DOI 10.15276/imms.v9.no4.209
УДК 004[056.53+413.4]

Informatics and Mathematical Methods in Simulation
Vol. 9 (2019), No. 4, pp. 209-221

СТРУКТУРИ АРХІТЕКТУРИ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

В.В. Мохор[1], В.В. Цуркан[2], Я.Ю. Дорогий[2], Ю.М. Штифурак[2]

[1]Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, вул. Генерала Наумова, 15, м. Київ, 03164, Україна; e-mail: v.mokhor@gmail.com
[2]Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», просп. Перемоги, 37, м. Київ, 03056, Україна; e-mail: v.v.tsurkan@gmail.com, argusyk@gmail.com, yura.shtyfurak@gmail.com

Розглянуто поняття структури архітектури систем управління інформаційною безпекою. Акцентовано увагу на тому, що це один з найбільш розповсюджених механізмів процесу їх архітектуризування. Показано його застосовність для розроблення, тлумачення, аналізування і використання описання архітектури систем управління інформаційною безпекою. Зважаючи на це, проаналізовано окремі різновиди структур. Зокрема, огляд і порівняльний аналіз методологій розроблення архітектур організацій; рамкові архітектури побудови інформаційних систем НАТО; аспекти використання структур при розробленні критичної ІТ інфраструктури; підходи до описання архітектури систем і окремих компонентів. Завдяки цьому встановлено можливість застосування структур стосовно розроблення архітектури систем управління інформаційною безпекою. Її представлено набором елементів і співвідношень між ними. Нею визначено одна або декілька зацікавлених сторін і їхня цікавість системою управління інформаційною безпекою. Цікавості структуровано однією або декількома точками зору на архітектуру. Кожною з них узагальнено структуру архітектури та, як наслідок, встановлено спосіб бачення означеної системи з урахуванням правил співвідношення. Показано можливість відображення архітектури систем управління інформаційною безпекою однією з таких типових різновидів структур: Захмана, Міністерства оборони Сполучених штатів Америки, Міністерства оборони Великобританії, відкритої групи, Крухтена «4+1», еталонної моделі для відкритого розподіленого оброблення, узагальненої еталонної архітектури організації. Проаналізовано особливості застосування типових структур стосовно розроблення архітектури систем управління інформаційною безпекою. Виокремлено аспекти, які доцільно при цьому врахувати. З огляду на них, зауважено їх орієнтованість на організації або системи, зокрема, програмні. Цим пояснено те, що здебільшого для розроблення архітектури використовується мова моделювання UML. Водночас показано перспективність застосування типових структур з огляду на встановлені особливості для розроблення архітектури систем управління інформаційною безпекою.

Ключові слова: система управління інформаційною безпекою, архітектура, описання архітектури, структура архітектури, концептуальна модель.

Вступ

Під структурою архітектури систем управління інформаційною безпекою розуміються домовленості, принципи та практики її описання у межах заданої області та/або об’єднання зацікавлених сторін. Це один з найбільш розповсюджених механізмів процесу архітектуризування систем. Завдяки його використанню розробляється, тлумачиться, аналізується і застосовується описання архітектури систем управління інформаційною безпекою з огляду на інтереси зацікавлених сторін. До того ж через структуру розкриваються умови описання та додаткові практики процесу архітектуризування систем [1, 2].

Аналіз останніх досліджень і публікацій

Останні дослідження і публікації орієнтовані на розглядання застосовності як окремих різновидів, так і структур архітектури систем та/або організацій загалом, наприклад, див. [1-6]. Зокрема, огляд і порівняльний аналіз методологій розроблення архітектури організацій виконано в [3]. Рамкові архітектури побудови інформаційних систем НАТО проаналізовано в [4]. Окрему увагу приділено їх використанню при розробленні критичної IT інфраструктури [5]. Крім цього, розглянуто підходи до описання архітектури як систем, так і окремих компонентів, зокрема [6].

Однак, розроблення систем управління інформаційною безпекою на основі структур архітектури залишилося поза увагою. Водночас можливість їх застосування стосовно таких систем розглянуто в [1, 2].

Мета роботи

Метою роботи є встановлення особливостей використання структур архітектури стосовно систем управління інформаційної безпекою.

Для досягнення сформованої мети розв'язано такі завдання:

- проаналізовано останні дослідження і публікації стосовно використання структур архітектури як до систем, так і, як наслідок, організацій;
- охарактеризовано концептуальну модель структури архітектури систем управління інформаційною безпекою;
- виокремлено та проаналізовано типові різновиди структур архітектури стосовно особливостей застосування до систем управління інформаційною безпекою.

Основна частина

Структура архітектури систем управління інформаційною безпекою представляється набором елементів і співвідношень між ними (див., наприклад [1], рис. 1). Так, нею визначаються принаймні одна або декілька зацікавлених сторін (зокрема [7], персонал, вище керівництво організації; підрядники) та їхня цікавість означеною системою в організації. Кожна з зацікавлених сторін може мати одну або декілька цікавостей. До того одна цікавість може бути притаманна декільком зацікавленим сторонам. Це відображається як користь або проблема, наприклад, від належного/неналежного управління ризиками інформаційної безпеки. Тоді як власне забезпечення збереженості конфіденційності, цілісності та доступності інформації завдяки оцінюванню ризиків є основною метою розробляння і впроваджування систем управління інформаційною безпекою в організації. У даному випадку організація є зовнішнім середовищем, яке, з одного боку, впливає, а, з іншого, взаємодіє з означеною системою [1, 2, 7].

Водночас одна або декілька цікавостей структуруються однією або декількома точками зору на архітектуру. Кожна з них є узагальненням структури архітектури, що встановлює спосіб бачення систем управління інформаційною безпекою. Точкою зору визначаються як зацікавлені сторони, так їхні цікавості. Крім цього здійснюється її узагальнення одним або декількома видами моделей [1, 2]. Їх різновидами, наприклад [8], при використані мови моделювання систем (Systems Modeling Language, SysML) є діаграми вимог, структури та поведінки.

Окрім точки зору, структура архітектури систем управління інформаційною безпекою узагальнюється правилами співвідношення [1]. Таке узагальнення обумовлено необхідністю їх встановлення між елементами концептуальної моделі (рис. 1).

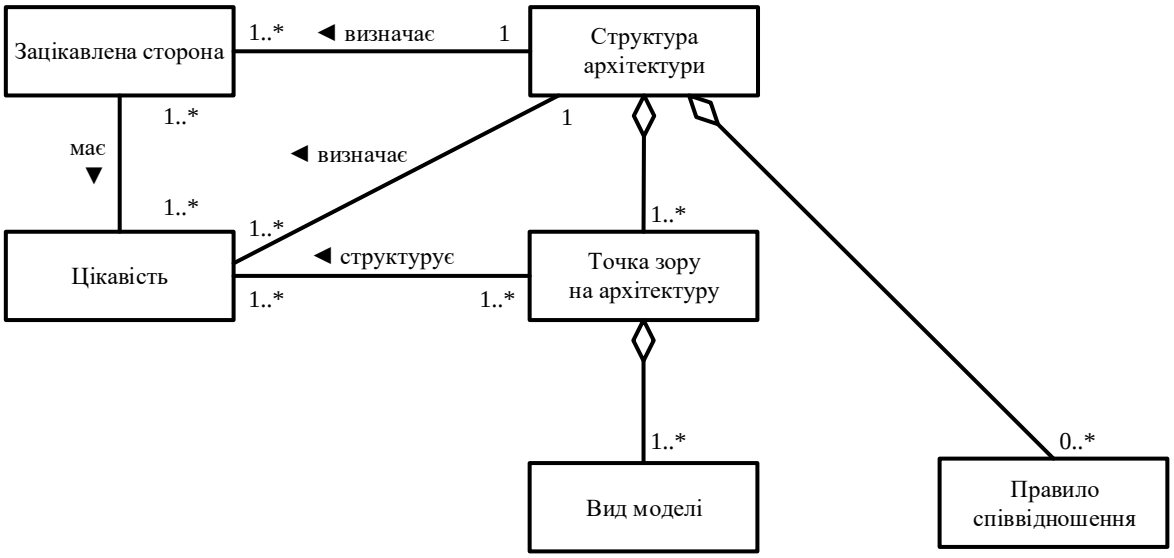

Рис. 1. Концептуальна модель структури архітектури систем управління інформаційною безпекою [1]

Як наслідок, архітектура систем управління інформаційною безпекою може відображатися одним з таких типових різновидів структур [1, 5]: Захмана, Міністерства оборони Сполучених штатів Америки, Міністерства оборони Великобританії, відкритої групи, Крухтена «4+1», еталонна модель для відкритого розподіленого оброблення, узагальнена еталонна архітектура організації.

Структура архітектури організації Захмана (The Zachman Enterprise Architecture Framework, ZEAF) є фундаментальною структурою, що відображається набором описових уявлень про системи управління інформаційною безпекою. Вона представляється таблицею 6×6 з виокремленими комунікаційними запитаннями як стовпцями та реіфікаційними перетвореннями як рядками (наприклад [9, 10], рис. 2). На перетині рядків і стовпців отримуються артефакти структури архітектури. Це обумовлено тим, що розташування кожного конкретного артефакту повинно бути визначеним і, як наслідок, відображення структури архітектури вважається завершеним лише за умови заповненості всіх комірок таблиці. Комірка вважається повною якщо вона містить артефакти, якими задаються системи управління інформаційною безпекою для конкретної ролі та з урахуванням конкретного аспекту. Завдяки цьому можливе адекватне описання даних систем з огляду на точку зору кожної зацікавленої сторони [5, 9, 10].

Описання структури архітектури систем управління інформаційною безпекою за Захманом здійснюється шляхом заповнення таблиці зверху вниз. Для цього використовується шість питальних слів: що, як, де, хто, коли та чому. Так, на першому рівні планується діяльність організації загалом, зокрема, визначаються її потреби та мета діяльності, внутрішні та зовнішні обставини стосовно їх впливання на системи управління інформаційною безпекою. Як зацікавлена сторона розглядається вище керівництво. Тоді як на другому рівні визначаються організаційні процеси (основні, додаткові), розмір і структура організації. Завдяки цьому отримується концептуальна модель систем управління інформаційною безпекою, що визначає притаманні їй функції. На даному рівні зацікавленою стороною є менеджер. Третій рівень орієнтований на розроблення логічної моделі з позицій архітектора. Характерною особливістю є описання процесів у термінах систем управління інформаційною безпекою. Її фізична модель отримується на четвертому рівні з огляду на точку зору проектувальника. При цьому враховуються обрані засоби та/або заходи забезпечення інформаційної безпеки. П’ятий рівень відповідає детальному реалізуванню систем управління інформаційною безпекою та зацікавленостей нею з боку розробника. Точка

зору користувача враховується на шостому рівні при описанні поведінки систем управління інформаційною безпекою [5, 9, 11].

Рис. 2. Структура архітектури Захмана [9, 10]

Структура архітектури відкритої групи (Open Group Architecture Framework, ToGAF) є методологією і структурою архітектури організації (наприклад [12], рис. 3). Включає набір стандартів, методів, зв'язків між фахівцями. Завдяки цьому можливе послідовне відображення потреб зацікавлених сторін, використання кращих практик та приділяння належної уваги як поточним вимогам, так і очікуваним потребам діяльності організації. Це досягається ітеративністю моделі процесів розроблення архітектури систем управління інформаційною безпекою з урахуванням наявних архітектурних ресурсів [12].

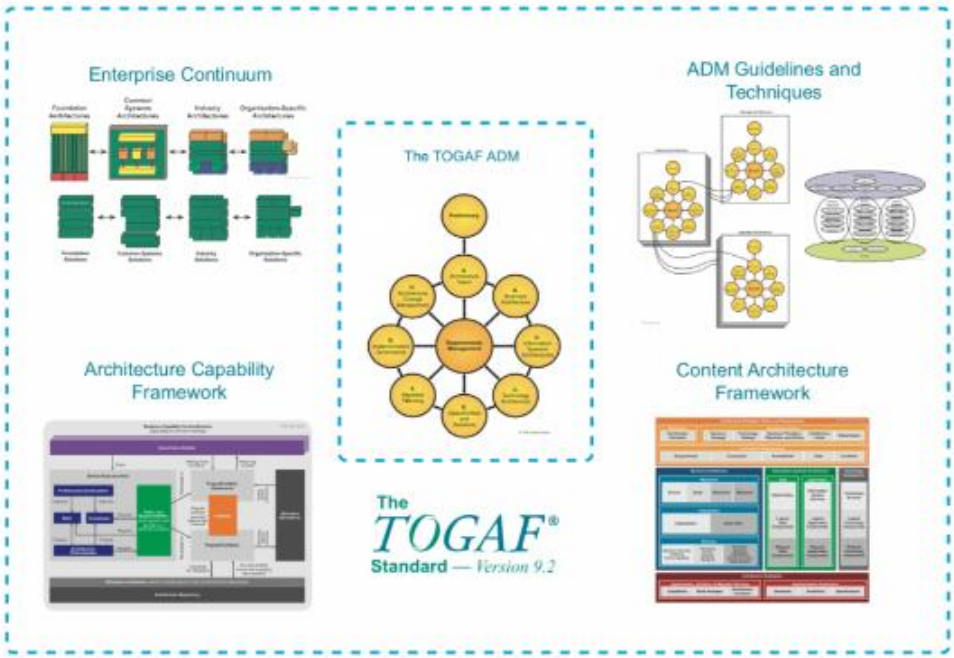

Рис. 3. Структура архітектури відкритої групи [12]

Найбільш важливим елементом у межах підходу ToGAF є метод розроблення архітектури (Architecture Development Method, ADM). За основу його використання взято покрокове розроблення архітектури систем управління інформаційною безпекою. Результат застосування ADM включає створення архітектурної бази, розроблення контенту, а також перехід та керування реалізацією архітектури. Такі заходи є основною ітеративного циклу її розроблення. Завдяки цьому можливе врахування мети діяльності та потреб зацікавлених сторін при розробленні архітектури систем управління інформаційною безпекою. Ітераційність ADM досягається виокремленням восьми фаз його застосовності. Так, на попередній фазі описуються першочергові дії налаштування структури ToGAF для розроблення архітектури систем управління інформаційною безпекою. Далі здійснюється послідовне проходження від встановлення області розроблення (фаза A) до керування її змінами (фаза H). Водночас можливе повернення від однієї фази до іншої для уточнення і деталізування розроблення архітектури [5, 12].

Структура архітектури Міністерства оборони Сполучених штатів Америки (Department of Defense Architecture Framework, DoDAF) є структурою та концептуальною моделлю, що сприяє прийняттю рішень зацікавленими сторонами (наприклад [13], рис. 4). Це досягається завдяки організованому обміну інформацією в організації. Як наслідок, використання DoDAF для розроблення архітектури систем управління інформаційною безпекою зосереджується на архітектурних даних, а не артефактах. При цьому на власників процесів організації (наприклад, вище керівництво, менеджери) покладається встановлення вимог та контролювання розвитку архітектури в межах їх повноважень і діяльності. Ними обирається архітектор та команда її розроблення з огляду на встановлені вимоги до архітектури систем управління інформаційною безпекою. Таким підходом забезпечується повторне використання інформації та обмін артефактами, моделями та точками зору на неї для спільного розуміння зацікавленими сторонами [5, 13].

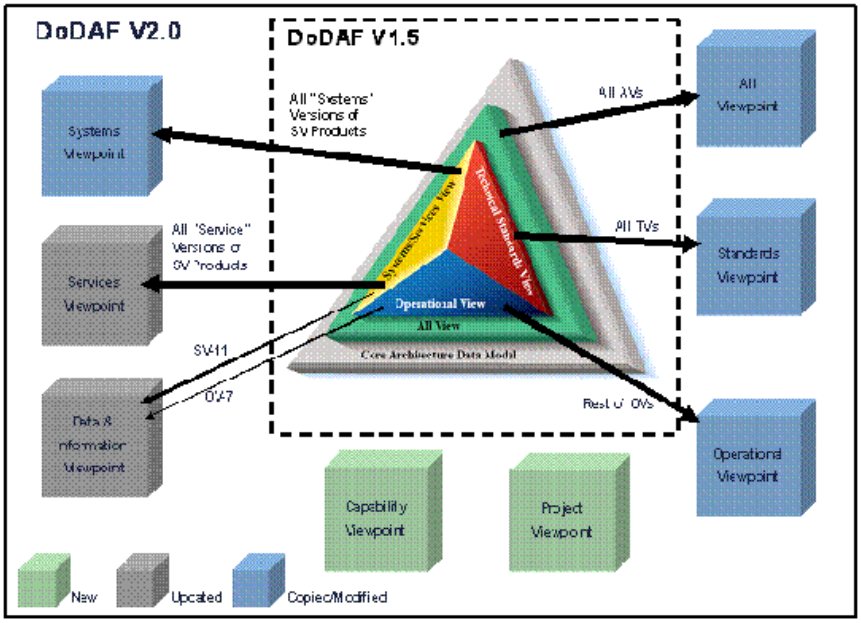

Рис. 4. Структура архітектури Міністерства оборони Сполучених штатів Америки [13]

За підходом DoDAF розроблення архітектури систем управління інформаційною безпекою зводиться до шести кроків [13]. На першому з них визначається її призначення та цільове використання. Насамперед, як описуватиметься архітектура, методи її розроблення, категорії архітектурних даних, потенційний вплив і процес оцінювання зусиль з огляду на задоволеність зацікавлених сторін. Область

застосування архітектури систем управління інформаційною безпекою встановлюється упродовж другого кроку. Завдяки цьому задається глибина та широта її описання, завдання, сутність і рівень деталізації. Третій крок орієнтований на визначення даних, що потрібні для підтримання розроблення архітектури систем управління інформаційною безпекою. Рівень деталізації даних і їх атрибутів встановлюється за результатами аналізування процесів в організації. Зважаючи на це, архітекторами накопичуються, упорядковуються і зберігаються дані в межах четвертого кроку. Для цього використовуються відповідні представлення, наприклад [13], діяльності, процесів і моделей даних. Аналізування архітектурних даних на п'ятому кроці дозволяє визначити та оцінити рівень дотримання вимог власниками процесів. Як наслідок, можливе або встановлення додаткових вимог, або уточнення поточних, зокрема, з третього по п'ятий кроки. На шостому кроці архітектурні дані представляються у зручному для прийняття рішень виді. Цьому сприяють результати, що отримуються за результатами третього та четвертого кроків.

Структура архітектури міністерства оборони Великобританії (British Ministry of Defence Architecture Framework, MoDAF) є набором правил і шаблонів описання, аналізування та ефективного керування оборонними організаціями зі структурою за підходом DoDAF (див., наприклад [5, 14], рис. 5). Цей набір правил і шаблонів тлумачиться як «представлення». Їх використання дозволяє графічно та текстово візуалізувати архітектуру систем управління інформаційною безпекою в організації. При цьому виокремлюється сім таких представлень, кожне з яких відображає окремий аспект зацікавлених сторін, а саме [5]: мету діяльності та ресурси для її досягнення (стратегічне); діяльність, функції ведення господарської та операційної діяльності (операційне); послуги підтримання завдань і дій операційного представлення (сервісно-орієнтоване); наслідки реалізування операційних та сервісно-орієнтованих представлень (системне); стандарти, правила, політики та настанови застосування до аспектів архітектури (технічне); потреби реалізування (придбання).

При використанні MoDAF для описання архітектури систем управління інформаційною безпекою в організації використовуються концептуальні моделі. З огляду на це складні проблеми діяльності поділяються на компоненти. Кожен з таких компонентів описується на найвищому рівні в мета-моделі MoDAF через подання інформації за допомогою різних точок зору. Хоча мета-модель є узагальненою моделлю будь-якої організації, кожен з компонентів доцільно створювати за конкретними стандартами для конкретної організації. При цьому забезпечується узгодженість і взаємозв'язок між представленням і даними. Такий підхід дозволяє забезпечити узгоджене використання різних середовищ моделювання архітектури [5, 14].

Рис. 5. Структура архітектури Міністерства оборони Великобританії [14]

Структура архітектури Крухтена «4+1» («4+1» View Model of Architecture Philippe Kruchten) орієнтована на використання п’яти представлень (наприклад [15], рис. 6). Зокрема, логічного, процесів, розроблення, фізичного, сценаріїв. Логічне представлення відображає об’єктну модель систем управління інформаційною безпекою. При цьому можливе виокремлення її як статичної (наприклад, діаграма класів), так і динамічної (наприклад, діаграма діяльності) логічної структур. Їх використання орієнтоване на представлення функціональних вимог до систем управління інформаційною безпекою. Тоді як нефункціональні вимоги враховуються за допомогою представлення процесів. Серед них виокремлюються, наприклад, доступність, продуктивність, стійкість до відмов. За даним представленням, процеси відображаються на декількох рівнях абстрагування. Так, на верхньому рівні процеси представляються набором незалежних логічних мереж програм з урахування застосовності фізичних (апаратних ресурсів). Тому рівень представлення процесів загалом орієнтований на «тактичне» керування завданнями. Це дозволяє виокремлювати серед них основні та додаткові і, як наслідок, розподіляти ресурси для їх виконання. Середовище розроблення систем, зокрема, управління інформаційною безпекою, розглядається на відповідному рівні представлення – розроблення. Передусім приділяється увага створенню і поєднанню підсистем в єдине ціле з урахуванням співвідношень між ними. Кожна з таких підсистем може розроблятися одним або декількома розробниками. В даному випадку повнота систем управління інформаційною безпекою залежить від описання усіх її елементів. До того ж, на даному рівні представлення враховуються внутрішні вимоги стосовно використання, наприклад, мов програмування, середовищ розроблення. Фізичним представленням систем управління інформаційною безпекою враховується, насамперед, реалізування нефункціональні вимог. Серед них виокремлюються доступність, надійність (відмовостійкість), продуктивність, масштабованість. При цьому визначаються такі елементи як мережі, процеси, завдання і об’єкти. Кожен з них відображається різними вузлами. Це дозволяє використовувати різні фізичні конфігурації залежно від завдань. Наприклад, розроблення або тестування, впровадження з огляду на потреби зацікавлених сторін. Цим обумовлюється гнучкість фізичного представлення систем управління інформаційною безпекою на рівні вузлів. Неперервність зазначених представлень забезпечується на рівні сценаріїв. Вони розглядаються як абстрагування найбільш важливих вимог до систем управління інформаційною безпекою. Для їх представлення використовуються діаграми сценаріїв і взаємодії. Звідси й назва структури архітектури Крухтена – «4+1» [15].

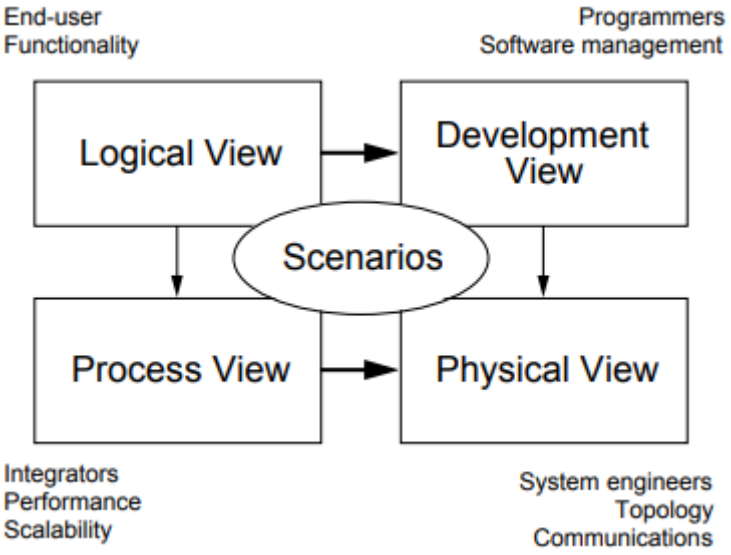

Рис. 6. Структура архітектури Крухтена «4+1» [15]

Еталонна модель для відкритого розподіленого оброблення (Reference Model of Open Distributed Processing, RM-ODP) (наприклад [16, 17]) орієнтується на створення архітектури систем управління інформаційною безпекою, якою підтримується розподіленість, міжсистемна взаємодія, сумісність і портативність [17]. Розробленню такого підходу передувала необхідність стандартизування моделі відкритого розподіленого оброблення як всередині організації, так і між ними. За основу такого оброблення взято узагальнену модель взаємодії відкритих систем.

Фундаментальними елементами структури RM-ODP є підхід до моделювання об'єктів для специфікування системи, специфікування системи з урахуванням точок зору, визначення інфраструктури системи, структури оцінювання відповідності систем [16]. Першим елементом забезпечується використання усталених практик об'єктно-орієнтованого підходу. Врахування потреб зацікавлених сторін стосовно специфікацій систем здійснюється другим елементом. Третій елемент втілює визначення функцій і структури систем відповідно до стандартів ODP. Тоді як четвертим елементом встановлюється одноманітність поведінки як підсистем, так і системи загалом [5, 16].

За структурою RM-ODP можливе використання п'яти точок зору для представлення різних аспектів систем управління інформаційною безпекою [5, 16, 17], а саме: організація, інформація, обчислювальна, інженерія, технологія. Точкою зору «Організація» визначаються вимоги високого рівня до систем, такі як мета, область впровадження, спільнота або користувачі, політика діяльності, керівні принципи, потоки та обмеження, виконані дії. Представлення семантики інформації, інформаційних структур, а також обмежень на тлумачення і використання інформації здійснюється у межах точки зору «Інформація». Обчислювальна точка зору орієнтована на функціональне декомпозиціювання систем об'єктами, що взаємодіють між собою через інтерфейси. Вони можуть бути як обчислювальними, так і об'єктами інфраструктури систем. Точкою зору «Інженерія» фокусуються на механізмах і функціях підтримання взаємодії між розподіленими об'єктами систем. Обирання технологій, продуктів, стандартів і технологічних об'єктів для підтримання реалізування систем здійснюється з огляду на точку зору «Технологія» [5, 16].

Модель відкритого розподіленого оброблення стандартизована міжнародними стандартами у чотирьох частинах [5]. Частиною 1 (ISO 10746-1 / ITU-T X.901) надається огляд і настанови використання еталонної моделі. Описання основ концепцій, визначення понять, правил та функцій моделювання систем ODP виконано в Частинах 2 та 3 (ISO 10746-2 / ITU-T X.902 та ISO 10746-3 / ITU-T X.903). Частиною 4 (ISO 10746-4 / ITU-T X.904) представляється описання архітектурної семантики, яка є технічною методикою опису для Частин 2 та 3. Основна мета використання цих стандартів полягає в наданні можливості реалізування переваг розподілу послуг оброблення інформації в гетерогенних середовищах за структурою RM-ODP.

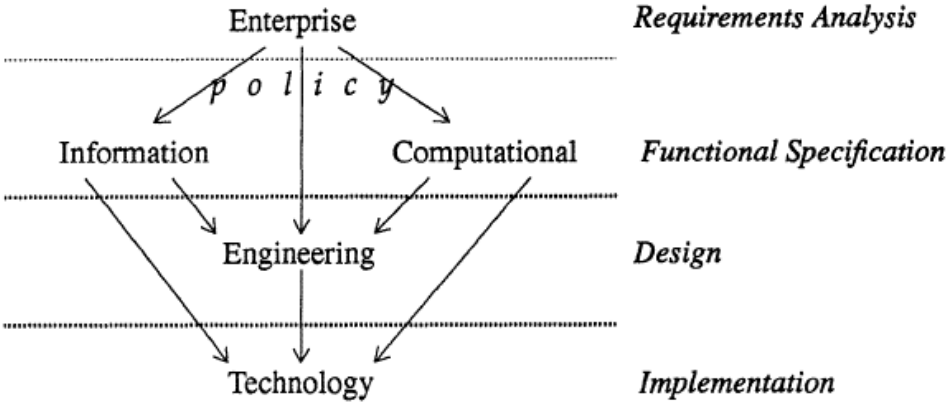

Рис. 7. Точки зору еталонної моделі відкритого розподіленого оброблення та інженерія програмного забезпечення [17]

Узагальнена еталонна архітектура та методологія організації (Generalised Enterprise Reference Architecture and Methodology, GERAM) орієнтована на врахування змін середовища діяльності організації при розробленні систем управління інформаційною безпекою. Представляється методами, моделями та інструментальними засобами розроблення і підтримання частини організації, організації загалом або мережі організацій (наприклад [18], рис. 8). Характерною особливістю даної структури є об'єднання підходів на основі моделей продуктів і врахування процесів. Крім цього важливим аспектом застосування є визначення циклів зворотного зв'язку на різних рівнях діяльності організації. Це розглядається як необхідна умова вдосконалення функціонування організації і, як наслідок, її адаптування до змінення технологій, суспільства, ринку [18].

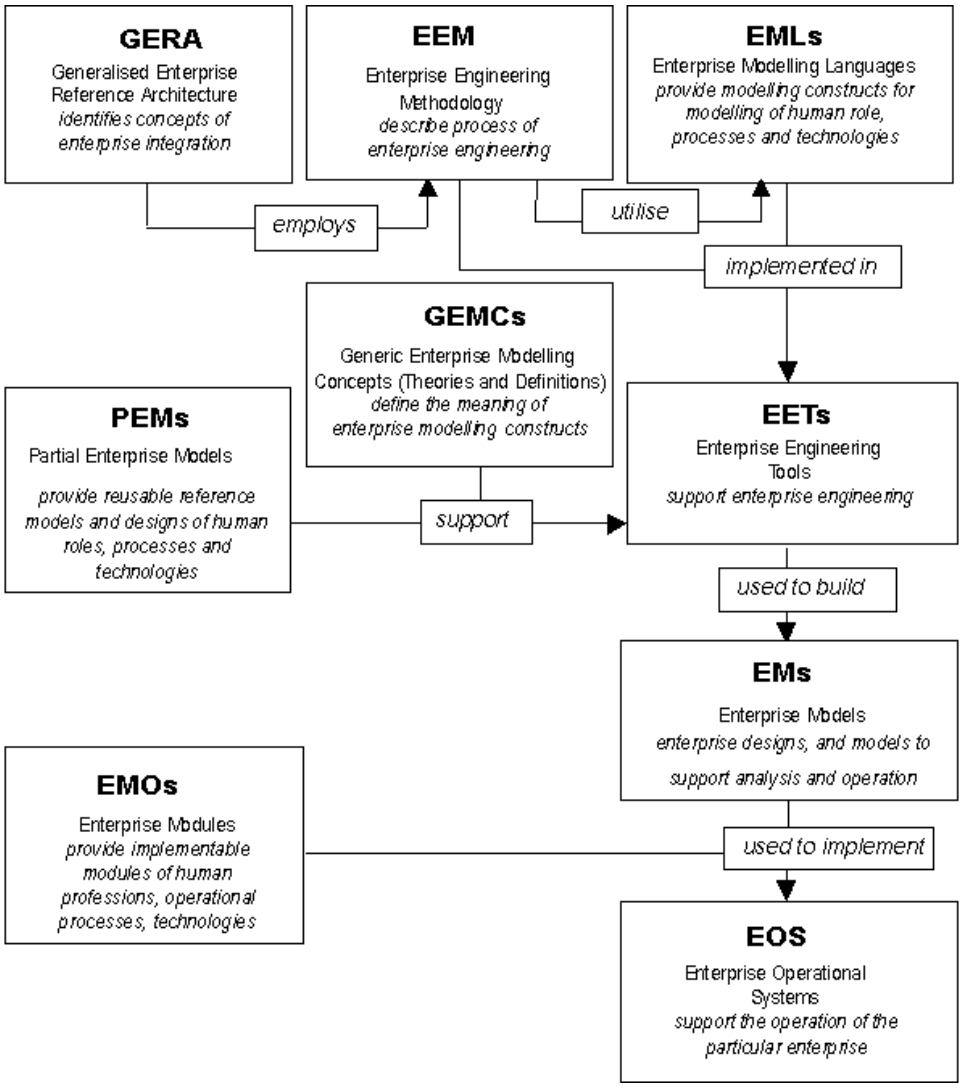

Рис. 8. Узагальнена еталонна архітектура організації і методології [18]

Одним із найбільш важливих елементів структури GERAM (рис. 8) є узагальнена стандартна архітектура організації (Generalised Enterprise Reference Architecture, GERA). Ним визначаються основні поняття стосовно розроблення і підтримання архітектури організації. Крім цього виокремлюються методологія інженерії організації (Enterprise Engineering Methodology, EEM) і мови моделювання організації (Enterprise Modelling Languages, EMLs). Вони використовуються для описування та моделювання структури, сутності та поведінки організацій. Водночас можливе представлення ролі людини в діяльності організації. До того ж процесів і технологій, що їх підтримують. Процес моделювання дозволяє побудувати моделі організації (Enterprise Models, EMs).

Ними представляються усі або частина операцій, завдання, її структура, інформаційні системи та системи управління. Такі моделі використовуються для впровадження операційної системи організації (Enterprise Operational Systems, EOS) і вдосконалювання здатності до оцінювання організаційних чи оперативних альтернатив. Тоді як застосовність методології інженерії і мов моделювання організації супроводжується інструментальними засобами (Enterprise Engineering Tools, EETs). Семантика мов моделювання визначається онтологіями, мета-моделями та словниками. Вони в сукупності називаються загальними концепціями моделювання організацій (Generic Enterprise Modelling Concepts, GEMC). При цьому процес моделювання вдосконалюється окремими моделями (Partial Enterprise Models, PEMs), якими відображаються ролі людей, процесів і технологій [18].

Розглянуті структури архітектур стосовно їх застосовності до систем управління інформаційною безпекою зведено в табл. 1 [1, 2, 5, 9-18]. З огляду на неї, доцільно зауважити їх орієнтованість на організації або системи, зокрема, програмні. Цим пояснюється те, що здебільшого для розроблення архітектури використовується універсальна мова моделювання (Unified Modeling Language, UML). Тоді як жодна з структур на практиці не застосовується для розроблення архітектури систем управління інформаційною безпекою.

Таблиця 1.

Порівняння структур архітектури для систем управління інформаційною безпекою

Різновид структури архітектури	Об’єкт застосовності структури архітектури	Мова моделювання	Застосовність до систем управління інформаційною безпекою
ZEAF	Система, організація	ArchiMate, UML	–
ToGAF	Система, організація	ArchiMate	–
DoDAF	Дані, система, організація	SysML, UML	–
MoDAF	Система, організація	SysML, UML	–
Крухтена «4+1»	Програмна система	UML	–
RM-ODP	Організація, система	UML	–
GERAM	Система, організація	EML	–

Висновки

Показано орієнтованість типових структур архітектури здебільшого на використання в організаціях та/або системах, зокрема, програмних. Як виняток, розглянуто приклади розроблення архітектури критичної IT інфраструктури. При цьому встановлено можливість використання типових структур стосовно систем управління інформаційною безпекою.

Охарактеризовано концептуальну модель структури архітектури систем управління інформаційною безпекою. Виокремлено її елементи (структура архітектури, точка зору на архітектуру, вид моделі, правило співвідношення, зацікавлені сторони,

цікавості) та співвідношення між ними. Акцентовано увагу на забезпеченні збереженості конфіденційності, цілісності та доступності інформації в організації завдяки оцінюванню ризиків як основній меті розроблення означених систем.

Проаналізовано особливості застосування типових структур стосовно розроблення архітектури систем управління інформаційною безпекою. Виокремлено аспекти, які доцільно при цьому врахувати. Водночас показано перспективність їх застосування з огляду на встановлені особливості для розроблення архітектури систем управління інформаційною безпекою.

Список літератури

1. ISO/IEC 42010:2011. Systems and software engineering. Architecture description. [First edition 2011-12-01]. Geneva, 2011. 46 p.
2. Мохор В.В., Цуркан В.В., Бакалинський О.О. Архітектура системи управління інформаційною безпекою. *Безпека інформації в інформаційно-телекомунікаційних системах : матеріали XX Ювілейної Міжнародної науково-практичної конференції* (м. Київ, 22-24 трав. 2018 р.). Київ, 2018. С. 38.
3. Штейнгарт Е.А., Бурмистров А.Н. Обзор и сравнительная характеристика методологий разработки архитектуры предприятия. *Научно-технические ведомости СПбГПУ. Экономические науки*. 2016. Т.245,№3. С. 111-129.
4. Кірпічіков Ю.А., Федорієнко В.А., Головченко О.В., Андрощук О.В. Аналіз рамкових архітектур побудови інформаційних систем НАТО та визначення особливостей архітектури C4ISR. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2017. Т.59,№ 1. С. 78-84.
5. Dorogyy Y., Tsurkan V., Telenyk S., Doroha-Ivaniuk O. A comparison enterprise architecture frameworks for critical IT infrastructure design. *Information Technology and Security*. 2017. Vol.5, Iss.2(9). Pp. 90-118.
6. Yamamoto S., Qiang Z., Morisaki S. A Composite Dependability for Enterprise Architecture. *Knowledge-Based and Intelligent Information & Engineering Systems*. 2018. Vol.126. Pp. 1130-1137.
7. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT). [На заміну ДСТУ ISO/IEC 27001:2010; чинний від 2015-12-18]. Вид. оф. Київ : ДП «УкрНДНЦ», 2015. 51 с.
8. SysML Open Source Project. URL: https://sysml.org/.
9. Zachman J.A. The Concise Definition of The Zachman Framework. URL: https://www.zachman.com/about-the-zachman-framework.
10. Zachman J.A. The Framework for Enterprise Architecture: Background, Description and Utility. URL:https://www.zachman.com/resources/ea-articles-reference/327-the-framework-for-enterprise-architecture-background-description-and-utility-by-john-a-zachman.
11. Карпенко С. Применение модели Захмана для проектирования ИТ-архитектуры предприятия. URL: http://www.management.com.ua/ims/ims177.html.
12. The TOGAF Standard, Version 9.2 Overview URL: https://www.opengroup.org/ togaf.
13. The DoDAF Architecture Framework Version 2.02. URL: https://dodcio.defense.gov/ Library/DoD-Architecture-Framework/.
14. MOD Architecture Framework. URL: https://www.gov.uk/guidance/mod-architecture- framework.
15. Kruchten, P. The «4+1» view model of software architecture. *IEEE Software*. 1995. Vol.12, Iss.6. Pp. 42-50.
16. The Reference Model of Open Distributed Processing (RM-ODP). URL: http://www.rm-odp.net/.
17. Raymond K., Armstrong L. Reference Model of Open Distributed Processing (RM-ODP): Introduction. *Open Distributed Processing*. 1994. Pp. 3-14.
18. GERAM: Generalised Enterprise Reference Architecture and Methodology. URL: http://www.ict.griffith.edu.au/~bernus/taskforce/geram/versions/geram1-6-3/ v1.6.3.html.

INFORMATION SECURITY MANAGEMENT SYSTEMS ARCHITECTURE FRAMEWORKS

V.V. Mokhor[1], V.V. Tsurkan[2], Y.Y. Dorohyi[2], Y.M. Shtyfurak[2]

[1]Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine,
15, General Naumov Str, Kyiv, 03164, Ukraine; e-mail: v.mokhor@gmail.com
[2]National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»,
37, Peremohy Ave., Kyiv, 03056, Ukraine; e-mail: v.v.tsurkan@gmail.com,
argusyk@gmail.com, yura.shtyfurak@gmail.com

The concept of information security management systems architecture framework is considered. Attention is drawn to the fact that this is one of the most common mechanisms of their architectural process. Its applicability for the development, interpretation, analysis and use of the information security management systems architecture description is shown. In view of this, some variants of frameworks have been analyzed. In particular, review and comparative analysis of methodologies for developing architectures of organizations; architecture frameworks for building NATO information systems; aspects of the use of frameworks in the development of critical IT infrastructure; approaches to describing the architecture of systems and individual components. Thanks to this, the possibility of applying frameworks to develop the information security management systems architecture has been established. It is represented by a set of elements and relations between them. It identifies one or more stakeholders and their interest in the information security management system. Interests are structured by one or more perspectives on architecture. Each of them summarizes the architecture framework and, as a consequence, establishes a way of seeing the specified system in accordance with the rules of ratio. The possibility of displaying the information security management systems architecture by one of the following types of frameworks is shown: Zahman, United States Department of Defense, Ministry of Defense of the United Kingdom, open group, Krukhten «4 + 1», reference model for open distributed processing, generalized reference architecture. The peculiarities of application of typical frameworks in the development of the information security management systems architecture are analyzed. Aspects that should be taken into account are distinguished. In view of them, their focus on organizations or systems, particularly software, is noted. This explains that mostly UML is used to design the architecture. At the same time the prospect of application of typical frameworks in view of the established features for the development of the information security management systems architecture is shown.

Keyword: information security management system, architecture, architecture description, architecture framework, conceptual mode.

СТРУКТУРЫ АРХИТЕКТУРЫ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.В. Мохор[1], В.В. Цуркан[2], Я.Ю. Дорогой[2], Ю.М. Штифурак[2]

[1]Институт проблем моделирования энергетики им. Г.Е. Пухова Национальной академии наук Украины,
ул. Генерала Наумова, 15, г. Киев, 03164, Украина; e-mail: v.mokhor@gmail.com
[2]Национальный технический университет Украины «Киевский политехнический институт имени Игоря Сикорского»,
проспект Победы, 37, г. Киев, 03056, Украина; e-mail: v.v.tsurkan@gmail.com, argusyk@gmail.com, yura.shtyfurak@gmail.com

Рассмотрены понятия структуры архитектуры систем управления информационной безопасности. Акцентировано внимание на том, что это один из наиболее распространенных механизмов процесса их архитектуризации. Показано его применимость для разработки, толкования, анализа и использования описания архитектуры систем управления информационной безопасностью. Учитывая это проанализированы отдельные разновидности структур. В частности, обзор и сравнительный анализ методологий разработки архитектур организаций; рамочные архитектуры построения информационных систем НАТО; аспекты использования структур при разработке критической ИТ инфраструктуры; подходы к описанию архитектуры систем и отдельных компонентов. Благодаря этому установлена возможность применения структур относительно разработки архитектуры систем управления информационной безопасностью. Ее представлено набором элементов и соотношений между ними. Ею определено одна или несколько заинтересованных сторон и их интерес системой управления информационной безопасностью. Интересы структурированы одной или несколькими точками зрения на архитектуру. Каждой из них обобщено структуру архитектуры и, как следствие, установлено способ виденья данной системы с учетом правил соотношений. Показана возможность отображения архитектуры систем управления информационной безопасностью одной из таких типовых разновидностей структур: Захмана, Министерства обороны Соединенных Штатов Америки, Министерства обороны Великобритании, открытой группы, Крухтена «4+1», эталонной модели для открытой распределенной обработки, обобщенной эталонной архитектуры организации. Проанализированы особенности применения типовых структур относительно разработки архитектуры систем управления информационной безопасностью. Выделены аспекты, которые целесообразно при этом учитывать. С учетом этого, отмечено их ориентированность на организации или системы, в частности, программные. Этим объясняется то, что в большинстве случаев для разработки архитектуры используется язык моделирования UML. В тоже время показано перспективность применения типовых структур учитывая установленные особенности разработки архитектуры систем управления информационной безопасностью.

Ключевые слова: система управления информационной безопасностью, архитектура, описания архитектуры, структура архитектуры, концептуальная модель.