УДК 004.056.53::519.876.2

ФУНКЦІОНАЛЬНЕ МОДЕЛЮВАННЯ СИСТЕМИ КЕРУВАННЯ РИЗИКОМ БЕЗПЕКИ ІНФОРМАЦІЇ

Володимир Мохор, Василь Цуркан, Ярослав Дорогий, Ольга Крук

Збереження конфіденційності, цілісності та доступності інформації в організації здійснюється шляхом розробляння та впроваджування системи керування ризиком. Для цього використовується узагальнений підхід, що описується в міжнародному стандарті ISO/IEC 27005:2011. З огляду на це, він уточнюються принципами та рекомендаціями ISO 31000:2009, IEC 31010:2009, ISO/TR 31004:2013. Тому означенні в цих нормативно-правових документах положення взаємодоповнюються та використовуються для розробляння та впроваджування системи керування ризиком безпеки інформації. Така система розробляється шляхом визначання для неї функціональних меж, функцій та умов їх виконання. Це стане можливим завдяки її функціональному моделюванню. Отримана при цьому функціональна модель представляється діаграмою в графічній нотації IDEF0. Відповідно до такого відображення, формалізується діяльність із керування ризиком безпеки інформації шляхом визначання мети, точки зору моделі та множини її функцій. Це дозволило наочно відобразити умови та результати їх виконання системою, що моделювалася, у встановлених межах.

Ключові слова: *ризик безпеки інформації, система керування ризиком безпеки інформації, функціональне моделювання, функціональна модель, IDEF0.*

Постановка проблеми

Керування ризиком безпеки інформації в організаціях здійснюється шляхом використання принципів та рекомендацій міжнародних стандартів ISO 31000 «Керування ризиками. Принципи та настанови», ISO/TR 31004 «Керування ризиками. Рекомендації для впроваджування ISO 31000», а також ISO/Guide 73 «Керування ризиками. Словник» [1-3]. Це обумовлено тим, що в ISO/IEC 27005 «Інформаційна технологія. Методи та засоби забезпечування безпеки. Керування ризиком безпеки інформації» наведено загальний підхід до керування ризиком безпеки інформації [4]. Тому означені в ньому положення до того ж доповнюються настановами міжнародного стандарту IEC 31010 «Керування ризиками. Методи оцінювання ризиків» [5]. Означені в цих нормативно-правових документах принципи та рекомендації використовуються для розробляння та впроваджування системи керування ризиком безпеки інформації. Така система розробляється з огляду на функціональні межі, функції та умови виконання функцій, що визначаються за результатами її функціонального моделювання в графічній нотації IDEF0 [6-8].

Аналіз останніх досліджень і публікацій

Аналізування та синтезування організаційно-технічних систем методом функціонального моделювання в нотації IDEF0 здійснюється в різноманітних сферах [8], зокрема й безпеки інформації [9-18]. Це обумовлено наявністю засобів для моделювання широкого спектру процесів забезпечування її конфіденційності, цілісності та доступності в організації на будь-якому рівні деталізації. Отримані при цьому результати використовуються як підґрунтя для прийняття рішень про реконструювання, замінювання або розробляння нової системи [8]. Так, система забезпечування безпеки інформації організації відображається графічною нотацією IDEF0 в [9]. Процес функціонування такої системи моделюється на прикладі військово-медичного закладу з виокремленням таких функцій як контролювання входу, виконання завдань, моніторинг. Разом з тим, функціональне моделювання процесу оцінювання захищеності інформаційних технологій за «Загальними критеріями» та основних процесів керування безпекою інформації в нотаціях IDEF0, IDEF3 та DFD розглядається в [10, 11]. При цьому виконується їх порівняльний аналіз та вибирається нотація DFD з огляду на високорівневість нотацій IDEF0, IDEF3. Такий вибір обумовлений дослідженням тільки потоків даних як при оцінюванні захищеності інформаційних технологій, так і в системі керування безпекою інформації без визначання функцій та послідовні їх виконання. Наприклад, в [12] вирішується завдання побудови моделей аналізу функціональної складової об'єкта дослідження. При цьому окреслюється межі його функціонування та завдяки декомпозиції функціональної моделі більш детально аналізуються його компоненти. Дослідження гарантій безпеки на основі моделювання процесу оцінювання в нотаціях IDEF0 і IDEF3 розглядається в [13]. Це дозволило задовольнити вимоги (ширина, глибина, строгість) до процесу оцінювання відповідності настановам міжнародного стандарту ISO/IEC 15408. Функціональне моделювання системи підтримки прийняття рішень стосовно забезпечування безпеки персональних даних виконано в [14]. Побудована функціональна модель дозволила описати предметну область та, як наслідок, сформувати інформаційний простір представляння знань про захист персональних даних. Крім цього, в нотації

IDEF0 побудовано функціональну модель автоматизованої системи керування безпекою інформації на основі багатоагентного підходу [15]. Серед основних функцій цієї системи виокремлено визначання складу багатоагнетного середовища, розробляння функцій і взаємозалежностей між агентами, кодування агентів. Завдяки цьому функціонально змодельовано та досліджено потік даних мережею. Варіанти побудови віртуальної інфраструктури в системі охорони здоров'я та завдання виявляння ризиків безпеки інформації в нотації IDEF0 моделюються в [16]. Такий підхід, орієнтується на аналізування процесів і потоків, виявляння вразливостей та недоліків функціонування інформаційної системи. На основі цього пропонується комплекс контрзаходів для зменшування ризику безпеки інформації. Вивчання потоків даних в інформаційній системі за допомогою функціонального моделювання в нотації IDEF0 виконано в [17]. Моделлю означеної системи відображається її функціональна структура, процеси та взаємодія між ними. Тоді як при функціональному моделюванні процесів оцінювання захищеності інформації і ресурсів системи електронної комерції в нотації IDEF0 виокремлено такі її функції [18]: побудова моделей системи електронної комерції, побудова моделей загроз і оцінювання ризиків, побудова моделей оцінювання рівня захищеності системи електронної комерції, побудова моделей формування звіту та надання рекомендацій.

З огляду на проведений аналіз останніх досліджень і публікацій, мета даної роботи формулюється як синтезування системи керування ризиком безпеки інформації шляхом визначання її функціональних меж і функцій методом функціонального моделювання в нотації IDEF0.

Виклад основного матеріалу дослідження

Функціональне моделювання системи керування ризиком безпеки інформації в нотації IDEF0 зводиться до її відображання окремим функціональним блоком як показано на рис. 1 [1-8]. Ним позначається функція верхнього рівня, її входи, виходи, обмеження, механізми та виклик, а також формулюється мета й точка зору побудови функціональної моделі. Завдяки цьому отриманою моделлю відображається структура системи керування ризиком безпеки інформації, функціональні межі, функції та умови їх виконання.

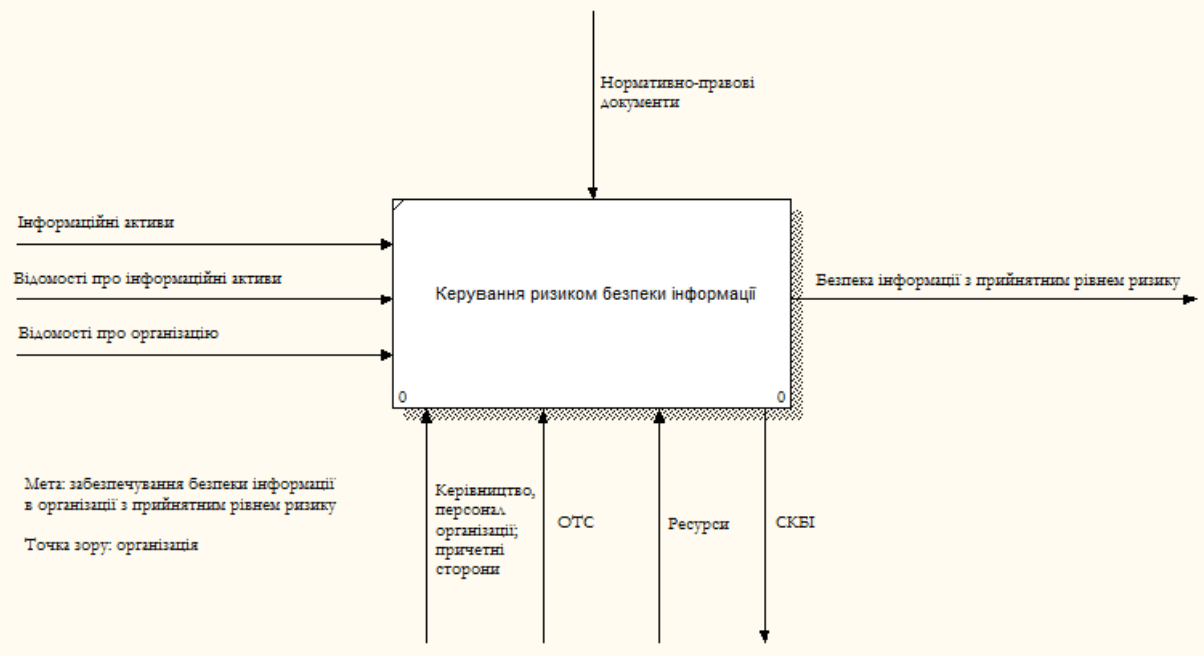

Рис. 1. Функціональна модель системи керування ризиком безпеки інформації

З огляду на рис. 1, система керування ризиком розробляється та впроваджується в організації з метою забезпечування безпеки інформації з прийнятним рівнем ризику. Це досягається шляхом встановлювання вимог до безпеки інформації в організації та, як наслідок, побудовою ефективної системи керування безпекою інформації [4, 19]. Тоді як система керування ризиком є її фундаментальною основою та невід'ємною частиною всіх видів діяльності, що пов'язані зі забезпечування безпеки інформації в організації [4].

Для цього визначаються потоки матеріальних та інформаційних об'єктів, перетворювання яких здійснюється функціональним блоком на рис. 1. У даному випадку матеріальними об'єктами є інформаційні активи організації, що описуються інформаційними потоками, а саме:

– інформацією про інформаційні активи, наприклад: назва, місце знаходження, прізвище, ім'я, по-батькові, посада відповідальних за них;

– інформацією про організацію, що використовується для з'ясування внутрішнього та зовнішнього контекстів системи керування ризиком безпеки інформації. Завдяки цьому визначаються її сфера та межі впроваджування, критерії оцінювання ризику, критерії впливу та критерії прийняття ризику. Результативність цього визначання обумовлюється наявністю таких відомостей про організацію [4]:

– стратегія та політика організації;
– процеси в організації;
– функції та структура організації;
– правові, керівні та договірні вимоги в організації;
– політика безпеки інформації в організації;
– місце знаходження організації та його географічні характеристики;
– обмеження діяльності організації;
– очікування причетних сторін;
– соціокультурне середовище.

Водночас діяльність із керування ризиком безпеки інформації обмежується вимогами, настановами та рекомендаціями відповідних нормативно-правових документів (див., наприклад [20], рис. 2). Зокрема, ними визначається ця діяльність, вводяться обмеження на процеси в рамках неї.

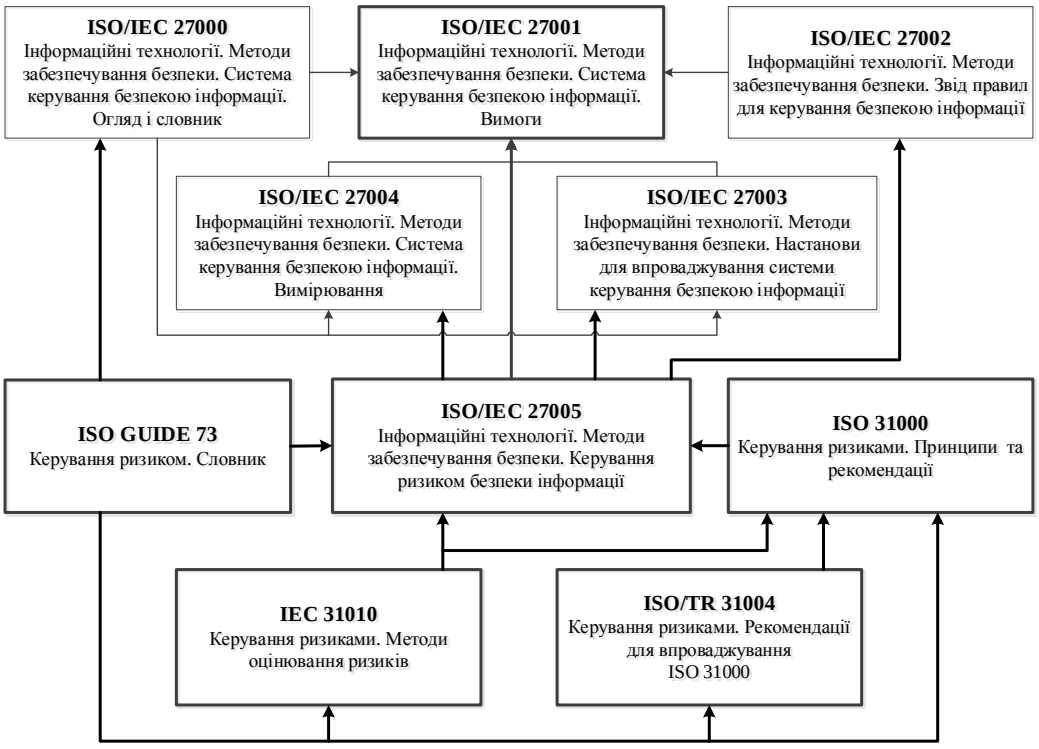

Рис. 2. Взаємозв'язок міжнародних стандартів серій ISO 27k та ISO 31k.

З урахуванням визначених нормативно-правовими документами обмежень здійснюється керування ризиком безпеки інформації на основі відомостей про інформаційні активи та організацію за допомогою

– механізмів (див. рис. 1[1-5, 8]):
  – керівництво, персонал організації та причетні сторони, що залучаються до розроблення та впроваджування системи керування ризиком безпеки інформації або мають відношення до цієї діяльності (причетні сторони);
  – організаційно-технічна система (ОТС), що визначається як організаційна структура та комплекс технічних засобів (обладнання) для керування ризиком безпеки інформації;
  – ресурси, що використовуються для керування ризиком безпеки інформації, наприклад [5]: компетентність, досвід, здібності та можливості групи оцінювання ризику; обмеження щодо часу та інших ресурсів організації; наявний бюджет, у разі залучання зовнішніх ресурсів.
– та виклику (див. рис. 1[1-5, 8]):
  – система керування безпекою інформації (СКБІ), що визначається для забезпечування взаємозв'язку системи керування ризиком безпеки з системою керування безпекою інформації.

Крім цього, за основним принципом функціонального моделювання в нотації IDEF0 класифікуються явища та події, що пов'язані з функціону-

ванням системи керування ризиком безпеки інформації. [1-5, 8]. Така класифікація спрощує визначання функціональних меж та сприяє вироблянню одноманітних підходів та прийомів моделювання означеної системи в сфері безпеки інформації [7, 8]. Це досягається поділом функцій на дві групи: основні та додаткові. У рамках кожної з цих груп визначаються класи блоків перетворювання для їх відображання. Внаслідок цього отримується відношення ієрархічної підпорядкованості за принципом «зверху-вниз» (див. рис. 3): діяльність – субдіяльність – процес – підпроцес [3, 7, 8].

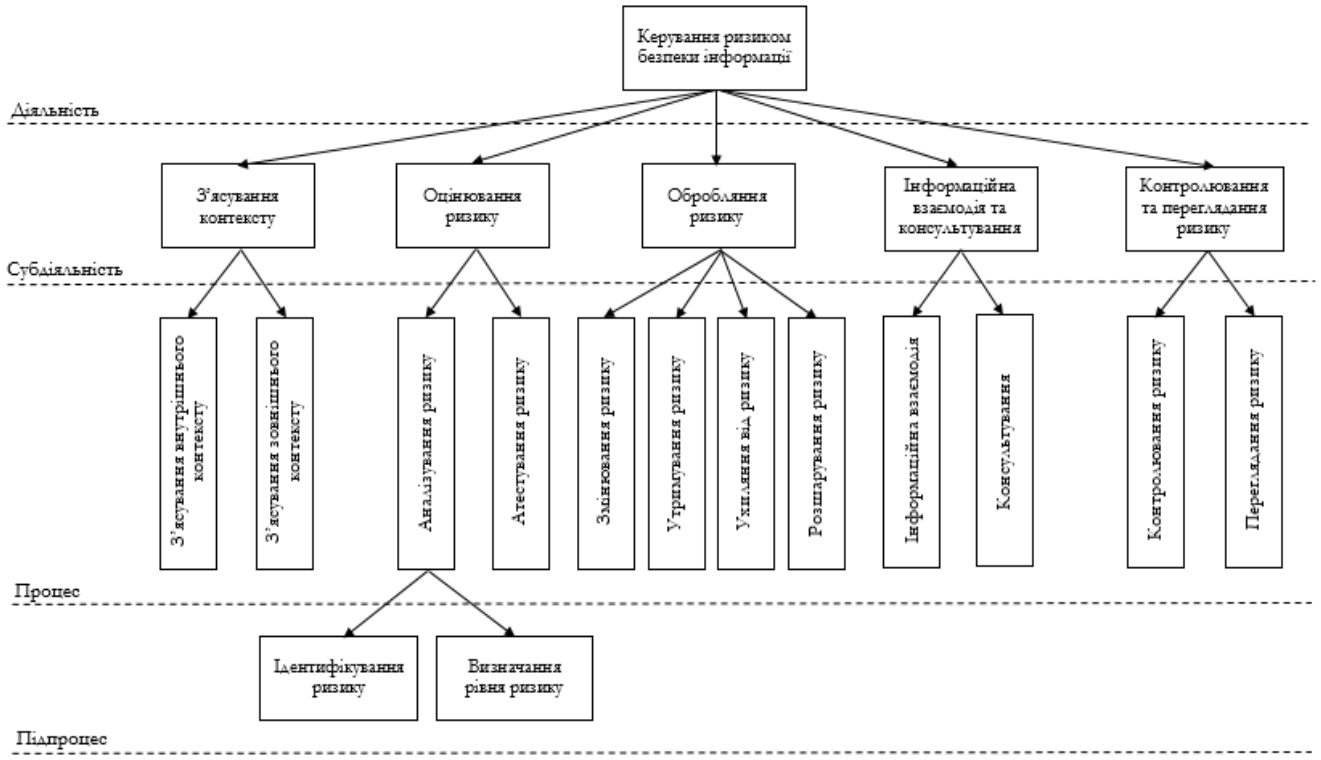

Рис. 3. Класифікація функцій системи керування ризиком безпеки інформації

Завдяки такому підходові можливе встановлювання відповідності між функціями та механізмами їх виконання. У даному випадку механізм може тлумачиться як організаційно-технічна структура. Водночас одним із основних принципів функціонального моделювання є «відокремленість» організації від функцій [7, 8]. Однак, незважаючи на це, між ієрархією функцій та ієрархією механізмів існує відповідність, що відображена на рис. 4 [8]. При цьому система керування ризиком безпеки інформації моделюється без орієнтування на організаційно-технічну систему, але з можливістю встановлювання відповідності між елементами функціональної моделі та об'єктами організаційно-технічної структури. Внаслідок цього вона розглядається як результат функціонального моделювання системи керування ризиком безпеки інформації [7, 8].

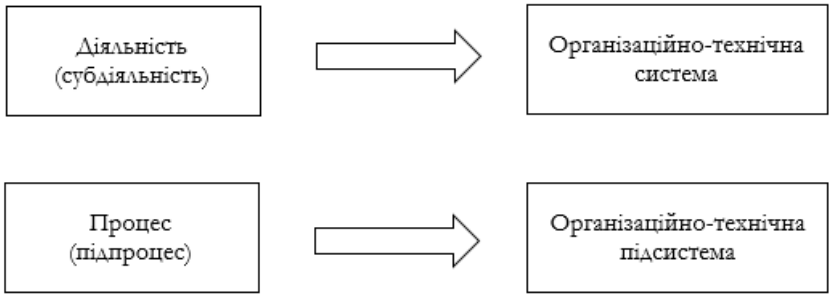

Рис. 4. Відповідність між функціями та організаційно-технічними структурами

Висновки

За результатами функціонального моделювання синтезовано систему керування ризиком безпеки інформації шляхом її відображання окремим функціональним блоком в нотації IDEF0. Завдяки цьому встановлено функцію верхнього рівня означеної системи як керування ризиком. Дану функцію визначено діяльністю із забезпечування безпеки інформації з прийнятним рівнем ризику в інтересах організації на основі інформації про неї та її інформаційні активи за допомогою механізмів і виклику з урахуванням обмежень, що накладаються відповідними нормативно-правовими документами.

Завдяки цьому стало можливим класифікування діяльності із керування ризиком безпеки інформації за принципом «зверху-вниз». Такою класифікацією спрощено визначання функціональних меж та вироблено єдиний підхід до моделювання відповідної системи в сфері безпеки інформації. Як наслідок, отримано відношення ієрархічної підпорядкованості: діяльність – субдіяльність – процес – підпроцес.

Перспективи подальших досліджень

У перспективах подальших досліджень планується декомпозиціювати функціональну модель системи керування ризиком безпеки інформації з огляду на отримане відношення ієрархічної підпорядкованості. Внаслідок цього буде визначено її підсистеми, модулі (комплекси) та блоки. Це сприяє зведенню діяльності, субдіяльності, процесів, підпроцесів до операцій та дій керування ризиком безпеки інформації і, в кінцевому випадку, деталізуванню відношення ієрархічної підпорядкованості до означених рівнів.

ЛІТЕРАТУРА

[1]. Мохор В. В. Изложение стандарта «ISO 31000:2009. Risk management. Principles and guidelines» на русском языке / В. В. Мохор, А. М. Богданов / Das Management. – 2011. – № 3. – С. 5-18.

[2]. Мохор В. В. BS 31100:2008. Обращение с рисками: общие практические рекомендации / В. В. Мохор, А. М. Богданов / Das Management. – 2011. – № 4. – С. 7-28.

[3]. Мохор В. В. Спроба локалізації ISO GUIDE 73:2009 «Risk management – Vocabulary» / В. В. Мохор, О. М. Богданов, О. М. Крук, В. В. Цуркан // Безпека інформації. – 2012. – Том 18, № 2. – С. 12-22.

[4]. Information technology. Security techniques. Information security risk management : ISO/IEC 27005:2011. – Second edition 2011-06-10. – Geneva, 2011. – P. 68.

[5]. Керування ризиком. Методи загального оцінювання ризику (IEC 31010:2009, IDT) : ДСТУ IEC 31010:2013. – [Чинний від 2014-07-01]. – К. : Мінекономрозвитку України, 2015. – 73 с. – (Національний стандарт України).

[6]. Systems and software engineering. System life cycle processes : ISO/IEC 15288:2015. – Second edition 2015-05-15. – Geneva, 2015. – P. 108.

[7]. Цуркан В. В. Функціональний підхід до моделювання процесу менеджування ризику безпеки інформації / В. В. Цуркан // Информационные технологии и безопасность. Оценка состояния: Материалы международной конференции ИТБ-2013. – К. : ИПРИ НАН Украины, 2013. – С. 193 - 194.

[8]. Методология функционального моделирования IDEF0 : РД IDEF0:2000. – [Действует с 2001-07-02]. – М. : Госстандарт России, 2000. – 75 с.

[9]. Атисков А. Ю. Автоматизация процесса проектирования системы информационной защиты предприятия средствами IDEF и UML / А. Ю. Атисков, Т. В. Монахова // Труды СПИИРАН. – 2006. – Т. 2, Вып. 3. – С. 115-119.

[10]. Зайцев О. Е. Подходы к структурному моделированию основных компонентов безопасности ИТ «Общих критериев» / О. Е. Зайцев, А. В. Любимов, А. В. Суханов // Теория и технология программирования и защиты информации. Применение вычислительной техники : труды 11-й науч.-техн. конф. (Санкт-Петербург, 18 мая 2007 г.) – С. 56-60.

[11]. Любимов А. В. Функциональное моделирование системы управления информационной безопасности организации по семейству стандартов ISO/IEC 2700x / А. В. Любимов, С. В. Шустиков, Н. В. Андреева // Научно-технический вестник информационных технологий, механики и оптики. – 2008. – № 7 (52). – С. 251-257.

[12]. Криволапов В. Г. Комплексная методика моделирования рисков информационной безопасности открытых систем : автореф. дис. на соискание научной степени канд. техн. наук : спец. 05.13.19 «Методы и системы защиты информации, информационная безопасность» / В. Г. Криволапов. – М., 2009. – 23 с.

[13]. Комин Д. С. IDEF модели оценки уровня гарантий информационной безопасности / Д. С. Комин, А. В. Потий // Вісник Харківського національного університету. – 2010. – № 925, вип. 14. – С. 98-105.

[14]. Васильев В. И. Система поддержки принятия решений по обеспечению персональных данных / В. И. Васильев, Н. В. Белков / Вестник УГАТУ. – 2011. – Том 15, № 5 (45). – С. 54-65.

[15]. Цыбулин А. М. Многоагентный подход к построению автоматизированной системы управления информационной безопасностью предприятия / А. М. Цыбулин // Известия ЮФУ. Технические науки. Информационная безопасность. – 2012. – № 12. – С. 111-116.

[16]. Булдакова Т. И. Анализ информационных рисков виртуальных инфраструктур здравоохранения [Электронный ресурс] / Т. И. Булдакова, С. И. Суятинов, Д.А. Миков // Информационное общество. – Режим доступа: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/87f599404bc9073d44257c2a00476485. – Дата доступа: февраль 2016. – Название с экрана.

[17]. Миков Д. А. Анализ методов изучения потоков данных для оценки рисков информационной безопасности / Д. А. Миков // Prospero. – 2014. – № 7. – С. 27-33.

[18]. Оладько В. С. Программный комплекс для оценки уровня защищенности систем электронной коммерции / В. С. Оладько // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. – 2015. – № 4 (33). – С. 46-53.

[19]. Information technology. Security techniques. Information security management systems. Requirements :

ISO/IEC 27001:2013. – Second edition 2013-10-01. – Geneva, 2013. – P. 23.

[20]. Мохор В. В. Нормативно-правовий аспект розробляння системи менеджовування ризику безпеки інформації / В.В. Мохор, В. В. Цуркан, О. М. Крук // Інформаційна безпека України : зб. наук. доп. та тез науково-технічної конференції (м. Київ, 12-13 березня 2015 р.). – К. : Київський національний університет імені Тараса Шевченка, 2015. – С. 122-123.

REFERENCE

[1]. Mokhor, V. V. & Bogdanov, A. M. (2011), 'Presentment of the standart «ISO 31000:2009. Risk management. Principles and guidelines» in russian', *Das Management*, No. 3, pp. 5-18.

[2]. Mokhor, V. V. & Bogdanov, A. M. (2011), 'BS 31100:2008. Risks handling : general practical recommendations', *Das Management*, 2011, No. 4, pp. 7-28.

[3]. Mokhor, V. V., Bohdanov, O. M., Kruk, O. V., Tsurkan, V. V. (2012), 'Localization attempt ISO GUIDE 73:2009 «Risk management – Vocabulary»', *Bezpeka ìnformacìì*, Vol. 18, No. 2, pp. 12-22.

[4]. International Organization for Standardization (2011), ISO/IEC 27005: *Information technology. Security techniques. Information security risk management*, Geneva, 68 p.

[5]. National standard of Ukraine (2013), DSTU IEC 31010: *Risk management. Risk assessment techniques*, Kyiv, 73 p.

[6]. International Organization for Standardization (2015), ISO/IEC 15288: *Systems and software engineering. System life cycle processes,* Geneva, 108 p.

[7]. Tsurkan, V. V. (2013), 'Functional approach to process modeling of information security risk managing', *Proceeding of informatioaln technologies and security. Assessment of international conference*, Problem of registration information Institute of National Academy of Sciences of Ukraine, Kyiv, pp. 193-194.

[8]. Guidance document (2000), GD IDEF0: *Methodology of functional modeling IDEF0*, Moscow, 75 p.

[9]. Atiskov, A. I. & Monakhova, T. V. (2006), 'Process automation of system engineering of enterprise information protection by IDEF and UML', *SPIIRAS Proceedings*, Vol. 2, Iss. 3, pp. 115-119.

[10]. Zaitcev, O. E (2007), 'Structural modeling approaches of the main components of IT security' in A. V., Liubimov, A. V., Sukhanov, *Proceedings of The theory and technology of programming and data protection. Application of computer technology on international conference*, ITMO University, St. Petersburg, pp. 56-60.

[11]. Liubimov, A. V., Shustikov, S. V., & Andreeva, N. V. (2008), 'Functional modeling of information security management system of the organization over the ISO/IEC 2700x standards', *Scientific and technical journal of information technologies, mechanics and optics*, № 7 (52), pp. 251-257.

[12]. Krivolapov, V. G. (2009), 'Complex technique of information security risk modeling open systems', PhD thesis, Moscow Engineering Physics Institute.

[13]. Komin, D. S. & Potii, A. V. (2010), 'The IDEF models of the security assurance level evaluation', *Bulletin of V. Karazin Kharkiv National University: mathematical modeling, information technology, automated control systems»*, No. 925, Iss. 14, pp. 98-105.

[14]. Vasilev, V. I. & Belkov, N. V. (2011), 'Decision Support System for the assurance of personal data', *Vestnik UGATU*, Vol. 15, No. 5 (45), pp. 54-65.

[15]. Tcybulin, A. M. (2012), 'Multi-agent approach to the construction of an automated enterprise information security management system', *Izvestiya SFedU: engineering sciences*, No. 12, pp. 111-116.Buldakova, T. I., Suiatinov, S. I. & Mikov, D. A. (2013), 'The analysis of information risks of virtual health infrastructures', *Information society*, viewed 17 February 2016, http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/87f599404bc9073d44257c2a00476485

[16]. Mikov, D. A. (2014), 'Analysis of the study data flow techniques for assessing information security risks', *Prospero*, No. 7, pp. 27-33.

[17]. Oladko, V. S. (2015), 'Software system to assess security level of e-commerce systems', *University Journal of Control and Computer Science*, No. 4 (33), pp. 46-53.

[18]. International Organization for Standardization (2013), ISO/IEC 27001: *Information security management systems. Requirements,* Geneva, 23 p.

[19]. Mokhor, V. V. (2015), 'Normative and legal aspects a information security risk management system designing' in V. V., Tsurkan, O. M., Kruk, *Proceedings of information security of Ukraine on ukrainian conference*, Taras Shevchenko National University, Kyiv, pp. 122-123.

ФУНКЦИОНАЛЬНОЕ МОДЕЛИРОВАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ РИСКОМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Сохранение конфиденциальности, целостности и доступности информации в организации осуществляется путем разработки и внедрения системы управления риском. Для этого используется обобщенный подход, который описывается в международном стандарте ISO/IEC 27005:2011. С учетом этого, он уточняется принципами и рекомендациями ISO 31000:2009, ISO/TR 31004:2013, IEC 31010:2009. Поэтому обозначенные в этих нормативно-правовых документах положения взаимодополняются и используются для разработки и внедрения системы управления риском безопасности информации. Такая система разрабатывается путем определения для нее функциональных границ, функций и условий их выполнения. Это станет возможным благодаря ее функциональному моделированию. Полученная при этом функциональная модель представляется диаграммой в нотации IDEF0. В соответствии с таким отображением, формализуется деятельность по управлению риском безопасности информации путем определения цели, точки зрения модели и множества ее функций. Это позволило наглядно отобразить условия и результаты их выполнения моделируемой системой в установленных границах.

Ключевые слова: риск безопасности информации, система управления риском безопасности информации, функциональное моделирование, функциональная модель, IDEF0.

FUNCTIONAL MODELING OF INFORMATION SECURITY RISK MANAGEMENT SYSTEM

Preservation of confidentiality, integrity and availability of information in organization is achieved by risk management system designing and implementation. For these purposes, a generic approach described in the international standard ISO/IEC 27005: 2011 is used. In view of above-mentioned, it is specified by the principles and recommendations of the ISO 31000:2009, ISO/TR 31004:2013, IEC 31010:2009. Therefore, the definitions from these legal documents are used for information security risk management system design and implementation. The system is developing by identifying her functional boundaries, functions and terms of their performance. This will be possible by the way of its functional simulation. Thus, resulting functional model will be presented in IDEF0 graphical diagram notation. According to this view, information security risk management activities are formalized by defining objectives, terms of model and set of functions. At last, such approach has given us the possibility to visualize the conditions and results of their execution by the system was simulated, within the prescribed limits.

Keywords: information security risk, information security risk management system, functional modeling, functional model, IDEF0.

Мохор Володимир Володимирович, доктор технічний наук, професор, завідувач кафедри кібербезпеки та застосування автоматизованих інформаційних систем та технологій Державного закладу «Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут».
E-mail: v.mokhor@gmail.com.

Мохор Владимир Владимирович, доктор технических наук, профессор, заведующий кафедрой кибербезопасности и применения автоматизированных информационных систем и технологий Государственного учреждения «Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт».

Mokhor Volodymyr, doctor of engineering science, professor, head of cybersecurity and application of information systems and technologies academic department, State institution «Institute of special communications and information security National technical university of Ukraine « Kyiv polytechnic institute».

Цуркан Василь Васильович, кандидат технічних наук, провідний науковий співробітник науково-дослідного центру Державного закладу «Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут».
E-mail: v.v.tsurkan@gmail.com.

Цуркан Василий Васильевич, кандидат технических наук, ведущий научный сотрудник научно-исследовательского центра Государственного учреждения «Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт».

Tsurkan Vasyl, candidate of engineering science, leading researcher of State institution «Institute of special communications and information security National technical university of Ukraine «Kyiv polytechnic institute».

Дорогий Ярослав Юрійович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та застосування автоматизованих інформаційних систем та технологій Державного закладу «Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут».
E-mail: argusyk@gmail.com.

Дорогой Ярослав Юрьевич, кандидат технических наук, доцент кафедры кибербезопасности и применения автоматизированных информационных систем и технологий Государственного учреждения «Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт».

Dorohyi Yaroslav, candidate of engineering science, associate professor, associate professor of cybersecurity and application of information systems and technologies academic department, State institution «Institute of special communications and information security National technical university of Ukraine «Kyiv polytechnic institute».

Крук Ольга Миколаївна, молодший науковий співробітник Інституту проблем моделювання в енергетиці імені Г.Є. Пухова Національної академії наук України.
E-mail: onk@conferen.ru.

Крук Ольга Николаевна, младший научный сотрудник Института проблем моделирования в энергетике имени Г.Е. Пухова Национальной академии наук Украины.

Kruk Olha, junior researcher of Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine.