INFORMATION SECURITY RISK MANAGEMENT

DOI 10.20535/2411-1031.2019.7.2.190569
УДК 004,056.53

ВОЛОДИМИР МОХОР,
ВАСИЛЬ ЦУРКАН

КОНЦЕПТУАЛЬНІ ОСНОВИ ОПИСАННЯ АРХІТЕКТУРИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Розглянуто проблематику розроблення системи управління інформаційною безпекою в організації. Представлено концептуальні основи описання її архітектури. Основні поняття стосовно архітектури системи управління інформаційною безпекою розкрито через її контекст. Контекст описання архітектури представляється основними елементами. До них належать: причетні сторони, мета, система управління інформаційною безпекою, навколишнє середовище, архітектура, описання архітектури. Причетні сторони зацікавлені в означеній системі. Така зацікавленість обумовлена потребою зберігання конфіденційності, цілісності та доступності інформаційних активів організації. Зважаючи на це формулюється мета розроблення означеної системи, що орієнтована на забезпечення інформаційної безпеки з прийнятним ризиком. Організація тлумачиться як навколишнє середовище функціонування системи управління інформаційною безпекою. Ним визначаються впливи на неї протягом її життєвого циклу з урахуванням взаємодії системи з навколишнім середовищем. Архітектурою відображається те, що є значним для системи управління інформаційною безпекою. Тоді як для вираження архітектури означеної системи використовується її описання. Описання архітектури системи управління інформаційної безпекою відображено архітектурним представленням. Ним представлено архітектуру з огляду на точку зору. Така точка зору характеризується двома аспектами: структурне представлення зацікавленостей причетних сторін; структурне представлення особливостей архітектури. Архітектурне представлення системи управління інформаційною безпекою відображається моделлю архітектури. Цією моделлю описуються особливості архітектури означеної системи з урахуванням зацікавленостей причетних сторін. Особливості архітектури відображаються видом моделі, через який здійснюється вплив на модель архітектури. Відношення між елементами описання архітектури показано зв’язками. Їх використання дозволяє представити відношення архітектури до зацікавленості в межах її описання. Таким чином, концептуальне описання архітектури системи управління інформаційною безпекою дозволить як розробити, так і обґрунтувати її розроблення з урахуванням зацікавленостей з боку організації і причетних сторін.

Ключові слова: система управління інформаційною безпекою; архітектура системи; описання архітектури системи; архітектурне представлення; модель архітектури; вид моделі.

Постановка проблеми. Архітектура системи управління інформаційною безпекою описується для вираження її основних понять і властивостей з огляду на навколишнє середовище (див., наприклад [1], рис. 1). Ці поняття та властивості втілюються у її елементах, відношеннях між ними, конкретних принципах розроблення. Тоді як під навколишнім середовищем розуміється організація незалежно від типу, розміру та природи. Організацією здійснюються впливи на систему управління інформаційною безпекою з урахуванням співвідношень між ними [1], [2]. Тому архітектурою представляється набір елементів, відношень між елементами, яким притаманні необхідні системні властивості. Вони тлумачаться як емерджентні властивості системи управління інформаційною безпекою, що повинні відповідати її характеристикам. До того ж описанням архітектури визначається,

по-перше, призначеність кожного елементу; по-друге, як вони співвідносяться між собою для досягнення очікуваного результату. Тоді як під очікуваним результатом розуміється забезпечення збереженості конфіденційності, цілісності та доступності інформації за результатами оцінювання ризиків [1], [3].

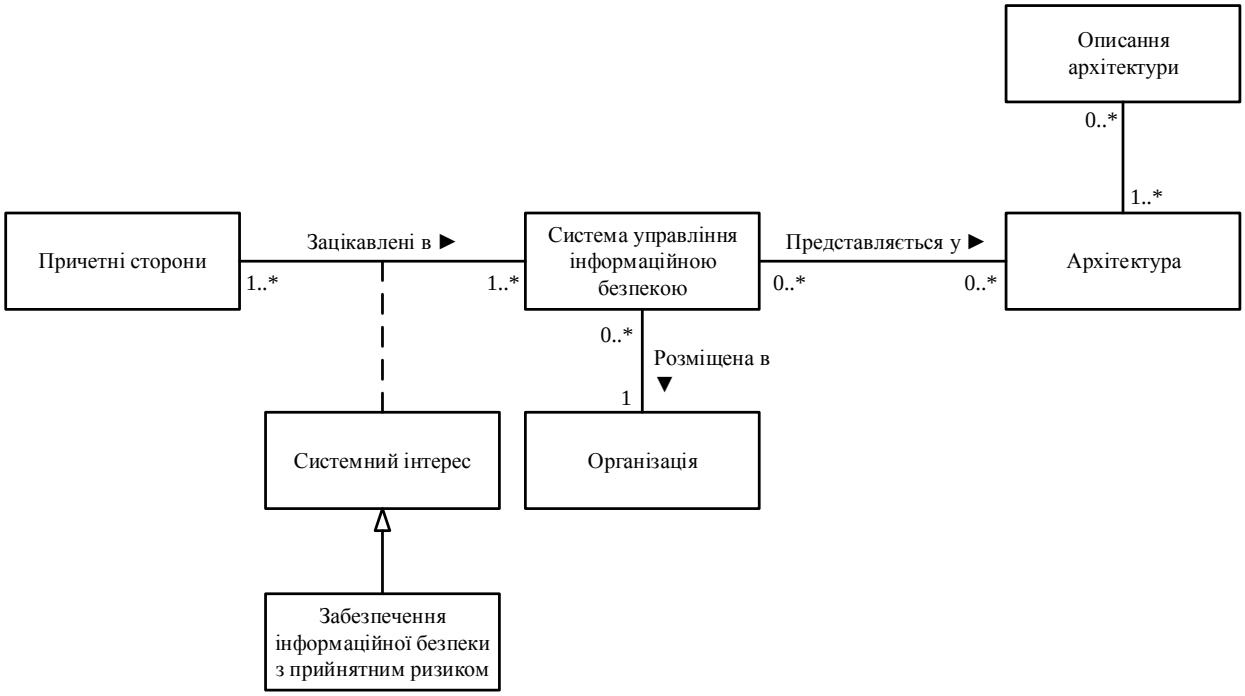

Рисунок 1 – Контекст описання архітекутри системи управління інформаційною безпекою

Аналіз останніх досліджень і публікацій. Забезпечення інформаційної безпеки регламентується положення міжнародних, національних і державних нормативних документів [2], [4] - [11]. Тоді як вимоги та настанови розроблення і впровадження системи управління інформаційною безпекою викладено в міжнародних стандартах серій 27k та 31k [2], [4] - [7]. Однак, використання означених настанов на практиці призводить до ускладнень через узагальненість їх формулювань. Насамперед [12], визначення структури, елементів, співвідношень між елементами системи управління інформаційною безпекою. При цьому її дослідження зводяться до розглядання здебільшого окремих аспектів, наприклад, [13] - [23]. Так, аналізування особливостей використання міжнародних стандартів серії ISO/IEC 27k розглянуто в [13]. Основні положення, принципи та методи побудови, етапи планування системи управління інформаційною безпекою розробляються у [14]. Формування проектних вимог до неї стосовно конкретної організації здійснюється завдяки встановленню можливості використання математичного апарату теорії систем масового обслуговування [15]. Проблематиці оцінювання ризику приділено увагу в [16] - [19]. Зокрема, оцінюванню і прогнозуванню рівня ризику в системах управління інформаційною безпекою [16]; концептуальним основам та методологічним підходам до ризик-орієнтованого, інтелектуального проактивного обирання засобів і заходів забезпечення конфіденційності, цілісності та доступності [17]; теоретико-методологічним, практичним та нормативно-правовим аспектам оцінювання ризиків інформаційної безпеки [18], дослідженню методів оброблення ризиків у системах управління інформаційною безпекою [19]. Крім цього виокремлюється проблематика проведення аудиту. Його теоретичні основи та програмні засоби викладено в [20]. Анкетування працівників організації при проведенні аудиту системи управління інформаційною безпекою досліджується у [21]. Нормативно-правовий аспект аудиту інформаційної безпеки на об’єктах критичної інфраструктури, в системах державних інформаційних ресурсів, та зокрема, стосовно й систем управління інформаційною безпекою

розкривається у [22]. Тоді як результати розроблення концептуальної моделі виведення і перетворення аудиторських доведень у висновки, настанови їх практичного використання наводяться у [23].

Отже, зосередженість на окремих важливих аспектах призводить до несистемності досліджень системи управління інформаційною безпекою і, як наслідок, проблематики, по-перше, виокремлення її елементів, співвідношень між ними; по-друге, визначення призначеності кожного елементу та як вони співвідносяться між собою для досягнення очікуваного результату. Тому встановлення концептуальних основ описання архітектури системи управління інформаційною безпекою є актуальним і практично направленим.

Метою даної роботи є встановлення концептуальних основ описання архітектури системи управління інформаційною безпекою.

Виклад основного матеріалу дослідження. Концептуальна модель описання архітектури системи управління інформаційною безпекою представлена на рис. 2. За основу її викладання стосовно означеної системи взято настанови, що визначаються в [1]. Моделлю відображаються основні поняття стосовно системи управління інформаційною безпекою і її архітектур. Такий підхід важливий для розуміння практики їх описання. Водночас це узгоджується і дозволяє тлумачити систему управління інформаційною безпекою як систему, що створена людиною. До того ж може складатися з апаратних і програмних засобів, даних, людей, процесів, процедур, обладнання. Тому концептуальна модель описання архітектури системи управління інформаційною безпекою відображається такими елементами (див. наприклад [1], рис. 2) [1]:

- *архітектура та описання архітектури*.

Основні поняття і властивості системи управління інформаційною безпекою в організації відображаються архітектурою, що виражається її описанням (див. рис. 2). При цьому не існує єдиної характеристики важливості елементів або співвідношень між ними. Вона може належати до [1]:

1) системних компонентів або елементів;
2) особливостей побудови елементів або співвідношень між ними;
3) принципів побудови системи управління інформаційною безпекою;
4) принципів керування розвитком системи управління інформаційною безпекою у процесі її життєвого циклу.

Водночас система управління інформаційною безпекою може відображатися декількома архітектурами (наприклад, для різних організацій). Тоді як одна архітектура може застосовуватися і характеризувати декілька систем [1].

- *зацікавлені сторони та інтереси*

Цей елемент відображає інтереси зацікавлених сторін стосовно системи управління інформаційною безпекою, що розробляється і впроваджується в організації. Насамперед, це забезпечення конфіденційності, цілісності та доступності інформації. У даному випадку збереженість даних властивостей розглядається як потреба зацікавленої сторони. Задоволенням такої потреби можуть цікавитися як одна, так і декілька зацікавлених сторін. Стосовно організації вони можуть бути внутрішніми та зовнішніми. Незважаючи на це кожна з них прагне впевнитися у тому, що ризики належно керуються [2]. Для розуміння їх потреб та очікувань в організації визначається важливість [2]:

1) зацікавлених сторін для системи управління інформаційною безпекою;
2) вимог визначених зацікавлених сторін до забезпечення інформаційної безпеки;

- *представлення архітектури та точки зору*

Описання архітектури може включати одне або декілька представлень. Представлення виражає архітектуру системи управління інформаційною безпекою з відповідною точкою зору. Вона характеризується двома аспектами [1]:

1) цікавості, що структурно представляються для зацікавлених сторін;
2) умовності, що встановлюються у представленнях архітектури.

При цьому будь-яка точка зору структурує одну або декілька цікавостей. Це означає, що цікавість може структуруватися декількома точками зору. Тому нею встановлюються умовності для розроблення і впровадження системи управління інформаційною безпекою. Умовності точки зору можуть включати мови, нотації, види моделей, правила розроблення, методи моделювання, методи аналізування у представленнях архітектури [1], [2].

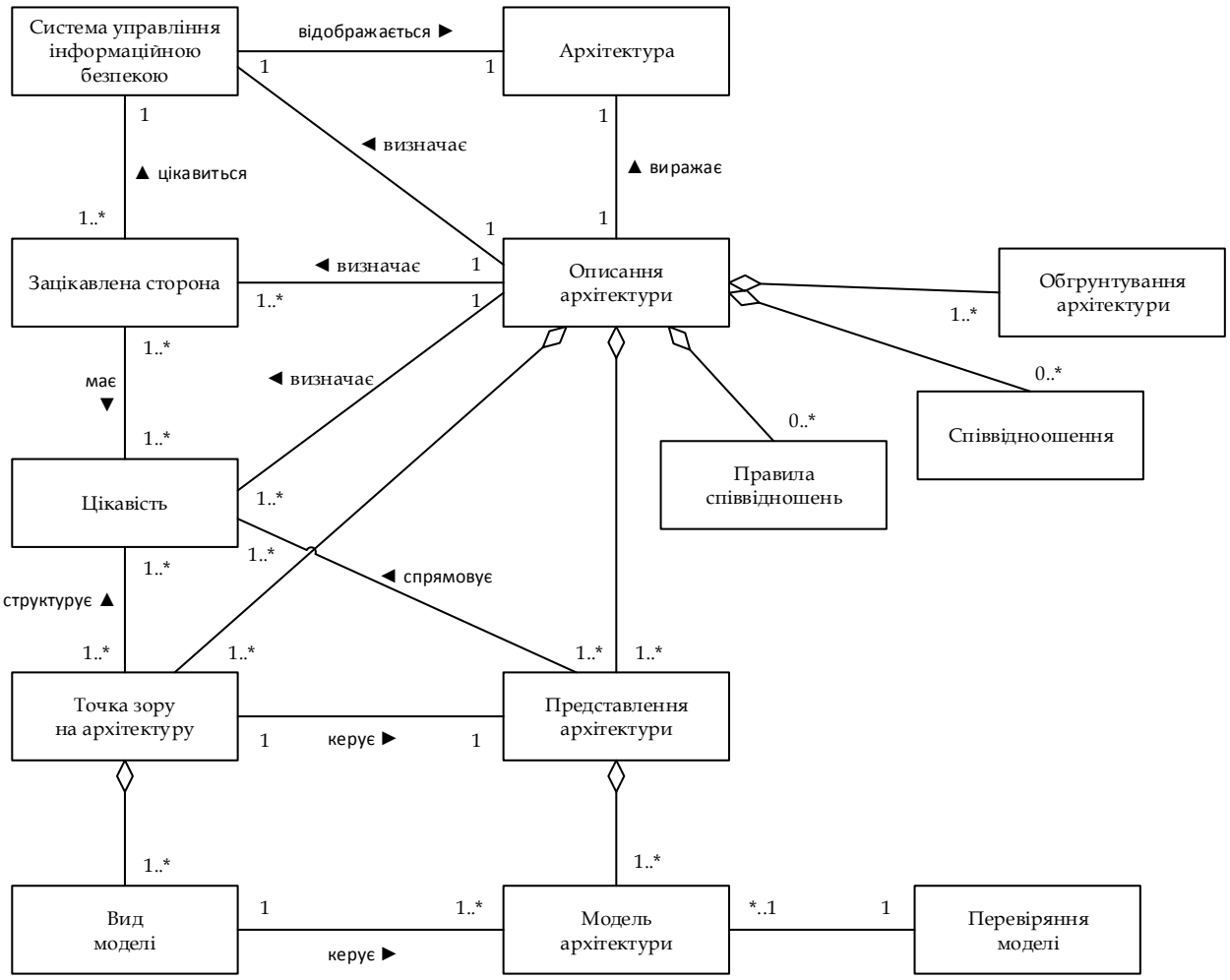

Рисунок 2 – Концептуальна модель описання архітектури системи управління інформаційною безпекою

– *моделі архітектури*

Одна або декілька моделей архітектури системи управління інформаційною безпекою утворюють її представлення [1], [2]. Модель архітектури орієнтована на задоволення потреб зацікавлених сторін. При цьому умовності моделювання відповідно до їх цікавостей визначаються видом моделі, що керує нею. Модель архітектури може бути частиною більш ніж одного представлення архітектури.

– *елементи та співвідношення*

Будь-яка конструкція в описанні архітектури є її елементом. Це найбільш прості елементи, що в сукупності описують основні поняття і властивості системи управління інформаційною безпекою в організації. До них належать [1]:

1) зацікавлені сторони;
2) цікавість;
3) точка зору;

4) представлення архітектури;
5) вид моделі;
6) модель архітектури;
7) обґрунтування архітектури;

Після того як визначено точки зору, види та наповнення моделей можливе розширення концептуальної моделі описання архітектури системи управління інформаційною безпекою додатковими елементами, наприклад, елементом перевіряння моделі (див. рис. 1). Водночас елементи описання архітектури пов'язані між собою співвідношеннями. Вони використовуються для вираження відношення архітектури до цікавостех у межах її описання. Наявні співвідношення керуються за встановленими правилами в межах або між описаннями архітектури;

- обґрунтування архітектури

Архітектура системи управління інформаційною безпекою обґрунтовується для пояснень, міркувань про причини прийняття рішень стосовно, наприклад, вибирання засобів та/або заходів оброблення ризиків у системі управління інформаційною безпекою. Таке обґрунтування може включати методологічні основи прийняття рішень, альтернативи, наслідки прийняття рішень, використання додаткових джерел. Рішення визначаються як системні цікавості. При цьому вони впливають на архітектуру, а саме [1]:

1) формулюванням вимог існування елементів описання архітектури;
2) зміненням властивостей елементів описання архітектури;
3) аналізування альтернатив стосовно окремих елементів описання архітектури;
4) встановлення нових цікавостей.

Структура архітектури систем управління інформаційною безпекою представляється набором елементів і співвідношень між ними (див., наприклад [1], рис. 3). Так, нею визначаються принаймні одна або декілька зацікавлених сторін (зокрема [7], персонал, вище керівництво організації; підрядники) та їхня цікавість означеною системою в організації. Кожна зі 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 (див., наприклад [1], [24], рис. 3).

Як наслідок, архітектура систем управління інформаційною безпекою може відображатися одним з таких типових різновидів структур [1], [24] : 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.

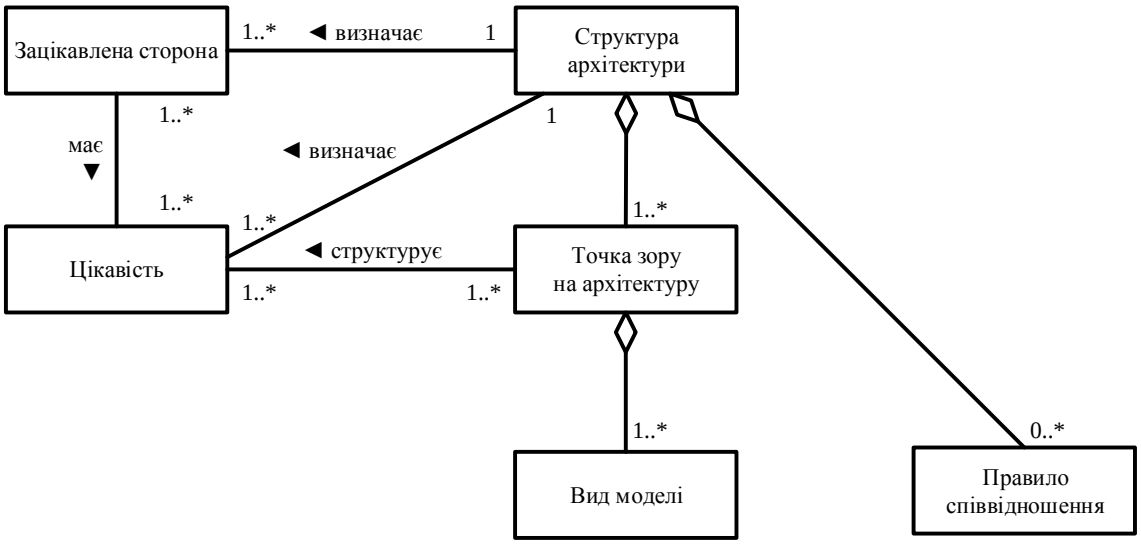

Рисунок 3 – Концептуальна модель структури архітектури систем управління інформаційною безпекою

Структура архітектури відкритої групи (Open Group Architecture Framework, ToGAF) є методологією і структурою архітектури організації. 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.

Структура архітектури Міністерства оборони Сполучених штатів Америки (Department of Defense Architecture Framework, DoDAF) є структурою та концептуальною моделлю, що сприяє прийняттю рішень зацікавленими сторонами. 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.

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. Цей набір правил і шаблонів тлумачиться як «представлення». Їх використання дозволяє графічно та текстово візуалізувати архітектуру систем управління інформаційною безпекою в організації.

Структура архітектури Крухтена «4+1» («4+1» View Model of Architecture Philippe Kruchten) орієнтована на використання п'яти представлень. 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.

Еталонна модель для відкритого розподіленого оброблення (Reference Model of Open Distributed Processing, RM-ODP) орієнтується на створення архітектури систем управління інформаційною безпекою, якою підтримується розподіленість, міжсистемна взаємодія, сумісність і портативність. 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.

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 та інструментальними засобами розроблення і підтримання частини організації, організації загалом або мережі організацій. Характерною особливістю даної структури є об'єднання підходів на основі моделей продуктів і врахування процесів.

Висновки. Отже, встановлено, що використання концептуальної основ дозволяє як виокремити елементи описання архітектури системи управління інформаційною безпекою в організації, визначити їх призначеність, так і встановити співвідношення між ними. Завдяки цьому можливе врахування потреб зацікавлених сторін, зокрема, і встановлених ними вимог до забезпечення конфіденційності, цілісності та доступності інформації. До того ж обґрунтування вибору архітектури системи управління інформаційною безпекою за її описанням в організації.

Показано орієнтованість типових структур архітектури здебільшого на використання в організаціях та/або системах, зокрема, програмних. Як виняток, розглянуто приклади розроблення архітектури критичної ІТ 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 ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] International Organization for Standardization. (2011, Febr. 1). *ISO/IEC 42010, Systems and software engineering. Architecture description*. Geneva, 2011, 46 p.

[2] ДП "УкрНДНЦ". (2015, Груд. 18). *ДСТУ ISO/IEC 27001, Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки. (ISO/IEC 27001:2013; Cor 1:2014, IDT)*. Київ, 2016, 22 с.

[3] Э. Халл, К. Джексон, и Дж. Дик. *Инженерия требований*. Москва: ДМК Пресс, 2017.

[4] ДП "УкрНДНЦ". (2015, Груд. 18). *ДСТУ ISO/IEC 27002, Інформаційні технології. Методи захисту. Звід правил (ISO/IEC 27002:2013; Cor 1:2014, IDT)*. Київ, 2016, 72 с.

[5] ДП "УкрНДНЦ". (2017, Січ. 1). *ДСТУ ISO/IEC 27005, Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT)*. Київ, 2016, 68 с.

[6] International Organization for Standardization. (2018, Febr. 15). *ISO 31000, Risk management. Guidelines*. Geneva, 2018, 16 p.

[7] МІНЕКОНОМРОЗВИТКУ УКРАЇНИ. (2014, Лип. 1). *ДСТУ IEC/ISO 31010, Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT)*. Київ, 2015, 80 с.

[8] National Institute of Standards and Technology. (2017, June 8). *SP 800-12 Rev. 1, An Introduction to Information Security*. [Online]. Available: https://csrc.nist.gov/ publications/ detail/sp/800-12/rev-1/final. Accessed on: June. 15, 2019.

[9] National Institute of Standards and Technology. (2006, March 9). *FIPS 200. Minimum Security Requirements for Federal Information and Information Systems*. [Online]. Available: https://csrc.nist.gov/publications/detail/fips/200/final. Accessed on: June 15, 2019.

[10] Bundesamt für Sicherheit in der Informationstechnik. *BSI-Standard 200-1:2017. Managementsysteme für Informationssicherheit*. [Online]. Verfügbar: https://www.bsi.bund.de/ SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_1.html. Zugriff am: Juni 15, 2019.

[11] Bundesamt für Sicherheit in der Informationstechnik. BSI-Standard 200-2:2017. IT-Grundschutz-Methodik. [Online]. Verfügbar: https://www.bsi.bund.de/ SharedDocs/Downloads/ DE/BSI/Grundschutz/Kompendium/standard_200_2.html. – Zugriff am: Juni 15, 2019.

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

[13] 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.

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

[15] В.В. Мохор, О.О. Бакалинський, О.М. Богданов, та В.В. Цуркан, "Дескриптивний аналіз аналогій між системами управління інформаційною безпекою та масового обслуговування", *Захист інформації*, том. 2, № 2, с. 119–126, 2017, doi: 10.18372/2410-7840.19.11435.

[16] Т.Ю. Зырянова, "Методы оценки и прогнозирования рисков в информационных системах", на *IX Международной научно-практической конференции Интеграция образовательной, научной и воспитательной деятельности в организациях общего и профессионального образования*. Екатеренбург, 2017, с. 58–68.

[17] А.А. Корниенко, и А.П. Глухов, "Модели и методы риск-ориентированного проактивного управления информационной безопасностью железнодорожной транспортной системы", *Бюллетень ОУС ОАО «РЖД»*. № 3, с. 42–54, 2018.

[18] Б.Б. Ахметов, А.Г. Корченко, А.Е. Архипов, и С.В. Казмирчук. *Построение систем анализа и оценивания рисков информационной безопасности. Теория и практические решения*. Актау, 2018.

[19] В.М. Горицький, та А.В. Мокій, "Дослідження методів обробки ризиків в системі управління інформаційною безпекою", на *Міжнародній науково-технічній конференції Перспективи телекомунікацій*. Київ, 2018, с. 1–3.

[20] А.Г. Серова, "Анализ теоретических основ и программных средств аудита системы управления информационной безопасностью", на *конференции Социально-экономические и естественно-научные парадигмы современности*. Ростов-на-Дону, 2018, с. 829–837.

[21] В.А. Бойправ, В.В. Ковалев, и Л.Л. Утин, "Программное средство для проведения аудита системы защиты информации организации", Доклады БГУИР, № 5 (115), с. 44–49, 2018.

[22] О.К. Юдін, Р.В. Зюбіна, та О.В. Матвійчук-Юдіна "Сучасні практики впровадження системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури", *Наукоємні технології*, №1 (41), с. 36–43, 2019, doi: 10.18372/2310-5461.41.13527.

[23] В.А. Воеводин "Концептуальная модель объекта аудита информационной безопасности" Comp. Nanotechnol, no. 3, pp. 92–95, 2019, doi: 10.33693/2313-223X-2019-6-3-92-95.

[24] Y. Dorogyy, V. Tsurkan, S. Telenyk, O. Doroha-Ivaniuk, "A comparison enterprise architecture frameworks for critical IT infrastructure design", *Information Technology and Security*, vol. 5, iss. 2 (9), pp. 90-118, 2017.

Стаття надійшла до редакції 02.09.2019.

REFERENCE

[1] International Organization for Standardization. (2011, Febr. 1). *ISO/IEC 42010, Systems and software engineering. Architecture description.* Geneva, 2011, 46 p.

[2] DP "UkrNDNTs". (2015, Dec. 18). *DSTU ISO/IEC 27001, Information technology. Security techniques. Information security management systems. Requirements. (ISO/IEC 27001:2013; Cor 1:2014, IDT)*. Kyiv, 2016, 22 p.

[3] E. Hall, K. Dzhekson, and Dzh. Dik, *Requirements engineering*. Moskow: DMK Press, 2017.

[4] DP "UkrNDNTs". (2015, Dec. 18). *DSTU ISO/IEC 27002, Information technology. Security techniques. Code of practice for information security controls. (ISO/IEC 27002:2013; Cor 1:2014, IDT).* Kyiv, 2016, 72 p.

[5] DP "UkrNDNTs". (2017, Jan. 1). DSTU ISO/IEC 27005, Information technology. Security techniques. Information security risk management. (ISO/IEC 27005:2011, IDT). Kyiv, 2016, 68 p.

[6] International Organization for Standardization. (2018, Febr. 15). *ISO 31000, Risk management. Guidelines.* Geneva, 2018, 16 p.

[7] Ministry for Development of Economy, Trade and Agriculture of Ukraine. (2014, July 1). *DSTU IEC/ISO 31010, Risk management. Risk assessment techniques. (IEC/ISO 31010:2009, IDT).* Kyiv, 2015, 80 p.

[8] National Institute of Standards and Technology. (2017, June 8). *SP 800-12 Rev. 1, An Introduction to Information Security.* [Online]. Available: https://csrc.nist.gov/ publications/ detail/sp/800-12/rev-1/final. Accessed on: June. 15, 2019.

[9] National Institute of Standards and Technology. (2006, March 9). *FIPS 200. Minimum Security Requirements for Federal Information and Information Systems.* [Online]. Available: https://csrc.nist.gov/publications/detail/fips/200/final. Accessed on: June 15, 2019.

[10] Bundesamt für Sicherheit in der Informationstechnik. *BSI-Standard 200-1:2017. Managementsysteme für Informationssicherheit.* [Online]. Verfügbar: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/ standard_200_1.html. Zugriff am: Juni 15, 2019.

[11] Bundesamt für Sicherheit in der Informationstechnik. *BSI-Standard 200-2:2017. IT-Grundschutz-Methodik.* [Online]. Verfügbar: https://www.bsi.bund.de/SharedDocs/ Downloads/ DE/BSI/Grundschutz/Kompendium/standard_200_2.html. – Zugriff am: Juni 15, 2019.

[12] 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.

[13] M. Komarov, S. Gonchar, 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.

[14] 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.

[15] V.V. Mokhor, O.O. Bakalynskyi, O.M. Bohdanov, and V.V. Tsurkan, "Descriptive analysis of analogies between information security management and queuing systems", *Zahist ìnformacìï*, vol. 2, no. 2, pp. 119–126, 2017, doi: 10.18372/2410-7840.19.11435.

[16] T.Y. Zyryanova, "Methods of risk assessment and forecasting in information systems", in *Proc. IX International scientific-practical conference Integration of educational, scientific and educational activities in organizations of general and vocational education*. Ekaterinburg, 2017, pp. 58–68.

[17] A.A. Kornienko, and A.P. Glukhov, "Models and methods of risk-oriented proactive management of information security of the railway transport system", *Bulletin of Joint Scientifi c Council of JSC Russian Railways*, no. 3, pp. 42–54, 2018.

[18] B.B. Akhmetov, O.H. Korchenko, O.Ye. Arkhipov, and S.V. Kazmirchuk. *Postroenie sistem analiza i otsenivaniya riskov informatsionnoy bezopasnosti. Teoriya i prakticheskie resheniya.* Aktau, 2018.
[19] V.M. Horytskyi, and A.V. Mokii, "Research methods of handling risks in information security management system", in *Proc. International Science and Technology Conference Telecommunication Perspectives*. Kyiv, 2018, pp. 1–3.
[20] A.G. Serova, "Analysis of the theoretical foundations and audit software tools for information security management system", in *Proc. conferences Socio-economic and natural-science paradigms of our time*. Rostov-on-Don, 2018, pp. 829–837.
[21] V.A. Boiprav, V.V. Kovalev, and L.L. Utin, "Software for audit of information protection system of the organization", *Doklady Belorusskogo gosudarstvennogo universiteta informatiki i radioèlektroniki*, no. 5 (115), pp. 44–49, 2018.
[22] O. Yudin, R. Ziubina, O. Matviichuk-Yudina, "The modern practices of implementation of the information security audit system on the critical infrastructure objects", *Science-Based Technologies*, no. 1 (41), pp. 36–43, 2019, doi: 10.18372/2310-5461.41.13527.
[23] V.A. Voevodin, "Conceptual model of information security auditobject", *Comp. Nanotechnol*, no., 3, pp. 92–95, 2019, doi: 10.33693/2313-223X-2019-6-3-92-95.
[24] Y. Dorogyy, V. Tsurkan, S. Telenyk, and O. Doroha-Ivaniuk, "A comparison enterprise architecture frameworks for critical IT infrastructure design", *Information Technology and Security*, vol. 5, iss. 2 (9), pp. 90-118, 2017.

VOLODYMYR MOKHOR,
VASYL TSURKAN

CONCEPTUAL BASIS OF DESCRIPTION FOR THE INFORMATION SECURITY MANAGEMENT SYSTEM ARCHITECTURE

The problems of information security management system development in the organization are considered. Conceptual bases of its architecture description are presented. Basic concepts regarding the information security management system architecture are disclosed through its context. The context of the architecture description is represented by the main elements. These include: parties involved, purpose, information security management system, environment, architecture, architecture descriptions. The parties involved are interested in the system. Such interest is driven by the need to maintain the confidentiality, integrity and accessibility of the organization's information assets. In view of this, the aim is to develop a defined system that is focused on providing information security with acceptable risk. The organization is interpreted as the environment of the functioning of the information security management system. It determines its effects during its life cycle, taking into account the interaction of the system with the environment. The architecture reflects what is significant to the information security management system. Whereas to describe the architecture of a designated system, its description is used. The information security management system architecture is described by an architectural view. It presents architecture from the point of view. This view is characterized by two aspects: a structural representation of the interests of the parties involved; structural representation of architecture features. The architectural representation of the information security management system is reflected by the architecture model. This model describes the features of the designated system architecture, taking into account the interests of the parties involved. Architecture features are reflected by the type of model through which the model is influenced. The relationships between the architectural description elements are shown in the links. Their use makes it possible to represent the attitude of architecture to the interest within its description. Thus, this conceptual description of the information security management system architecture will allow both to develop and justify its development taking into account the interests of the organization and the parties involved.

Keywords: information security management system; system architecture; system architecture description; architectural representation; architecture model; model kind.

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.

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.