DOI: 10.20535/2411-1031.2018.6.2.153488
УДК 004.056.53::001.891.572

ЮЛІЯ КОЖЕДУБ

ФУНКЦІОНАЛЬНА МОДЕЛЬ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Предметом дослідження є моделювання системи забезпечення інформаційною безпекою для організацій. Виокремлено проблеми моделювання означених систем, що пов'язані з розкриттям як природи процесу забезпечення інформаційної безпеки, так і з напрямом розробки практичних методів безпеки інформації. При цьому ретельно вивчаються статистика порушень, причини, що їх обумовлюють, особи порушників, сутність прийомів, які використовуються порушниками, обставини, за яких було виявлене порушення (модель порушника інформаційної безпеки). Практичне розв'язання реалізовано частково комплексною системою захисту інформації, де обов'язковими документами, що входять до Плану захисту, є: модель загроз і модель порушника інформаційної безпеки Потреби щодо захисту інформації наявні для будь-яких організацій, підприємств і установ будь-якої сфери діяльності і будь-якої форми власності. Такі вимоги зумовлені класифікацією інформації, нормативно-правовими документами, запитами замовника стосовно розроблення і впровадження систем забезпечення інформаційної безпеки. Для створення таких систем пропонується використання наукового методу – моделювання. Його універсальність і дієвість доведено практикою застосування і відтворення інструментами реалізації результатів. Тому метою статті є розроблення функціональної моделі системи забезпечення інформаційною безпекою організації. Результати роботи відображають теоретичне дослідження основ моделювання, аналізування практичного застосування результатів для різноманітних систем (зокрема, систем забезпечення інформаційної безпеки), вимоги та критерії до моделей і перевірки відтворюваності реальних процесів, явищ і функціонування систем забезпечення інформаційної безпеки. Підсумовуючи, констатуємо важливість наведеного дослідження для цілей створення унікальної для кожної окремо узятої організації системи, метою якої є забезпечення інформаційної безпеки. Різноманітність моделей та способів моделювання підтверджує безумовну та виняткову цінність дослідження із застосуванням принципів моделювання для організацій України сфери забезпечення інформаційної безпеки.

Ключові слова: інформаційна безпека, забезпечення інформаційної безпеки, система забезпечення інформаційної безпеки, функціональне моделювання, функціональна модель.

Постановка проблеми. Моделювання процесів узагальнено передбачає послідовне виконання трьох етапів дослідження [1]. Перший – перехід від вихідної практичної проблеми до постановки теоретичного завдання. Другий – вивчення і вирішення цього завдання. Третій – перехід від висновків за результатами вирішення завдання назад до практичної проблеми.

У сфері моделювання процесів (зокрема діяльності або управління та в інших сферах застосування), доцільно виділити чотири складові, щоб досягнути цілей моделювання: чітка поставка завдання – формулювання прийнятної моделі – застосування підходящого наукового методу дослідження – визначення умов застосовності [1].

Перший складник моделювання – завдання, як правило, породжено потребами прикладної сфери діяльності. При цьому відбувається одна з можливих математичних формалізацій реальної ситуації. Математична формалізація зазвичай дає змогу змоделювати очікувані результати в рамках вибраної моделі й дослідити як вибрана модель може допомогти перевірити гіпотезу, що досліджується [2].

Завдання може бути породжено також узагальненням потреб ряду прикладних сфер діяльності (наприклад, порівняння двох груп пацієнтів або під час зіставлення результатів обробки деталей двома способами). Таким чином, одна і та сама сформульована математична модель може застосовуватися для вирішення найрізноманітніших за своєю прикладною сутністю завдань. Важливо підкреслити, що виділення переліку завдань знаходиться поза законами і правилами математики – це перелік вимог технічного завдання, який фахівці різних сфер діяльності надають фахівцям з математичного моделювання для подальшої формалізації. Вибір методу, який використовується в межах певної моделі, відбувається за законами і правилами математики, тобто йдеться, наприклад, про метод оцінювання, про метод перевірки гіпотези, про метод доказовості теореми. У подальшому розробляються і досліджуються алгоритми щодо практичного застосування і доказовості наведених припущень. Розглянемо останній елемент четвірки – умови застосовності. Цей елемент використовують для перевірки й опису реальної дійсності процесів, що досліджуються.

Аналіз останніх досліджень і публікацій. Методологічний аналіз – перший етап моделювання систем, процесів управління, та й взагалі будь-якого дослідження. Він визначає вихідні постановки для теоретичного опрацювання, а тому багато в чому і успіх всього дослідження. Аналіз динаміки розвитку методів моделювання дає змогу виділити найбільш перспективні методи, наведені в [2], які застосовуються насамперед в економічних науках. Численні моделі процесів управління описані в літературі [2] - [5]. Їх практичним використанням зазвичай займаються інформаційно-аналітичні підрозділи, служби контролю, якості і надійності, маркетингу. Методологію моделювання процесів наведено в [6].

Проблеми моделювання системи забезпечення інформаційної безпеки пов’язані з розкриттям природи явища, яке полягає у порушенні властивостей інформації, так і з напрямом розроблення практичних методів її захисту (моделі захисту). Серйозно вивчається статистика порушень, причини, що їх обумовлюють, особи порушників, сутність прийомів, які використовуються порушниками, обставини, за яких було виявлене порушення (модель порушника інформаційної безпеки). Практичне розв’язання реалізовано частково комплексною системою захисту інформації, де обов’язковими документами, що входять до Плану захисту організації є: модель загроз і модель порушника інформаційної безпеки.

Незважаючи на широке застосування результатів моделювання в науці і техніці, комплексного та системного дослідження щодо моделювання систем забезпечення інформаційної безпеки немає.

Метою статті є побудова функціональної моделі системи забезпечення інформаційної безпеки, яка б дала змогу створити умови для сталого функціонування організації, запобігати загрозам її безпеці, захищати законні інтереси організації від протиправних і злочинних посягань порушників інформаційної безпеки, недопущення викрадання інформаційних активів, розголошення, втрати, витоку, викривлення і знищення інформації.

Для досягнення вказаної мети необхідно вирішити такі окремі **завдання**:

- проаналізувати теоретичні положення основ моделювання для цілей забезпечення інформаційної безпеки;
- показати критерії і умови застосування функціональних моделей для систем забезпечення інформаційної безпеки;
- побудувати модель системи забезпечення інформаційною безпекою, а також створену функціональну модель відобразити блок-схемою.

Виклад основного матеріалу дослідження. Елементами системи забезпечення інформаційної безпеки є [7]:

- споруди, приміщення і території, на яких розташовані автоматизовані інформаційні системи і де можуть проводитись переговори й обмін інформацією;
- технічні засоби автоматизованих інформаційних систем – комп’ютерне обладнання, обладнання локальних мереж, кабельна система, телекомунікаційне обладнання;
- програмні засоби автоматизованих інформаційних систем;

– інформація, що зберігається і обробляється у автоматизованій інформаційній системі;

– автономні знімні носії інформації;

– співробітники організації, які працюють з автоматизованою інформаційною системою і є носіями інформації про захист системи.

Щоб досягнути стану захищеності системи забезпечення інформаційної безпеки, потрібно виконати такі завдання [7]:

– визначення категорії доступу до інформації;

– прогнозування і своєчасне виявлення загроз інформаційній безпеці, причин і умов, що сприяють нанесенню фінансових, матеріальних і моральних збитків;

– створення умов функціонування з найменшою вірогідністю реалізації загроз інформаційній безпеці і нанесення різних видів втрат (наприклад, вартісних і моральних);

– створення механізму й умов оперативного реагування на загрози інформаційної безпеки і прояви негативних тенденцій у функціонуванні організації, ефективне запобігання виникненню подій і інцидентів інформаційної безпеки на основі правових, організаційних і технічних заходів, і засобів забезпечення інформаційної безпеки;

– створення умов для максимального відшкодування і локалізації шкоди, завданої неправомірними діями фізичних і юридичних осіб, послаблення негативного впливу наслідків порушення інформаційної безпеки на досягнення стратегічних цілей організації [7].

Модель (фр. modèle, у перекладі з лат. modulus – “міра, аналог, зразок”) – це система, дослідження якої є засобом для отримання інформації про іншу систему [8, с. 48]; уявлення деякого реального процесу, пристрою або концепції [9].

Модель є абстрактне уявлення реальності в будь-якій формі (наприклад, в математичній, фізичній, символічній, графічній чи дескриптивній), призначене для подання певних аспектів цієї реальності, що дає змогу отримати відповіді на питання, що досліджуються [10].

Кількість параметрів, що характеризують поведінку не тільки реальної системи, але і її моделі, дуже значна. Для спрощення процесу вивчення реальних систем виділяють чотири рівні моделей, що розрізняються кількістю і ступенем важливості враховуваних властивостей і параметрів. Це – функціональна, принципова, структурна і параметрична моделі.

Функціональна модель призначена для вивчення особливостей роботи (функціонування) системи і її призначення у взаємозв’язку з внутрішніми та зовнішніми елементами.

Функція – найсуттєвіша характеристика будь-якої системи, відображає її призначення, і те, для чого вона потрібна. Подібні моделі оперують, перш за все, з функціональними параметрами. Графічним представленням цих моделей є блок-схеми. Вони відображають порядок дій, спрямованих на досягнення заданих цілей (так звана “функціональна схема”). Функціональною моделлю є абстрактна модель.

Модель принципу дії характеризує найсуттєвіші (принципові) зв’язки і властивості реальної системи. Це основні фізичні, біологічні, хімічні, соціальні і тому подібні явища, що забезпечують функціонування системи, або будь-які інші принципові положення, на яких базується досліджуваний процес (або планована діяльність). Прагнуть до того, щоб кількість врахованих властивостей і параметрів, що її характеризують, була незначною (залишають найбільш важливі), а прозорість моделі – максимальною, так щоб трудомісткість роботи з моделлю не відволікала увагу від суті досліджуваних явищ. Як правило, описують подібні моделі параметри – функціональні, а також фізичні характеристики процесів і явищ. Принципові вихідні положення (методи, способи, напрямки тощо) покладено в основі будь-якої діяльності або роботи.

Графічним представленням моделей принципу дії слугують: блок-схема, функціональна схема, принципова схема.

Поняття “інформація” (походить від лат. informatio – ознайомлення, пояснення) і на сьогоднішній день є одним із поширених і ключових в різних сфера діяльності. Це пояснюється багатоаспектністю інформації (існуванням в живій і неживій природі, в кібернетичних системах, в суспільстві), різноманітністю її форм проявів в матеріальному світі, особливостями в способах її вивчення і використання різними областями науки і практики [11]. У визначенні поняття “інформація” в різні роки переважали три основні підходи: недетермінований, техноцентричний і антропоцентричний.

Недетермінований підхід до визначення поняття інформації (від лат. determinare – обмежити, визначити) полягає у відмові від тлумачення інформації на тій підставі, що вона є фундаментальним поняттям, яке має необмежені рамки. Один із засновників кібернетики Норд Вінер визначав інформацію як позначення змісту, який отримується нами із зовнішнього світу в процесі пристосування до нього і приведення відповідно до нього нашого мислення. Він стверджував, що: “Інформація є інформація, а не матерія і не енергія” [11].

У розвитку цієї ідеї ряд дослідників розглядали інформацію як основу всього існуючого, первинну складову всіх явищ і процесів.

Значення техноцентричного підходу полягає в тому, що інформацію ототожнюють з даними, які мають кількісний вимір (обсяг, швидкість передачі, пропускну здатність каналу). Основоположник теорії інформації Клод Шеннон в 60-х роках XX століття обґрунтував поняття “інформації” як «упорядкованої субстанції, яку можна описати математично: кількість інформації тим більше, чим більше невизначеності усувається при отриманні цієї інформації» [7].

Цей підхід і зараз переважає в точних науках і широко застосовується під час розробки та реалізації багатьох, насамперед, апаратно-програмних засобів захисту інформації. Однак в цьому випадку не розглядається змістовний аспект інформації, що не дає змогу використовувати вказаний підхід до правового регулювання інформаційних відносин.

Зміст антропоцентричного підходу полягає в тому, що інформацію ототожнюють з відомостями або фактами, які теоретично можуть бути отримані і засвоєні, тобто перетворені в знання. Саме цей підхід знайшов широке застосування в юридичній науці і чинному законодавстві.

Модель в загальному сенсі (узагальнена модель) створюється з метою отримання і (або) зберігання інформації специфічним об’єктом (у формі уявного образу, опису знаковими засобами або матеріальної системи), що відображає властивості, характеристики та зв’язки об’єкта-оригіналу довільної природи, суттєві для задачі , розв’язуваної суб’єктом [12, с. 44]. Наприклад, для теорії прийняття рішень найбільш корисні моделі, які виражаються словами чи формулами, алгоритмами і іншими математичними засобами [1].

Моделі можна поділити на такі види:

1) функціональні моделі – висловлюють прямі залежності між ендогенними і екзогенними змінними (ендогенні змінні – це такі змінні, значення яких визначаються в ході діяльності компонентів (елементів) системи, тобто “всередині” системи. Екзогенні змінні – це змінні, які визначаються або дослідником, або ззовні, тобто в будь-якому випадку діють на систему ззовні [1]);

2) моделі, виражені за допомогою систем рівнянь щодо ендогенних величин;

3) моделі оптимізаційного типу. Основна частина моделі – система рівнянь щодо ендогенних змінних, мета таких моделей – знайти оптимальне рішення для деякого показника;

4) імітаційні моделі – дуже точне відображення досліджуваного явища. Математична формалізація через це може містити складні, нелінійні, стохастичні залежності.

Моделі також можна покласифікувати на керовані і прогнозні. Керовані моделі відповідають на такі питання: “Що буде, якщо ...?”, “Як досягти бажаного?”, і містять три групи змінних: 1) змінні, що характеризують поточний стан об’єкта; 2) дії, що керують –

змінні, що впливають на зміну цього стану і піддаються цілеспрямованому вибору; 3) вихідні дані і зовнішні впливи, тобто параметри, що задаються ззовні, і основні параметри.

У прогнозних моделях керування не виділено явно. Вони відповідають на питання: "Що буде, якщо все залишиться без змін?"

Також моделі можна поділити за способом вимірювання часу на безперервні і дискретні. У будь-якому разі, якщо в моделі є наявним час, то модель називається динамічною. Найчастіше в моделях використовується дискретний час, тому що інформація надходить дискретно: звіти, баланси та інші документи складаються періодично, але з формальної точки зору безперервна модель може виявитися більш простою для вивчення.

Особливе місце займають в методології моделювання імітаційні системи. Як підкреслено в [13], "будь-яка модель, в принципі, імітаційна, бо вона імітує реальність", оскільки вона аналізує процес за допомогою варіантних розрахунків. Отже, імітаційна система – це сукупність моделей, що імітують протікання досліджуваного процесу, об'єднана зі спеціальною системою допоміжних програм та інформаційною базою, що дають змогу досить просто й оперативно реалізувати варіантні розрахунки [13]. Таким чином, під імітацією розуміється чисельний метод проведення машинних експериментів з математичними моделями, що описують поведінку складних систем протягом тривалих періодів часу [3], при цьому імітаційний експеримент складається з наступних шести етапів:

1) формулювання завдання;
2) побудова математичної моделі;
3) складання програми для ЕОМ;
4) оцінка придатності моделі;
5) планування експерименту;
6) обробка результатів експерименту.

Дещо інший (більш детальний) список етапів наведено в [4]. Імітаційне моделювання (simulation modelling) широко застосовується в різних областях, наприклад в економіці [3]. Іншим застосунком може бути теорія ігор (інші назви – теорія конфлікту, або теорія конфліктних ситуацій), що зародилася як теорія раціональної поведінки двох гравців з протилежними інтересами. Теорія ігор є так само імітаційною динамічною моделлю. Вона найбільш проста, коли кожен з гравців прагне мінімізувати свій середній програш, тобто максимізувати свій середній виграш. Звідси ясно, що теорія ігор схильна надмірно спрощувати реальну поведінку в ситуації конфлікту. Учасники конфлікту можуть оцінювати свій ризик за іншими критеріями. За наявності декількох гравців можливі коаліції. Велике значення має стійкість точок рівноваги і коаліцій.

Ще один яскравий приклад застосування імітаційного моделювання – теорія дуополії (інша назва – модель конкуренції двох фірм) О. Курно. Новий поштовх теорії дуополії надано у класичній монографії Дж. Фон Неймана і О.Моргенштейна [5]. У підручниках, присвячених цій теорії зазвичай розбирається "дилема в'язня" і точка рівноваги Неша.

Будь-яку організацію можна розглядати як складну систему, для якої практично неможливо отримати єдиний опис процесу її виробничої діяльності, що відповідає на всі питання з точки зору управління, придатного для досягнення всіх ключових цілей і завдань. Будучи за своєю природою багатогранною за формами і змістом уявлення, організація як сукупність взаємопов'язаних компонентів може бути описана у вигляді цілого ряду самостійних, закінчених "проекцій", кількість яких визначається головним чином цілями управління [14].

Наприклад, одна і та сама організація може бути представлена:

- деревом процесів, за допомогою яких організація виконує свою місію;
- сукупністю джерел і каналів зв'язку, потоків інформації і типів даних;
- організаційною структурою;
- інфраструктурою (території, будівлі, споруди, комунікації).

Кожна організація (як система) створюються для того, щоб створювати додану вартість

(отримувати прибуток), тому визнано, що для загального керівництва ключовою метою є представлення об'єкта у вигляді мережі процесів, що визначають його місію. Такі процеси прийнято називати бізнес-процесами. Саме уявлення (моделювання) об'єкта у вигляді набору бізнес-процесів визначає всі інші його "проекції" (див. рис.1).

Рисунок1 – Представлення різних моделей для об'єкта моделювання [14]

Подібні системи завжди ґрунтуються на проведенні глибокого передпроектного обстеження діяльності організації. Результатом цього обстеження є експертний висновок, в якому окремими пунктами виносяться рекомендації щодо усунення вразливостей в управлінні діяльністю. На підставі цього висновку, безпосередньо перед проектом впровадження системи автоматизації, проводиться так звана реорганізація бізнес-процесів. Подібні комплексні обстеження організацій завжди є складними і істотно відрізняються один від одного завданнями.

Процес опису об'єкта моделювання (системи) для цілей загального керівництва починають з опису процесів, що визначають цільове призначення, і продовжують до досягнення необхідного ступеня "прозорості", достатнього для коректного аналізу і вироблення ефективних управлінських рішень.

Аналіз функціонування американських компаній показує [14], що в тих організаціях, де потік робіт організовується так, щоб відповідати наявній функціональності організації, керівництво середньої ланки робить наголос на аналізі ресурсів, операцій, що виконуються, і на суворому дотриманні персоналом регламентувальних правил і розпоряджень. Очевидно, що в таких організаціях процеси завжди оптимізуються так, щоб відповідати організаційній структурі організації, а персонал має сильну мотивацію слідувати правилам і мінімізувати споживання ресурсів. В організаціях, де функції, ресурси і управління скеровуються відповідно до виконуваних процесів, керуючий персонал концентрує увагу на роботі з внутрішніми постачальниками і на обслуговуванні внутрішніх споживачів. У цій ситуації персонал має сильну мотивацію для концентрації уваги на якості та інших характеристиках продуктів, що виробляються (наданні послуг). Такий аналіз також показує, що при збереженні функціональності організації неможливо досягти значних результатів від проведення реінжинірингу ділових процесів, так як це призводить тільки до субоптимальних рішень.

Моделювання завжди передбачає прийняття припущень щодо ступеня важливості досліджуваного явища, процесу, системи. При цьому повинні задовольнятися такі вимоги до моделей:

– адекватність, тобто відповідність моделі вихідній реальній системі і врахування,

перш за все, найбільш важливих якостей, зв'язків і характеристик. Оцінити адекватність вибраної моделі, особливо, наприклад, на початковій стадії проектування, коли вид системи, що створюється, ще невідомий, дуже складно. У такій ситуації часто покладаються на досвід попередніх розробок або застосовують методи, наприклад, послідовних наближень;

– точність, тобто ступінь збігу отриманих в процесі моделювання результатів із заздалегідь встановленими, бажаними. Тут важливим завданням є оцінка потрібної точності результатів і наявної точності вихідних даних, узгодження їх як між собою, так і з точністю використовуваної моделі;

– універсальність, тобто можливість застосування моделі до аналізу ряду однотипних систем в одному або декількох режимах функціонування. Це дозволяє розширити область застосовності моделі для вирішення більшого кола завдань;

– доцільна економічність, тобто точність одержуваних результатів і спільність рішення задачі повинні ув'язуватися з витратами на моделювання. І вдалий вибір моделі, як показує практика, – результат компромісу між відпущеними ресурсами і особливостями використовуваної моделі.

Моделювання систем забезпечення інформаційної безпеки дає змогу визначити необхідні і достатні умови її захищеності. Організаційні питання відіграють важливу роль під час розробки технічних аспектів захисту інформації й окремих її компонентів. Вирішення проблеми забезпечення інформаційної безпеки орієнтовано на два завдання. Перше – переконати користувачів у необхідності забезпечення інформаційної безпеки і досягти однозначного розуміння вирішення проблеми, друге – синтезувати систему забезпечення інформаційної безпеки. Під час розробки системи забезпечення інформаційної безпеки доцільно пам'ятати, що абсолютна захищеність інформації неможлива, отже необхідно оцінити ступінь ризику інформаційної безпеки. Під час переходу до експлуатації системи забезпечення інформаційної безпеки необхідно підтримувати заданий рівень її захищеності. Інакше можуть виникати проблеми, пов'язані зі зміною кадрів, з невідповідністю розробленої схеми захисту реальним умовам, тому необхідна періодична оцінка рівня захищеності інформації. Ключовою фігурою в теорії захисту інформації є порушник, його практичні і теоретичні можливості, апріорні знання, час і місце дій.

При синтезі системи забезпечення інформаційної безпеки необхідно відповісти на питання:

– якою має бути структура;
– які функції є обов'язковими;
– які тактика і стратегія щодо порушників, фактів порушень та їх наслідків.

Міжнародний стандарт [15] визначає інформаційну безпеку як: "збереження конфіденційності, цілісності та доступності інформації". Тоді як міжнародний стандарт [16] – це перелік вимог до системи менеджменту інформаційної безпеки, обов'язкових для сертифікації організації, яка запровадила систему менеджменту інформаційної безпеки, а сам стандарт є настановою щодо впровадження. Його можна використати під час проектування механізмів контролю, вибраних організацією для оброблення ризиків інформаційної безпеки.

ISO/IEC 27001 визначає процеси, що представляють можливість встановлювати, застосовувати, переглядати, контролювати і підтримувати ефективну систему менеджменту інформаційної безпеки; встановлює вимоги до розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та вдосконалення документованої системи менеджменту інформаційної безпеки в контексті існуючих бізнес ризиків організації [11].

Система управління інформаційною безпекою на основі стандарту ISO/IEC 27001 дає змогу:

– зробити більшість інформаційних активів найбільш зрозумілими для загального менеджменту організації;
– виявляти основні загрози безпеки для наявних бізнес-процесів;
– розраховувати ризики і приймати рішення на основі бізнес цілей організації;

– забезпечити ефективне управління системою в критичних ситуаціях;

– проводити процес виконання політики безпеки (знаходити і виправляти слабкі місця в системі забезпечення інформаційної безпеки);

– чітко визначити особисту відповідальність;

– досягти зменшення і оптимізації вартості підтримки системи забезпечення інформаційної безпеки безпеки;

– полегшити інтеграцію підсистеми безпеки в бізнес-процеси і інтеграцію з іншими стандартами на системи менеджменту;

– продемонструвати клієнтам, партнерам, власникам бізнесу свою прихильність до інформаційної безпеки;

– отримати міжнародне визнання і підвищення авторитету організації, як на внутрішньому ринку, так і на зовнішніх ринках;

– підкреслити прозорість і чистоту бізнесу перед законом завдяки відповідності вимогам стандарту.

Поряд з елементами управління у [16] приділено велику увагу питанням розробки політики безпеки, роботі з персоналом (прийом на роботу, навчання, звільнення з роботи), забезпечення безперервності виробничого процесу, юридичним вимогам. Вимоги стандарту [16] мають загальний характер і можуть використані широким колом організацій – малими, середніми і великими – у комерційних і промислових секторах ринку: фінансовому та страховому, у сфері телекомунікацій, комунальних послуг, у секторах роздрібної торгівлі і виробництва, різних галузях сервісу, транспортній сфері, органах влади .

Інформаційної безпеки досягають впровадженням відповідного набору елементів управління, зокрема політики, процесів, процедур, організаційною структурою і програмним забезпеченням та апаратними функціями. Ці елементи управління повинні розроблені, впроваджені, моніторені, оглядні та покращенні, за необхідності, для того, щоб впевнитись, що безпеки досягнуто і бізнес-цілі організації будуть виконані.

Важливим моментом створення інформаційної системи з метою автоматизації інформаційних процесів організації є аналіз функціональної взаємодії об’єктів автоматизації. Аналітики наводять результати у вигляді функціональної моделі. Склад функціональної моделі істотно залежить від контексту конкретної системи і може бути представлено за допомогою досить широкого спектра документів.

Визначимо функціональну модель інформаційної системи, як сукупність деяких моделей, призначених для опису процесів обробки інформації. Будемо називати ці моделі конструкціями функціональної моделі. Нижче наведено перелік основних конструкцій функціональної моделі, які необхідні для виконання проектування інформаційної системи.

У дослідженні теорій управління досить часто використовують комп’ютерні моделі. Вони можуть бути представлені у вигляді структури системи управління, технологічної схеми процесу управління, комплексу характеристик управління, чинників, що впливають на ефективність управління, структури інформації, взаємодії функцій управління тощо.

Застосування подібних моделей може бути досить ефективним під час проведення дослідження систем управління, проте слід мати на увазі, що методи дослідження дають відчутний ефект і корисний результат лише в комплексі. Моделювання найбільш ефективно, коли дослідник має справу з добре структурованими проблемами, коли достатньо інформації для оцінки ситуацій і проблем, а також наявна відпрацьована методологія роботи з моделями. Найбільш відомими труднощами використання моделей у дослідженні систем управління є дуже висока вартість, недостовірна початкова інформація про об’єкт, надмірне спрощення характеристик, помилки в методології моделювання.

Під час управління організаціями використовують традиційні форми концептуального моделювання, де враховуються інформаційні потоки, які проходять між керуючими ланками, і лише деякі з них можуть взаємодіяти між собою, утворюючи керівну інформаційну систему для підтримки і прийняття рішень. Нові задачі застосування інформаційної системи дають змогу розгортати інформаційні процеси в бік обробки транзакцій і зв’язків між ними.

Для ефективного інформаційного управління доцільно використовувати процес моделювання як засіб покращення інформативності процесів управління, а також як спосіб виділення інформаційних рівнів організаційної структури організації. Моделювання застосовується для опису діяльності організації за допомогою використання графічних зображень, подій, станів та інформаційних ланцюгів і атрибутів. Створені моделі інформаційних процесів можуть містити проаналізовані дані, що виникли в процесі управління і, можливо, інші залучені зовнішні інформаційні потоки.

Одним із основних пріоритетів у вивченні моделювання є аналіз управління інформаційним процесом організації. Така активність у залученні цього процесу до інформаційного управління зумовила науковий та комерційний інтерес, направлений на створення прогресивних (оптимальних і раціональних) рішень для управління інформаційними потоками. Яскравим прикладом моделювання діяльності організації є процес моделювання інформаційних потоків – як спосіб документування управлінських процесів в організації.

Процес моделювання широко застосовується в організаціях як спосіб підвищення поінформованості та визначення надлишковості або дефіциту інформаційних процесів в окремих ланках ієрархічної структури. Цей підхід застосовують для опису діяльності організації і містить графічні зображення, логічні події станів потоків інформації, інші атрибути.

Будуючи модель інформаційної системи, часто не мають формальної теоретичної основи, яка відрізняє її від інших методик. Тому є необхідність створення теоретичних рамкових принципів (англ. *Framework*) для отримання пояснень, хоча недосконаліть теоретичної основи в концептуальному моделюванні визначається як критична перспектива побудови бази даних. Організація, як живий організм являє собою систему організованих інформаційних процесів, що надходять ззовні, що циркулюють всередині, створюваних в якості результату. При цьому далеко не всі вони формуються свідомо керівництвом і/або працівниками, об’єктивна реальність грає свою помітну роль.

Функціональна модель – це система пов’язаних систем (див., наприклад, рис. 2, 3): окрім запланованого, багатоструктурні елементи, процеси і функції виникають у тому числі як результат помилок в управлінні, нерозуміння працівником поставленого завдання або необ’єктивної оцінки досягнутого результату керівником. Неадекватний аналіз зовнішніх впливів, дублювання завдань, різноманіття рішень, психологія прийняття рішень і багато інші обставини є підставами для дослідження моделей управління організацією.

Важливим моментом створення інформаційної системи з метою автоматизації інформаційних процесів організації є аналіз функціональної взаємодії об’єктів автоматизації. Аналітики наводять результати у вигляді функціональної моделі. Склад функціональної моделі істотно залежить від контексту конкретної системи і її може бути представлено за допомогою досить широкого спектра документів у вигляді текстової і графічної інформації.

Система управління інформаційною безпекою є перш за все системою документації, на всі процеси, що стосуються інформаційної діяльності, та інформаційних відносин організації. Зазначена система документації відповідає вимогам міжнародних стандартів серії ISO/IEC 27k, а також залежить від структури організації, виду та форми власності організації (приватна, державна) й сфери діяльності самої організації, оскільки інформація наявна скрізь і вимоги до неї наявні завжди. На рис. 2 представлено систему, що об’єднує 14 напрямів забезпечення інформаційної безпеки поіменованих так, що відображають сутність функціонування системи менеджменту.

У разі застосування системи управління інформаційною безпекою кожна з категорій безпеки (А.5–А.18, див. рис. 2) є системою, що безпосередньо пов’язана і взаємодіє з іншими системами. Кожну категорію безпеки можна відобразити набором правил, що містяться у процедурах інструкціях, звітах, планах, методиках, політиках тощо, системоутворювальним елементом який є інформація, що потребує захисту за законодавством України.

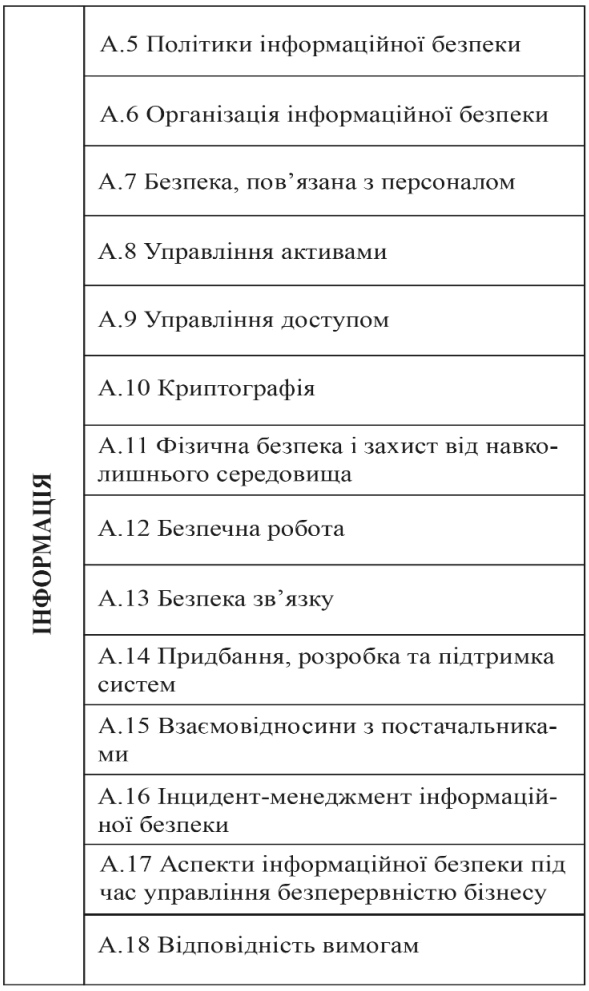

Рис. 2 – Модель «Система управління інформаційною безпекою»

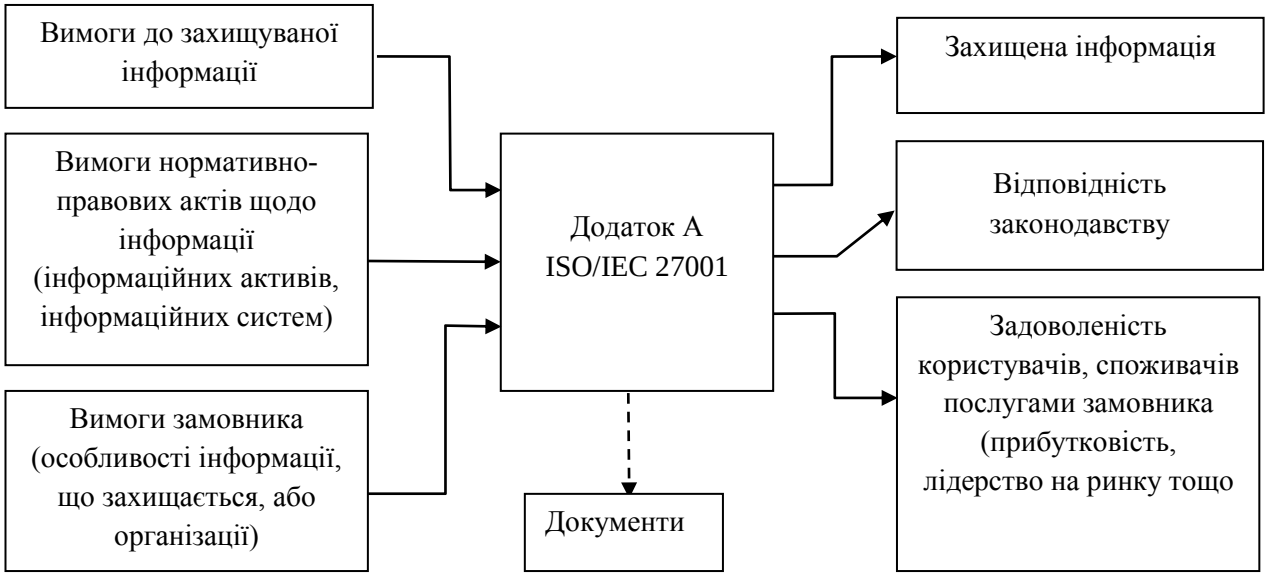

Рисунок 3 – Функціональна модель системи забезпечення інформаційною безпекою

Висновки. Численні методи та інструменти моделювання інформаційних процесів виникли внаслідок попиту на створення власних інформаційних систем організацій для поліпшення стану забезпечення інформаційної безпеки. Ці методи дають змогу наочно

продемонструвати складові інформаційного процесу в єдиній схемі функціонування організацій. Для цього використано ефективну та зручну методологією моделювання, що забезпечить доволі широкі масштаби охоплення діяльності організації із моделюванням всієї повноти технологічного процесу. Запропонована функціональна модель використовує стандарти серії ISO/IEC 27k. Додаток А ISO/IEC 27001 є системоутворювальним чинником, що поєднує елементи системи забезпечення інформаційної безпеки організації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] А. И. Орлов, *Менеджмент*. Москва, Российская Федерация: Изумруд, 2003.

[2] А. И. Орлов, *Эконометрика*. Москва, Российская Федерация: Экзамен, 2003.

[3] Т. Нейлор, *Машинные имитационные эксперименты с моделями экономических систем*. Москва, СССР: Мир, 1975.

[4] К. А. Багриновский, и В. П. Бусыгин, *Математика плановых решений*. Москва, СССР: Наука, 1980.

[5] Дж. фон Нейман, и О. Моргенштейн, *Теория игр и экономическое поведение*. Москва, СССР: Наука, 1970.

[6] Е. И. Всяких, *Практика и проблематика моделирования бизнес-процессов* [Електронний ресурс]. Доступно: https://econ.wikireading.ru/73264.

[7] В. Ю. Артемов, О. С. Лєнков, А. С. Пашков, О. М. Стаднік, та В.О. Хорошко, *Нормативно-правовий довідник з охорони інформації в Україні*. Київ, Україна: ДУІКТ, 2010.

[8] А. И. Уёмов, *Логические основы метода моделирования*. Москва, СССР: Мысль, 1971.

[9] International Organization for Standardization. *ISO/IEC/IEEE 24765:2010. Systems and software engineering. Vocabulary* [Online]. Available: https://www.smaele.nl/documents/iso/ISO-24765-2010.pdf.

[10] М. Р. Когаловский, *Глоссарий по информационному обществу*. Москва, Российская Федерация: Институт развития информационного общества, 2009.

[11] С. Л. Ємельянов, Н. І. Логінова, О. В. Тодощак, та В. Ф. Якутко, *Використання інформаційних технологій в судах*. Одеса, Україна: Фенікс, 2014.

[12] Я. Г. Неуймин, *Модели в науке и технике. История, теория, практика.* Ленинград, СССР: Наука, 1984.

[13] Н.Н. Моисеев, *Математические задачи системного анализа*. Москва, СССР: Наука, 1981.

[14] Функциональные модели и процесс моделирования [Online]. Available: http://www.itstan.ru/ funk-strukt-analiz/funkcionalnye-modeli-i-process-modelirovanija.html.

[15] International Organization for Standardization. *ISO/IEC 27000:2018. Information technology. Security techniques. Information security management systems. Overview and vocabulary* [Online]. Available: https://www.iso.org/standard/73906.html.

[16] International Organization for Standardization. *ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements* [Online]. Available: https://www.iso.org/standard/54534.html.

[17] International Organization for Standardization. *ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls* [Online]. Available: https://www.iso.org/standard/54533.html.

[18] М. Р. Когаловский, *Перспективные технологии информационных систем*. Москва, Российская Федерация: ДМК Пресс; Компания АйТи, 2003.

[19] В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, та С. В. Толюпа, *Інформаційна та кібербезпека: соціотехнічний аспект*. Київ, Україна: ДУТ, 2015.

Стаття надійшла до редакції 21 вересня 2018 року.

REFERENCES

[1] A. I. Orlov, *Management*. Moscow, Russia: Izumrud, 2003.

[2] A. I. Orlov, *Econometrics*. Moscow, Russia Examen, 2003.

[3] T. Naylor, *Machine imitation experiments with models of economic systems*. Moscow, USSR: Mir, 1975.

[4] K. A. Bagrinovsky, and V. P. Busygin, *Mathematics of planned decisions*. Moscow, USSR: Nauka, 1980.

[5] Dzh. fon Neumann, and O. Morgenshtein, *Theory of games and economic behavior*. Moscow, USSR: Nauka, 1970.

[6] E. I. Vsjakikh, *Practice and problems of business process modeling* [Online]. Available: https://econ.wikireading.ru/73264.

[7] V. Yu. Artemov, O. S. Lenkov, A. S. Pashkov, O. M. Stadnik, and V. O. Khoroshko, *Normative legal guide on information security in Ukraine*. Kyiv, Ukraine: DUIKT, 2010.

[8] A. I. U'omov, *Logical Foundations of the Modeling Method*. Moscow, USSR: Mysl, 1971.

[9] International Organization for Standardization. *ISO/IEC/IEEE 24765:2010. Systems and software engineering. Vocabulary* [Online]. Available: https://www.smaele.nl/documents/iso/ISO-24765-2010.pdf.

[10] M. R. Kogalovsky, *Glossary on the Information Society*. Moscow, Russia: Institute for the Development of the Information Society, 2009.

[11] S. L. Yemelianov, N. I. Loginova, O. V. Todoshchak, and V. F. Yakutko, *Use of Information Technologies in Courts*. Odessa, Ukraine: Phenix, 2014.

[12] Y.G. Neuymin, *Models in science and technology. History, theory, practice*. Leningrad, USSR: Nauka, 1984.

[13] N. N. Moiseev, *Mathematical problems of system analysis*. Moscow, USSR: Nauka, 1981.

[14] *Functional models and modeling process*, electronic resource: http://www.itstan.ru/funk-strukt-analiz/funkcionalnye-modeli-i-process-modelirovanija.html.

[15] International Organization for Standardization. *ISO/IEC 27000:2018. Information technology. Security techniques. Information security management systems. Overview and vocabulary* [Online]. Available: https://www.iso.org/standard/73906.html.

[16] International Organization for Standardization. *ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements* [Online]. Available: https://www.iso.org/standard/54534.html.

[17] International Organization for Standardization. *ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls* [Online]. Available: https://www.iso.org/standard/54533.html.

[18] M. R. Kogalovsky, *Perspective technologies of information systems*. Moscow, Russia: DMK Press; Company AiTi, 2003.

[19] V. L. Buryachok, V. B. Tolubko, V. O. Khoroshko, and S. V. Tolyupa, *Information and cyber security: the socio-technical aspect*. Kyiv, Ukraine: DUT, 2015.

ЮЛИЯ КОЖЕДУБ

ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Предметом исследования является моделирование системы обеспечения информационной безопасности организаций. Выделены проблемы моделирования таких систем, которые связаны как с раскрытием природы процесса обеспечения информационной безопасности, так и с направлением разработки практических методов безопасности информации. При этом тщательно изучаются статистика нарушений, причины, которые их обуславливают, личности нарушителей, сущность приёмов, используемых нарушителями, обстоятельства выявления нарушений (модель нарушителя информационной безопасности).

Практическое решение частично представлено комплексной системой защиты информации, где обязательным документом для организаций, что входят в Плант защиты, являются: модель угроз и модель нарушителя. Потребности в защите информации присущи для любых организаций, предприятий и учреждений любой сферы деятельности и любой формы собственности. Такие требования обусловленные классификацией информации, нормативно-правовыми документами, запросами заказчика относительно разработки и внедрения систем обеспечения информационной безопасности. Для создания таких систем предлагается использование научного метода – моделирования. Его универсальность и результативность доведено практикой применения и воспроизведения инструментами реализации результатов. Поэтому целью статьи является разработка функциональной модели системы обеспечения информационной безопасности организации. Результаты работы отображают теоретическое исследование основ моделирования, анализа, практического применения результатов для разнообразных систем (в частности, систем обеспечения информационной безопасности), требования и критерии к моделям и проверке возобновления реальных процессов, явлений и функционирования систем обеспечения информационной безопасности. Обобщая, констатируем важность данного исследования для целей создания уникальной для каждой отдельно взятой организации системы, целью которой является обеспечение информационной безопасности. Разнообразие моделей и способов моделирования подтверждает безусловную и исключительную ценность исследования с применением принципов моделирования для организаций Украины сферы обеспечения информационной безопасности.

Ключевые слова: информационная безопасность, обеспечение информационной безопасности, система обеспечения информационной безопасности, функциональное моделирование, функциональная модель.

YULIIA KOZHEDUB

FUNCTIONAL MODEL OF INFORMATION SECURITY SYSTEMS

The subject of the study is modeling the information security system for organizations where there are special requirements for protected information under the legislation of Ukraine. Special requirements for information protection are available for any organizations, enterprises and institutions of any sphere of activity and any form of ownership. Such requirements are conditioned by the classification of information, regulatory documents, special requests of the customer for such security information systems, as well as the verification of the compliance of sharp requirements and the satisfaction of users and/or customers with the establishment of information security systems. The research topic is related to the creation of a security information system and attempts to simulate the most effective and most effective protection system by means of a scientific method – modeling, which is used in various fields of activity. The versatility and effectiveness of simulation has been proven by the practice of applying and reproducing tools for implementing simulation results. Therefore, the purpose of this article is to develop a functional model of information security for an organization where circulating confidential and/or service information that needs protection in accordance with Ukrainian legislation. The research was based on the methodology of simulating and comparing different types, levels, and applications of models in the practical work of creating information security systems. The results of the work reflect the theoretical study of the foundations of modeling, analysis of the practical application of results for various systems, knowledge of requirements and criteria for models, and verification of the reproducibility of real processes, phenomena and the functioning of information security systems, based on the restrictions and conditions regarding the protected information. The scope of the results is due to the specific needs of organizations to calculate various results using the simulation methodology. Summing up, we note the importance of this study for the purpose of creating a unique information security system for each individual organization whose purpose is to provide

information security. The variety of models and methods of modeling confirms the unconditional and exceptional value of the research using the principles of simulation for Ukrainian security information security organizations.

Key words: information security, providing information security, information security system, functional modeling, functional model.

Юлія Василівна Кожедуб, кандидат технічних наук, доцент кафедри управління, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0001-6181-5519.

E-mail: JuliaKozhedub@email.ua.

Юлия Васильевна Кожедуб, кандидат технических наук, доцент кафедры управления, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.

Yuliia Kozhedub, candidate of technical sciences, associate professor at the management academic department, Institute of special communication and information protection National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.