацікавлених сторін у системне рішення. Це досягається специфікуванням вимог до систем управління інформаційною безпекою відповідною діаграмою у графічній нотації SysML. На цій діаграмі можливе їхнє представлення як стосовно встановлених характеристик, так і можливе уточнення шляхом визначенням атрибутів вимог. Серед них виокремлюються, наприклад, ідентифікатор, пріоритет, ризик, складність, тип. Тож таким представленням можливе сприяння наданню впевненості зацікавленим сторонам належного управління ризиками з прийнятним рівнем.

У перспективах подальших досліджень планується на основі запропонованого методу аналізування вимог розробити логічну структуру систем управління інформаційною безпекою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] International Organization for Standardization. (2013, Sept. 25). *ISO/IEC 27001:2013, Information technology. Security techniques. Information security management systems. Requirements*. [Online]. Available: https://www.iso.org/ standard/54534.html. Accessed on: May 14, 2020.

[2] ДП “УкрНДНЦ”. (2015, Dec. 18). *ДСТУ ISO/IEC 27001:2015, Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor. 1:2014, IDT)*. Київ, 2016, 22 с.

[3] International Organization for Standardization. (2013, Sept. 25). *ISO/IEC 27002:2013, Information technology. Security techniques. Code of practice for information security controls*. [Online]. Available: https://www.iso.org/standard/54534.html. Accessed on: May 14, 2020.

[4] International Organization for Standardization. (2019, Mar. 08). *ISO/IEC/IEEE 15026-1:2019, Systems and software engineering. Systems and software assurance. Part1: Concepts and vocabulary*. [Online]. Available: https://www.iso.org/standard/73567.html. Accessed on: May 14, 2020.

[5] International Organization for Standardization. (2017, Apr. 12). *ISO/IEC 27003:2017, Information technology. Security techniques. Information security management systems. Guidance*. [Online]. Available: https://www.iso.org/ru/standard/63417.html. Accessed on: May 14, 2020.

[6] Верховна рада України. VIII скликання, 7 сесія. (2017, Жовт. 05). *Закон № 2163-VIII, Про основні засади забезпечення кібербезпеки України*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/2163-19#n89. Дата звернення: Трав. 14, 2020.

[7] Кабінет Міністрів України. (2019, Черв. 19). *Постанова № 518, Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури.* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/518-2019-%D0% BF#Text. Дата звернення: Трав. 14, 2020.

[8] Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг. (2019, Жовт. 07). *Постанова № 2094, Про прийняття попереднього рішення про сертифікацію оператора системи передачі електричної енергії*. [Електронний ресурс]. Доступно: https://www.nerc.gov.ua/index.php?id=44925. Дата звернення: Трав. 14, 2020.

[9] Верховна рада України. II скликання, 1 сесія. (1994, Лип. 05; зі змінами). *Закон № 80/94-ВР, Про захист інформації в інформаційно-телекомунікаційних системах*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/80/94-%D0% B2% D1% 80#Text. Дата звернення: Трав. 14, 2020.

[10] Кабінет Міністрів України. (2018, Листоп. 07). *Постанова № 992, Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/992-2018-%D0%BF#Text. Дата звернення: Трав. 14, 2020.

[11] Національний банк України. (2017, Верес. 28). *Постанова № 95, Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України.* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/ laws/show/v0095500-17#Text. Дата звернення: Трав. 14, 2020.

[12] В. В. Цуркан, "Специфікація вимог до систем управління інформаційною безпекою", на *XI всеукраїнській науково-практичній конференції Актуальні проблеми управління інформаційною безпекою держави*, Київ, 2020, с. 221.

[13] K. Wiegers, and J. Beatty, *Software Requirements (Developer Best Practices)*. Redmond, Washington, USA: Microsoft Press, 2013.

[14] С. Б. Гордиенко, В. В. Алейников, А. В. Литвинов, и О. В. Рзаев, "Актуальные вопросы построения и сертификации системы управления информационной безопасностью компании". *Сучасний захист інформації*, № 1, с. 10-15, 2014.

[15] A. I. H. Suhaimi, D. Bao, Y. Goto, and J. Cheng, "Development of ISMEE: An Information Security Management Engineering Environment", in *Computer Science and its Applications. Lecture Notes in Electrical Engineering*, vol. 330, J. Park, I. Stojmenovic, H. Jeong, and G. Yi, Eds. Berlin, Germany: Springer, 2015, pp. 1325-1330, doi: 10.1007/ 978-3-662-45402-2_184.

[16] Y. You, I. Cho, and K. Lee, "An advanced approach to security measurement system". *The Journal of Supercomputing*, vol. 72, iss. 9, pp. 3443-3454, 2016, doi: 10.1007/s11227-015-1585-7.

[17] В. О. Сиротюк, "Модели, методы и средства разработки и внедрения эффективной системы управления информационной безопасностью патентного ведомства", *Науковедение*, т. 9, № 6, 2017. [Электронный ресурс]. Доступно: https://naukovedenie.ru/ PDF/06TVN617.pdf. Дата обращения: Май 14, 2020.

[18] D. Proença, and J. Borbinha, "Information Security Management Systems - A Maturity Model Based on ISO/IEC 27001", in: *Business Information Systems. BIS 2018. Lecture Notes in Business Information Processing*, vol 320, W. Abramowicz, and A. Paschke, Eds. Berlin, Germany: Springer, Cham, 2018, pp. 102-114, doi: 10.1007/978-3-319-93931-5_8.

[19] V. Diamantopoulou, A. Tsohou, and M. Karyda, "General Data Protection Regulation and ISO/IEC 27001:2013: Synergies of Activities Towards Organisations' Compliance", *in Trust, Privacy and Security in Digital Business. Lecture Notes in Computer Science*, vol. 11711, S. Gritzalis, E. Weippl, S. Katsikas, G. Anderst-Kotsis, A. Tjoa, and I. Khalil, Eds. Berlin, Germany: Springer, Cham, 2019, pp. 94-109, doi: 10.1007/978-3-030-27813-7_7.

[20] В. В. Селифанов, и Р. В. Мещеряков, “Методика формирования допустимых вариантов организационного состава и структуры автоматизированной системы управления информационной безопасностью”, *Моделирование, оптимизация информационные технологии*, т. 8, вып. 1, с. 1-13, 2020, doi: 10.26102/2310-6018/2020.28.1.001.

[21] International Organization for Standardization. (2018, Dec. 12). *ISO/IEC/IEEE* 24748-2*:2018, Systems and software engineering. Life cycle management. Part 2: Guidelines for the application of ISO/IEC/IEEE 15288 (System life cycle processes).* [Online]. Available: https://www.iso.org/standard/70816.html. Accessed on: May 14, 2020.

[22] International Organization for Standardization. (2018, Nov. 28). *ISO/IEC/IEEE 29148:2018, Systems and software engineering. Life cycle processes. Requirements engineering.* [Online]. Available: https://www.iso.org/standard/70816.html. Accessed on: May 14, 2020.

[23] SysML Open Source Project. [Online]. Available: https://sysml.org/. Accessed on: May 14, 2020.

[24] Model based systems engineering with Sparx Systems Enterprise Architect. [Online]. Available: https://sparxsystems.com/resources/user-guides/. Accessed on: May 14, 2020.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (9), 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

REQUIREMENTS ANALYSIS METHOD OF INFORMATION SECURITY MANAGEMENT SYSTEMS

Abstract. The process of analyzing the requirements for information security management systems is considered. The obligation to comply with the requirements of the international standard ISO/IEC 27001 is shown. This provides confidence to stakeholders in the proper management of information security risks with an acceptable level. This is due to the internal and external circumstances of influencing the goal and achieving the expected results of organizations. In addition, the identification of stakeholders, their needs and expectations from the development of information security management systems are also considered. It is established that now the main focus is on taking into account the requirements for the process of developing these systems or to ensure information security in organizations. The transformation of the needs, expectations and related constraints of stakeholders into an appropriate systemic solution has been overlooked. These limitations have been overcome through the method of analyzing the requirements for information security management systems. Its use allows, based on the needs, expectations and related constraints of stakeholders, to identify relevant statements in established syntactic forms. There is need to check each of them for correctness of formulation and compliance with the characteristics of both the individual requirement and the set of requirements. For their systematization, establishment of relations the graphic notation SysML is applied. In view of this, the requirement is considered as a stereotype of a class with properties and constraints. Relationships are used to establish relationships between requirements. Their combination is represented by a diagram in the graphical notation SysML and, as a result, allows you to specify the requirements for information security management systems. In the prospects of further research, it is planned to develop its logical structure on the basis of the proposed method.

Keywords: information security management system, requirement, characteristics of requirement, requirements analysis, requirement diagram, SysML.

REFERENCES

[1] International Organization for Standardization. (2013, Sept. 25). *ISO/IEC 27001:2013, Information technology. Security techniques. Information security management systems. Requirements*. [Online]. Available: https://www.iso.org/ standard/54534.html. Accessed on: May 14, 2020.

[2] DP "UkrNDNTs". (2015, Dec. 18). *DSTU ISO/IEC 27001:2015, Information technology. Security techniques. Information security management systems. Requirements*. Kyiv, 2016, 22 p.

[3] International Organization for Standardization. (2013, Sept. 25). *ISO/IEC 27002:2013, Information technology. Security techniques. Code of practice for information security controls*. [Online]. Available: https://www.iso.org/standard/54534.html. Accessed on: May 14, 2020.

[4] International Organization for Standardization. (2019, Mar. 08). *ISO/IEC/IEEE 15026-1:2019, Systems and software engineering. Systems and software assurance. Part1: Concepts and vocabulary*. [Online]. Available: https://www.iso.org/standard/73567.html. Accessed on: May 14, 2020.

[5] International Organization for Standardization. (2017, Apr. 12). *ISO/IEC 27003:2017, Information technology. Security techniques. Information security management systems. Guidance*. [Online]. Available: https://www.iso.org/ru/standard/63417.html. Accessed on: May 14, 2020.

[6] Verkhovna Rada Ukrainy. VIII convocation, 7th session. (2017, Oct. 05). *Law № 2163-VIII, On the Basic Principles of Cyber Security of Ukraine.* [Online]. Available: https://zakon.rada.gov.ua/laws/show/2163-19#n89. Accessed on: May. 14, 2020.

[7] Cabinet of Ministers of Ukraine. (2019, June 19). *Resolution № 518, On approval of the General requirements for cyber protection of critical infrastructure.* [Online]. Available: https://zakon.rada.gov.ua/laws/show/518-2019-%D0% BF#Text. Accessed on: May. 14, 2020.

[8] National energy and utilities regulatory commission of Ukraine. (2019, Oct. 07). *Resolution № 2094, On the adoption of the previous decision on the certification of the transmission system operator of electricity.* [Online]. Available: https://www.nerc.gov.ua/ index.php?id=44925. Accessed on: May. 14, 2020.

[9] Verkhovna Rada Ukrainy. II convocation, 1st session. (1994, July 05; with changes). *Law № 80/94-BP, On information protection in information and telecommunication systems.* [Online]. Available: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2% D1%80#Text. Accessed on: May. 14, 2020.

[10. Cabinet of Ministers of Ukraine. (2018, Nov. 07). *Resolution № 992, On approval requirements in the field of electronic trust services and confirm the compliance of trust in electronic services.* [Online]. Available: https://zakon.rada.gov.ua/laws/show/992-2018-%D0%BF#Text. Accessed on: May. 14, 2020.

[11] National Bank of Ukraine. (2017, Sept. 28). *Resolution № 95, On approval of the Regulations on the organization of measures to ensure information security in the banking system of Ukraine*. [Online]. Available: https://zakon.rada.gov.ua/ laws/show/v0095500-17#Text. Accessed on: May. 14, 2020.

[12] V. V. Tsurkan, "Specification of requirements for information security management systems", in *Proc. Ukrainian scientific-practical conference Actual problems of information security management of the state*, Kyiv, 2020, p. 221.

[13] K. Wiegers, and J. Beatty, *Software Requirements (Developer Best Practices)*. Redmond, Washington, USA: Microsoft Press, 2013.

[14] S. B. Gordienko, V. V. Aleinikov, A.V. Litvinov, and O.V. Rzayev, "Current issues of construction and certification of the company's information security management system". *Modern Information Security*, no. 1, pp. 10-15, 2014.

[15] A. I. H. Suhaimi, D. Bao, Y. Goto, and J. Cheng, "Development of ISMEE: An Information Security Management Engineering Environment", in *Computer Science and its Applications. Lecture Notes in Electrical Engineering*, vol. 330, J. Park, I. Stojmenovic, H. Jeong, and G. Yi, Eds. Berlin, Germany: Springer, 2015, pp. 1325-1330, doi: 10.1007/ 978-3-662-45402-2_184.

[16] Y. You, I. Cho, and K. Lee, "An advanced approach to security measurement system". *The Journal of Supercomputing*, vol. 72, iss. 9, pp. 3443-3454, 2016, doi: 10.1007/s11227-015-1585-7.

[17] V. O. Sirotyuk, "Models, methods and tools for developing and implementing an effective information security management system of the patent office", *Naukovedenie*, vol. 9, no. 6, 2017. [Online]. Available: https://naukovedenie.ru/PDF/ 06TVN617.pdf. Accessed on: May. 14, 2020.

[18] D. Proença, and J. Borbinha, "Information Security Management Systems - A Maturity Model Based on ISO/IEC 27001", in: *Business Information Systems. BIS 2018. Lecture Notes in Business Information Processing*, vol 320, W. Abramowicz, and A. Paschke, Eds. Berlin, Germany: Springer, Cham, 2018, pp. 102-114, doi: 10.1007/978-3-319-93931-5_8.

[19] V. Diamantopoulou, A. Tsohou, and M. Karyda, "General Data Protection Regulation and ISO/IEC 27001:2013: Synergies of Activities Towards Organisations' Compliance", *in Trust, Privacy and Security in Digital Business. Lecture Notes in Computer Science*, vol. 11711, S. Gritzalis, E. Weippl, S. Katsikas, G. Anderst-Kotsis, A. Tjoa, and I. Khalil, Eds. Berlin, Germany: Springer, Cham, 2019, pp. 94-109, doi: 10.1007/978-3-030-27813-7_7.

[20] V. V. Selifanov, and R. V. Meshcheryako, "Methods of acceptable options formation of organizational structure and the structure of the automated information security management system", *Modeling, optimization and information technology*, vol. 8, iss. 1, pp. 1-13, 2020, doi: 10.26102/2310-6018/2020.28.1.001.

[21] International Organization for Standardization. (2018, Dec. 12). *ISO/IEC/IEEE* 24748-2*:2018, Systems and software engineering. Life cycle management. Part 2: Guidelines for the application of ISO/IEC/IEEE 15288 (System life cycle processes).* [Online]. Available: https://www.iso.org/standard/70816.html. Accessed on: May 14, 2020.

[22] International Organization for Standardization. (2018, Nov. 28). *ISO/IEC/IEEE 29148:2018, Systems and software engineering. Life cycle processes. Requirements engineering.* [Online]. Available: https://www.iso.org/standard/70816.html. Accessed on: May 14, 2020.

[23] SysML Open Source Project. [Online]. Available: https://sysml.org/. Accessed on: May 14, 2020.

[24] Model based systems engineering with Sparx Systems Enterprise Architect. [Online]. Available: https://sparxsystems.com/resources/user-guides/. Accessed on: May 14, 2020.