© Mokhor V., Tsurkan V., Dorohyi Ya. Conceptual architecture description model of information security management system // Ukrainian Scientific Journal of Information Security, 2019, vol. 25, issue 3, pp. 162-166.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ / INFORMATION SECURITY MANAGEMENT

DOI: 10.18372/2225-5036.25.14461

КОНЦЕПТУАЛЬНА МОДЕЛЬ ОПИСАННЯ АРХІТЕКТУРИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Володимир Мохор[1], Василь Цуркан[2], Ярослав Дорогий[2]

[1]Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Україна
[2]НТУУ «Київський політехнічний інститут імені Ігоря Сікорського», Україна

МОХОР Володимир Володимирович, член-кореспондент НАН України, д.т.н., професор

Рік та місце народження: 1955 рік, м. Київ, Україна.
Освіта: Київський інститут інженерів цивільної авіації (з 2000 року – Національний авіаційний університет), 1977 рік.
Посада: директор.
Наукові інтереси: теорія ризиків, інформаційна безпека, кібербезпека, математичне і комп'ютерне моделювання.
Публікації: понад 250 наукових публікацій, серед яких монографії, навчальні посібники, наукові статті та патенти на винаходи.
E-mail: v.mokhor@gmail.com.
Orcid ID: 0000-0001-5419-9332.

ЦУРКАН Василь Васильович, к.т.н., доцент

Рік та місце народження: 1982 рік, м. Харків, Україна.
Освіта: Національний технічний університет України «Київський політехнічний інститут» (з 2016 - Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського)», 2005 рік.
Посада: доцент кафедри кібербезпеки і застосування інформаційних систем і технологій з 2016 року.
Наукові інтереси: системні дослідження системи управління інформаційною безпекою, теорія ризиків.
Публікації: понад 100 наукових публікацій, серед яких монографії, наукові статті.
E-mail: v.v.tsurkan@gmail.com.
Orcid ID: 0000-0003-1352-042X.

ДОРОГИЙ Ярослав Юрійович, к.т.н., доцент

Рік та місце народження: 1979 рік, м. Київ, Україна.
Освіта: Національний технічний університет України «Київський політехнічний інститут» (з 2016 - Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського), 2002 рік.
Посада: доцент кафедри автоматики і управління в технічних системах з 2016 року.
Наукові інтереси: інформаційні технології, штучний інтелект, критичні IT-інфраструктури.
Публікації: понад 150 наукових публікацій, серед яких монографії, навчальні посібники, наукові статті.
E-mail: argusyk@gmail.com.
Orcid ID: 0000-0003-3848-9852.

Анотація. *Розглянуто основні поняття і властивості архітектури системи управління інформаційною безпекою з огляду на вплив з боку організації. При цьому враховано здійснення впливів організацією на означену систему з урахуванням співвідношень між ними. Тому архітектуру представлено набором елементів, відношень між елементами, яким притаманні необхідні системні властивості. Крім цього акцентовано увагу на визначенні описанням архітектури призначеності кожного з елементів та співвідношень між ними для досягнення системою управління інформаційною безпекою очікуваного результату. Цей результат тлумачено як забезпечення збереженості конфіденційності, цілісності та доступності інформації за результатами оцінювання ризиків. За основу концептуальної моделі описання архітектури системи управління інформаційною безпекою взято настанови ISO/IEC 42010. Моделлю відображаються основні поняття стосовно означеної си-*

стеми та 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. Вона може складатися з апаратних і програмних засобів, даних, людей, процесів, процедур, обладнання. Тому концептуальну модель описання архітектури системи управління інформаційною безпекою відображено такими елементами як архітектура та описання архітектури; зацікавлені сторони та інтереси; представлення архітектури та точки зору; моделі архітектури; елементи та співвідношення; обґрунтування архітектури. Такий підхід дозволяє як виокремити елементи системи управління інформаційною безпекою, визначити їх призначеність, так і встановити співвідношення між ними.

Ключові слова: *інформаційна безпека, система управління інформаційною безпекою, архітектура, описання архітектури, представлення архітектури, модель архітектури, концептуальна модель.*

Вступ

Архітектура системи управління інформаційною безпекою описується для вираження її основних понять і властивостей з огляду на навколишнє середовище [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].

Аналіз існуючих досліджень

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 дослідження концептуальної моделі описання архітектури системи управління інформаційною безпекою є актуальним і практично направленим.

Метою даної роботи є визначення елементів, співвідношень між елементами описання архітектури системи управління інформаційною безпекою за його концептуальною моделлю.

Основна частина дослідження

Концептуальна модель описання архітектури системи управління інформаційною безпекою представлена на рис. 1. 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. рис. 1) [1]:

1. *Архітектура та описання архітектури*.

Основні поняття і властивості системи управління інформаційною безпекою в організації відображаються архітектурою, що виражається її описанням (див. рис. 1). 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].

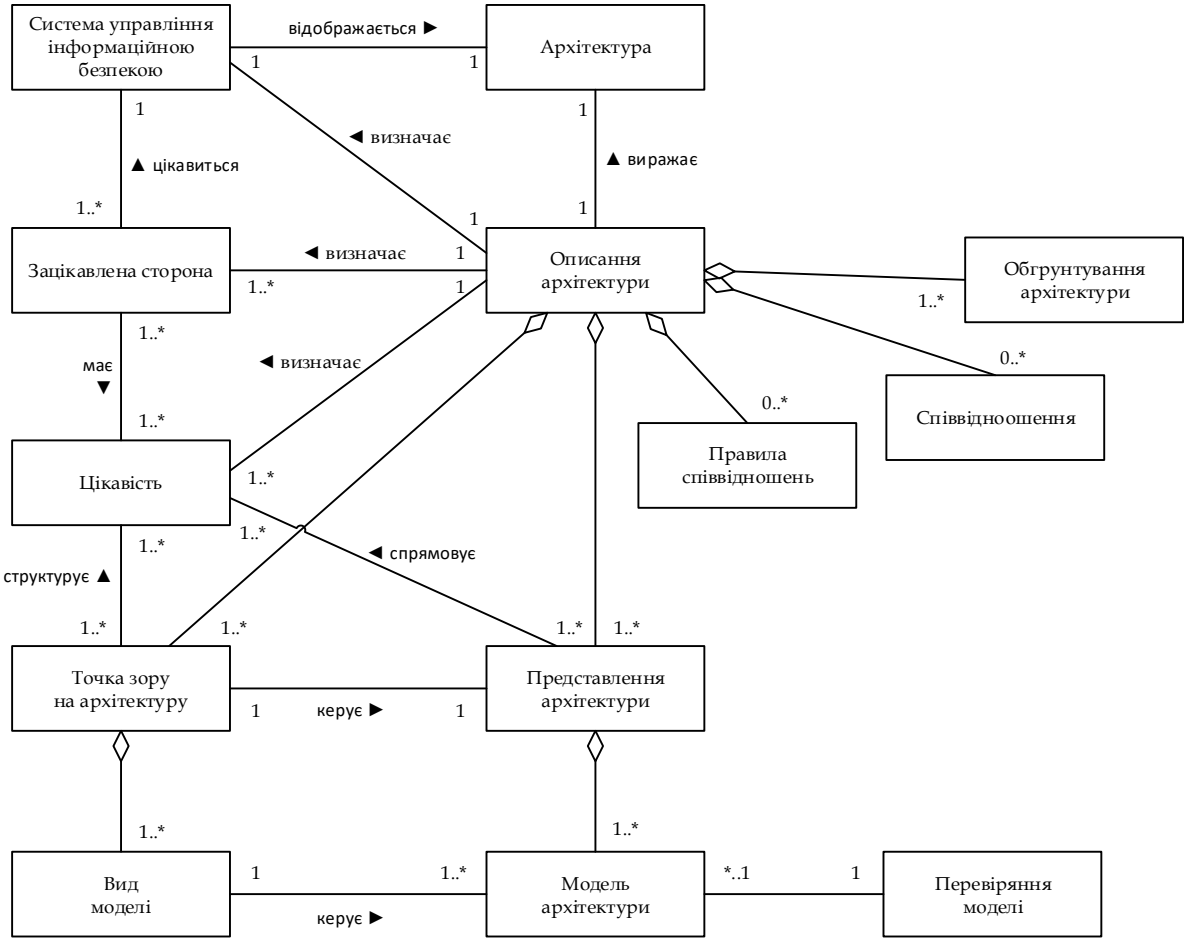

Рис. 1. Концептуальна модель описання архітектури системи управління інформаційною безпекою

2. 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]:

5) зацікавлених сторін для системи управління інформаційною безпекою;

6) вимог визначених зацікавлених сторін до забезпечення інформаційної безпеки;

3. 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].

4. 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.

5. 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.

6. 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.

Висновки

Отже, використання концептуальної моделі 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.

Література

[1]. ISO/IEC 42010:2011. Systems and software engineering. Architecture description. [First edition 2011-12-01]. Geneva, 2011, 46 p.

[2]. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27001:2013; Cor 1:2014, IDT). [Чинний від 2015-12-18]. Київ, 2016, 22 с.

[3]. Э. Халл, К. Джексон, Дж. Дик, *Инженерия требований*, пер. с анг. А. Снастина; под ред. В. Батоврина. М.: ДМК Пресс, 2017, 218 с.

[4]. ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Звід правил (ISO/IEC 27002:2013; Cor 1:2014, IDT). [Чинний від 2015-12-18]. Київ, 2016, 72 с.

[5]. ДСТУ ISO/IEC 27005:2015. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT). [Чинний від 2017-01-01]. Київ, 2016, 68 с.

[6]. ISO 31000:2018. Risk management. Guidelines. [Effective from 2018-02-15]. Geneva, 2018, 16 p.

[7]. ДСТУ IEC/ISO 31010:2013. Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT). [Чинний від 2014-07-01]. Київ, 2015, 80 с.

[8]. SP 800-12 Rev. 1:2017. 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]. FIPS 200:2006. Minimum Security Requirements for Federal Information and Information Systems [Online]. Available: https://csrc.nist.gov/publi-cations/detail/fips/200/final. Accessed on: June 15, 2019.

[10]. 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]. 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. Мохор, В. Цуркан, О. Бакалинський, "Архітектура системи управління інформаційною безпекою", *Безпека інформації в інформаційно-телекомунікаційних системах : матеріали XX Ювілейної Міжнародної науково-практичної конференції*. Київ : НДЦ "ТЕЗІС" КПІ ім. Ігоря Сікорського, С. 38, 2018.

[13]. М. Комаров, С. Гончар, А. 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. Комаров, С. Гончар, "Методика побудови системи управління інформаційною безпекою на об'єктах критичної інфраструктури", *Моделювання та інформаційні технології*, Вип. 81, С. 12-19, 2017.

[15]. В. Мохор, О. Бакалинський, О. Богданов, 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. Зырянова, "Методы оценки и прогнозирования рисков в информационных системах", *Интеграция образовательной, научной и воспитательной деятельности в организациях общего и профессионального образования:*

материалы IX Международной научно-практической конференции (Екатеренбург, 26 апреля 2017 года), С. 58-68, 2017.

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

[18]. Б. Ахметов, А. Корченко, А. Архипов, С. Казмирчук, *Построение систем анализа и оценивания рисков информационной безопасности. Теория и практические решения. Монография. В 2-кн. Кн.1*, Актау: редакционно-издательский отдел КГУТИ им. Ш. Есенова, 2018, 387 с.

[19]. В. Горицький, А. Мокій, "Дослідження методів обробки ризиків в системі управління інформаційною безпекою", *Перспективи телекомунікацій: збірник матеріалів Міжнародної науково-технічної конференції (Київ, 16-20 квітня 2018 року)*, С. 1-3, 2018.

[20]. А. Серова, "Анализ теоретических основ и программных средств аудита системы управления информационной безопасностью", *Социально-экономические и естественно-научные парадигмы современности: сборник трудов конференции (Ростов-на-Дону, 30 марта 2018 года)*, С. 829-837, 2018.

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

[22]. О. Юдін, "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. Воеводин, "Концептуальная модель объекта аудита информационной безопасности", *Сотр. Nanotechnol*, Вып. 3, С. 92-95, 2019. DOI: 10.33693/2313-223X-2019-6-3-92-95.

УДК 004[056.53+413.4]

Мохор В.В., Цуркан В.В., Дорогой Я.Ю. Концептуальная модель описания системы управления информационной безопасностью

Аннотация. *Рассмотрены основные понятия и свойства архитектуры системы управления информационной безопасностью учитывая влияние со стороны организации. При этом учтено осуществления воздействий организацией на указанную систему с учетом соотношений между ними. Поэтому архитектуру представлено набором элементов, отношений между элементами, которым присущи необходимые системные свойства. Кроме этого, акцентировано внимание на определении описанием архитектуры назначения каждого из элементов и соотношений между ними для достижения системой управления информационной безопасностью ожидаемого результата. Этот результат истолковано как обеспечение сохранности конфиденциальности, целостности и доступности информации по результатам оценки рисков. За основу концептуальной модели описания архитектуры системы управления информационной безопасностью взято рекомендации ISO/IEC 42010. Моделью отражаются основные понятия относительно обозначенной системы и ее архитектур. Такой подход важен для понимания практики их описания. В то же время это согласуется и позволяет толковать систему управления информационной безопасностью как систему, которая создана человеком. Она может состоять из аппаратных и программных средств, данных, людей, процессов, процедур, оборудования. Поэтому концептуальную модель описания архитектуры системы управления информационной безопасностью отражено такими элементами как архитектура и описание архитектуры; заинтересованные стороны и интересы; представления архитектуры и точки зрения; модели архитектуры; элементы и соотношения; обоснование архитектуры. Такой подход позволяет как выделить элементы системы управления информационной безопасностью, определить их назначение, так и установить соотношение между ними.*

Ключевые слова: *информационная безопасность, система управления информационной безопасностью, архитектура, описание архитектуры, представление архитектуры, модель архитектуры, концептуальная модель.*

Mokhor V., Tsurkan V., Dorohyi Ya. Conceptual architecture description model of information security management system

Abstract. *The basic concepts and properties of the information security management system architecture are considered in view of the influence of the organization. This takes into account the impact of the organization on the specified system and correspondences between them. Therefore, architecture is represented by a set of elements, relationships between elements that have the necessary system properties. In addition, the focus is on defining the architecture of the each elements purpose and the correspondences between them to achieve the expected result of the information security management system. This result is interpreted as ensuring the confidentiality, integrity and availability of information based on the risk assessment results. The conceptual model for describing the architecture of the information security management system is based on ISO/IEC 42010 guidelines. This approach is important for understanding the practice of describing them. At the same time, this is consistent and allows one to interpret the information security management system as a human-created system. It may consist of hardware and software, data, people, processes, procedures, equipment. Therefore, the conceptual model for describing the architecture of an information security management system is reflected by such elements as architecture and architecture description; stakeholders and interests; presentation of architecture and perspective; models of architecture; elements and correspondences; justification of architecture. This approach allows one to isolate the elements of the information security management system, determine their purpose, and establish a relationship between them.*

Keywords: *information security, information security management system, architecture, architecture description, architecture view, architecture model, conceptual model.*

Отримано 1 *грудня 2019 року*, затверджено редколегією 23 *грудня 2019 року*