ISSN 2411-1031. Information Technology and Security. January-June 2015. Vol. 3. Iss. 1 (4)

INFORMATION SECURITY

УДК 004.91/.056.5::006.015.8

ЮЛІЯ КОЖЕДУБ

ПРО ОСОБЛИВОСТІ СИСТЕМНОГО ТА ПРОЦЕСНОГО ПІДХОДІВ ПІД ЧАС СТВОРЕННЯ ІТ-ПРОЕКТІВ У СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ

Наводиться узагальнене теоретичне дослідження відомих наукових підходів до створення ІТ-проектів у сфері захисту інформації, що їх запроваджують для систем захисту інформації. Дослідження також ґрунтувалось на міжнародних документах, що їх застосовують фахівці у сфері захисту інформації. Загальновизнана міжнародна практика стандартизації і наукові підходи, застосовувані під час створення ІТ-проектів у сфері захисту інформації є головними чинниками, що відповідають вимогам щодо захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства.

Ключові слова: захист інформації, інформація, ІТ-проекти, міжнародні стандарти, процесний підхід, системний підхід.

Постановка проблеми. Словник термінів ЮНЕСКО визначає інформацію як універсальну субстанцію, що пронизує усі сфери людського буття, що слугує нам провідником знань і думок, вона є й інструментом спілкування, взаєморозуміння та співробітництва для ствердження стереотипів мислення й поведінки.

Визначаючи у такий спосіб термін «інформація», ми намагаємось охопити багатогранність цього поняття, що беззаперечно стосується найширшого всеосяжного знання людини про цей світ і про своє положення у ньому. Ось тому є розмежування даних, що має стосунок до різних сторін життя людини, ділення контекстного наповнення інформації на суспільне, особисте, службове. Метою цього є намагання пояснити важливість отриманої інформації (даних, параметрів, характеристик у різних напрямках діяльності людини, а тому захист інформації – це прерогатива держави (органів влади) й окремої людини зокрема.

На сучасному етапі розвитку суспільства інформація є найважливішим ресурсом людства. Традиційні матеріальні ресурси поступово втрачають своє первісне вагове значення і на зміну їм приходять інформаційні ресурси, що з плином часу не убувають, а неухильно зростають, набуваючи нового, властивого сучасному світу прискорення та надаючи новий зміст технологіям. Інформація на четвертому рівні науково-технічної революції, що поширюється на усі галузі науки й техніки, стає дедалі більше стратегічним ресурсом суспільства, його рушійною й продуктивною силою й отримала назву інформаційної революції. Окрім того, наукове пізнання й осмислення науково-технічного прогресу відображають той факт, що інформація та знання стають новим значним чинником виробництва, його матеріально-технологічним підґрунтям для переходу людства до вищого етапу цивілізаційного прогресу – інформаційного постіндустріального суспільства [1].

Широке використання інформаційних ресурсів сучасним суспільством робить цілком закономірною і неабияк актуальною проблему захисту інформації. За інтенсивного розвитку ринку інформаційних продуктів й нових послуг у сфері комп'ютерних технологій, що розширює можливості людини сучасного світу, інформація стає повноцінним товаром, тобто має усі властивості сучасного товарного продукту і подібно іншим товарам, інформація потребує надійного захисту.

Аналіз останніх досліджень і публікацій. У новому міжнародному стандарті [2] визначено, що управління проектами виконується через процеси. Процеси, вибрані для

виконування проекту, слід систематизувати, а кожну стадію життєвого циклу проекту слід закінчувати конкретними задокументованими результатами, які необхідно регулярно переглядати під час виконання проекту, щоб виконати усі заявлені вимоги. Окрім того, в термінологічному міжнародному стандарті, що відкриває серію стандартів на системи управління інформаційною безпекою (далі – СУІБ) [3] визначено, що для реалізації СУІБ треба створити проект СУІБ, це будуть відповідно структуровані заходи, що їх провадить організація. Цікавими дослідженнями є напрацювання Домарєва В. В., Домарєва Д. В., Ромаки В. А., Козлюк І. О., Дудикевича В. Б., Гарасима Ю. Р., Гаранюка Г. І., Горяної О. Г., Чунарьової А. В., Чунарьова А. В., Шевченка С. Ю. щодо створення та впровадження СУІБ.

Постановка завдання. Створення ІТ-проектів у сфері захисту інформації залежить від сфери діяльності та сфери застосування технології. Для цього застосовують певні методи захисту, за допомогою визначених способів, засобів і прийомів та певного плану робіт можна забезпечити діяльність, щоб унеможливити спроби проникнення зловмисника, помилки персоналу, виходу з ладу окремих блоків техніки, спотворення чи несанкціонованого використання ресурсів мережі, інформації, зокрема даних, що зберігають, передають чи обробляють, а також програмні й апаратні засоби.

Виклад основного матеріалу дослідження. Кожна країна має певну державну систему захисту інформації, що передбачає, по-перше, нормативно-правовий складник системи, по-друге, нормативну базу функціонування системи, по-третє, технічну частину, що реалізує функціонування системи, по-четверте, наукову основу, що передбачає розвиток системи і, нарешті, п’яте, організаційну, що є базисом для роботи багатьох людей цієї країни, визначає їхні дії. На думку автора, будь-який проект, створений, щоб забезпечити функціонування системи в сфері захисту інформації, має насамперед відповідати вимогам щодо відповідності зазначеної системи.

Нормативно-правове регулювання забезпечення захисту інформації закріплено статтями 17, 31, 32, 34 Основного Закону України – Конституції України, а також у Законах України, Указах Президента України, постановах і розпорядженнях Кабінету Міністрів України, інших нормативно-правових актах, що регулюють сферу інформаційних відносин [4]. Вони визначають державні пріоритети, встановлюють відповідальність за порушення невід’ємних прав і свобод людини, її конституційні права та зобов’язання щодо дотримання іншими правил співмешкання і соціальності.

Нормативні документи – це значний прошарок документів, розроблений для створення нормативного регулювання діяльності в сфері захисту інформації. Насамперед це стандарти, що уніфікують певні знання, унормовують терміни; інструкції та правила, що деталізують основні положення до рівня повсякденної діяльності, подають конкретні алгоритми дій у певних ситуаціях (нормальні режими роботи й анормальні). Обмовимось, що в рамках створеної в організації (на підприємстві) системи управління інформаційною безпекою таких документів має бути достатньо, щоб упорядкувати роботу цієї організації (підприємства), забезпечивши бездоганну й працездатну Політику безпеки в цій організації (підприємстві). Такий перелік має містити документи, що їх періодично переглядають, доопрацьовують, змінюють, поновлюють, тобто виконують роботу щодо покращення системи, а документування є необхідною і відповідальною роботою системи управління.

Науковою основою сфери захисту інформації, що забезпечує розвиток та планування діяльності системи, є: криптологія, теорія прийняття рішень, інформатика, інформологія й новітня наука – інформаціологія. Ці наукові дисципліни, що їх викладають у вищих навчальних закладах, визначають майбутнє систем управління і на ці науки, наукові концепції, теорії управління покладено не лише наукове обґрунтування функціонування діяльності в сфері захисту інформації, вони, окрім того, мають працювати на випередження.

Організаційну структуру системи захисту інформації визначає [5], де вказано, що Державна служба спеціального зв’язку та захисту інформації є окремим органом виконавчої влади і має певні повноваження та структуру щодо своїх визначених функцій, регулятором у сфері захисту інформації в Україні. Організаційне забезпечення системи захисту інформації

полягає у дотриманні правил, встановлених у нормативно-правових актах і нормативних документах з технічного захисту інформації [4]. Зокрема у [6] зазначено, що організаційні заходи мають регламентувати порядок інформаційної діяльності, враховуючи норми і вимоги технічного захисту інформації для всіх періодів життєвого циклу об'єкта захисту. Цього досягають створенням комплексу адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціонування засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення технічного захисту інформації [7].

Наявність системи забезпечення захисту інформації уможливлює надійне забезпечення національної безпеки країни через забезпечення інформаційної безпеки, захисту інформації, інформаційних технологій [8]. Головне призначення цієї системи полягає у досягненні цілей національної безпеки в інформаційній сфері, а отже основною функцією даної системи є захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, забезпечення збалансованого існування інтересів особи, суспільства і держави.

За національним стандартом [9], що було розроблено на основі відомого та визнаного міжнародного стандарту ISO 9000:2008, процесний підхід базується на таких твердженнях: усі види діяльності описуються у вигляді взаємопов'язаних процесів; визначення ключових процесів; управління ресурсами як результативним процесом; більш ефективне досягнення бажаних результатів; можливість використання інформаційних технологій для своєчасного прийняття управлінських рішень. Отже, якщо будь-яка діяльність або комплекс видів діяльності, що використовують ресурси для перетворення входів на виходи, можна розглядати як процес, то для ефективного функціонування організація (підприємство) має визначити взаємопов'язані та взаємодійні процеси й ефективно управляти ними. Процес може виконуватися у різних структурних підрозділах, що спільно впливають на досягнення спільної мети (формування спільних виходів). Систематичне визначення процесів та їх взаємодії в організації, а також управління ними називають процесним підходом. Процесний підхід трактує управління як серію безпосередніх взаємопов'язаних дій. Ці дії, кожна з яких сама по собі вже є процесом, значною мірою визначають успіх діяльності організації. Вони дістали назву «управлінські функції». Кожна управлінська функція – це також процес. Отже, процес управління є поєднанням функцій планування, організування, мотивації, контролювання та регулювання. Ці п'ять первинних функцій управління поєднано з процесами комунікацій та прийняття рішень. Керівництво (лідерство) – це самостійна діяльність [10] і у даній статті цей компонент не буде розглядатись.

Щоб забезпечити правильне управління процесами, організувати взаємодію між структурними підрозділами підприємства (організації), слід забезпечувати однозначне розуміння всіма учасниками процесу їх відповідальності і повноважень, а тому треба організовувати взаємодію під час вирішення завдань чи то проблем, які охоплюють декілька структурних підрозділів організації. Як свідчить світовий досвід, найбільш прогресивним напрямком у підвищенні результативності та ефективності роботи підприємств (організацій, державних органів тощо) є системний підхід до організації діяльності, що її може бути організовано наприклад на принципах загального управління й відповідних, визнаних міжнародним суспільством, стандартах з управління [11]. Системний підхід полягає в тому, що це підхід, за якого будь-яку систему (чи менший елемент – об'єкт) розглядають як сукупність взаємозв'язаних елементів (компонентів). Для управління організації (підприємства) системний підхід полягає у координації усіх аспектів діяльності, постійному плануванні, управлінні взаємопов'язаними процесами для результативного й ефективного досягнення поставлених цілей. Система управління, побудована за такою моделлю, охоплює усі організаційні, ресурсні, методологічні і, що найбільш важливо, соціальні чинники, призводить до помітного підвищення ефективності управління, націлена на неперервний саморозвиток і удосконалення. Так системний аналіз має важливе значення в теорії управління персоналом, його методичні концепції лежать в тих дисциплінах, що стосуються

проблем прийняття рішень у відповідних науках: теорії операцій і достатньо загальній теорії управління [12]. Згідно з системним підходом керівник має розглядати організацію як сукупність взаємопов'язаних елементів, таких як: люди, структура, завдання, технологія, що їх орієнтовано на досягнення певних цілей і тісно переплетені з зовнішнім світом, тобто отримуючи із зовнішнього середовища інформацію, капітал, матеріали, трудові ресурси (це «входи» процесного підходу) у процесі діяльності (перетворення) вони перетворюються на підприємстві у продукцію чи послуги (це «виходи» процесного підходу). Якщо організація управління ефективна, то в процесі перетворення утворюється додаткова вартість. За цих умов збільшується обсяг продажу, зростають прибуток, а отже і задоволеність працівників результатами своєї праці.

У першому установчому документі, що став першоджерелом створення стандартизованих правил для сфери інформаційної безпеки [13], було наведено основні положення за якими американське відомство оборони визначало ступінь захищеності інформаційно-обчислювальних систем. У ній систематизовано наводились основні поняття, рекомендації і класифікація видів загроз безпеки інформаційних систем і методи захисту від них. У цій книзі також було наведено науково обґрунтовані норми й правила, що описують системний підхід для забезпечення безпеки інформаційних систем і їх елементів. Запропонована в цій книзі методологія по суті стала загальноприйнятою і в тій чи іншій мірі увійшла, спочатку, в міжнародні стандарти, що уніфікували й унормували вимоги до захисту інформації в комп'ютерних системах та мережах, а потім через процедуру гармонізації, увійшли в національні стандарти багатьох країн світу у сфері захисту інформації, безпеки інформаційних технологій, що їх застосовують й нині.

Висновки. Формування управління як науки, як галузі наукових досліджень частково було відгуком на потреби великого бізнесу та конкурентного середовища ринку, частково – спробою скористатися перевагами нової техніки, а частково зумовлене науковими розробками найбільш ефективних методів виконання робіт, а тому системний та процесний підходи зробили суттєвий внесок у розвиток теорії та практики управління: всі сучасні науки побудовані за принципами системного та процесного підходів. Застосування цих підходів є передумовою створення нового, єдиного і більш оптимального підходу (загальної методології) до наукового пізнання світу, щоб гарантовано отримати найбільш повне і цілісне уявлення про цей світ. Системний та процесний підходи разом з використанням комп'ютерних технологій допоможуть досліджувати складні технічні, економічні, екологічні, культурні, соціальні, політичні системи, а результатом таких досліджень стане досягнення нового рівня ефективності та продуктивності праці людей та покращення життя суспільства.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Чухно А. А. Інституціонально-інформаційна економіка. Технологічні уклади : сутність та особливості розвитку [Електронний ресурс] / А. А. Чухно // Українські підручники он-лайн. – Режим доступу : http://pidruchniki.ws/12631113/ekonomika/tehnologichni_ukladi_sutnist_osoblivosti_rozvitkua. – Дата доступу : лютий 2015. – Назва з екрану.

2. Guidance on project management : ISO 21500:2012 [Електронний ресурс]. – Режим доступу : https://www.iso.org/obp/ui/#iso:std:iso:_21500:ed-1:v1:en. – Дата доступу : січень 2015. – Назва з екрану.

3. Information technology. Security techniques. Information security management systems. Overview and vocabulary : ISO/IEC 27000:2014 [Electronic resource]. – Access mode : https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en. – Access data : January 2015. – The title of the screen.

4. Нормативно-правова база [Електронний ресурс] / Державна служба спеціального зв'язку та захисту інформації України. – Режим доступу : http://www.dstszi.gov.ua. – Дата доступу : березень 2015. – Назва з екрану.

5. Про Державну службу спеціального зв'язку та захисту інформації України [Електронний ресурс] / Закони України // Верховна Рада України. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/3475-15. – Дата доступу : лютий 2015. – Назва з екрану.

6. Захист інформації. Технічний захист інформації. Основні положення : ДСТУ 3396.0-96. – [Чинний від 1997-01-01]. – К. : Держстандарт України, 1996. – 6 с.

7. Захист інформації. Технічний захист інформації. Порядок проведення робіт : ДСТУ 3396.1-96. – [Чинний від 1997-07-01]. – К. : Держстандарт України, 1996. – 7 с.

8. Про основи національної безпеки України [Електронний ресурс] / Закони України // Верховна Рада України. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/964-15. – Дата доступу : лютий 2015. – Назва з екрану.

9. Система управління якістю. Вимоги (ISO 9001:2008, IDT) : ДСТУ ISO 9001:2009. – [Чинний від 2009-09-01]. – К. : Держспоживстандарт України, 2009. – 26 с.

10. Процесний, системний і ситуаційний підходи в управлінні [Електронний ресурс]. – Режим доступу : http://ru.osvita.ua/vnz/reports/management/14996/. – Дата доступу : січень 2015. – Назва з екрану.

11. Розробка та впровадження системи управління якістю [Електронний ресурс] / Міністерство оборони України. – Режим доступу : http://www.mil.gov.ua/index/index.php?part=quality_management_system&lang=ua. – Дата доступу : січень 2015. – Назва з екрану.

12. Основы системного подхода и их приложение к разработке территориальных автоматизированных систем управления / Под ред. Ф.И. Перегудова. – Томск : ТГУ, 1976. – 244 с.

13. Trusted Computer System Evaluation Criteria : «Orange Book». [Electronic resource] / Department of Defense. – Access mode : http://csrc.nist.gov/publications/history/dod85.pdf. – Access data : January 2015. – The title of the screen.

Стаття надійшла до редакції 12.03.2015.

REFERENCES

1. Chukhno, A.A. (2010), *Institutional and Information economy. Technology modes : the nature and of especially the development* [*Instytutsionalno-informatsiina ekonomika. Tekhnolohichni uklady : sutnist ta osoblyvosti rozvytku*], available at : http://pidruchniki.ws/12631113/ekonomika/tehnologichni_ukladi_sutnist_osoblivosti_rozvitkua (accessed 22 January 2015).

2. International Organization for Standardization (2012), ISO 21500 : 2012, *Guidance on project management*, available at : https://www.iso.org/obp/ui/#iso:std:iso:21500:ed-1:v1:en (accessed 08 January 2015).

3. International Organization for Standardization (2014), ISO/IEC 27000 : 2014, *Information technology. Security techniques. Information security management systems. Overview and vocabulary*, available at : https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en (accessed 03 February 2015).

4. Legislature, *State Service for Special Communications and Information Protection of Ukraine*, available at : http://www.dstszi.gov.ua (accessed 01 March 2015).

5. O*n State Service of Special Communication and Information Security of Ukraine*, available at : http://zakon3.rada.gov.ua/laws/show/3475-15 (accessed 21 February 2015).

6. State Committee for Standardization (1996), DSTU 3396.0-96, *Data protection. Technical protection of information. The main provisions* [*Zakhyst informatsii. Tekhnichnyi zakhyst informatsii. Osnovni polozhennia*], Kiev, 6 p.

7. State Committee for Standardization (1996), DSTU 3396.1-96, *Data protection. Technical protection of information. The conduct of work* [*Zakhyst informatsii. Tekhnichnyi zakhyst informatsii. Poriadok provedennia robit*], Kiev, 7 p.

8. *On National Security of Ukraine*, available at : http://zakon5.rada.gov.ua/laws/show/964-15 (accessed 21 February 2015).

9. State Committee for Standardization (2009), DSTU ISO 9001-2008, *Quality Management System.* Requirements [*Systema upravlinnia yakistiu. Vymohy*], Kiev, 26 p.

10. *The process, system and situational approaches in management* [*Protsesnyi, systemnyi i sytuatsiinyi pidkhody v upravlinni*], available at : http://ru.osvita.ua/vnz/reports/management/14996/ (accessed 11 January 2015).

Development and implementation of quality management [*Rozrobka ta vprovadzhennia systemy upravlinnia yakistiu*], available at : http://www.mil.gov.ua/index/index.php?part=quality_management_system&lang=ua (accessed 17 January 2015).

11. Peregudov, F.I. (1976), *Bases of system approach in their applications to the appendix of territorial automated control systems*, TGU, Tomsk, 244 p.

12. *Trusted Computer System Evaluation Criteria : «Orange Book»*, available at : http://csrc.nist.gov/publications/history/dod85.pdf (accessed 27 January 2015).

ЮЛІЯ КОЖЕДУБ

ПРО ОСОБЕННОСТИ СИСТЕМНОГО И ПРОЦЕСНОГО ПОДХОДОВ ПРИ СОЗДАНИИ ИТ-ПРОЕКТОВ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ

Наводится обобщенное теоретическое исследование известных научных подходов к созданию ИТ-проектов в сфере защиты информации, которые применяют для систем защиты информации. Исследование также основывалось на международных документах, которые применяют специалисты в сфере защиты информации. Общепризнанная международная практика стандартизации и научные подходы, применяемые при создании ИТ-проектов в сфере защиты информации являются главными факторами, которые отвечают требованиям защищенности жизненно важных интересов человека и гражданина, общества и государства, при которой обеспечиваются стабильное развитие общества.

Ключевые слова: защита информации, информация, ИТ-проекты, международные стандарты, процессный подход, системный подход.

YULIYA KOZHEDUB

ABOUT FEATURES OF THE SYSTEM AND PROCESS APPROACHES CREATING IT PROJECTS IN THE FIELD OF INFORMATION SECURITY

The article presents a summary theoretical study known scientific approaches to the creation of IT projects in the field of information security, which they introduce for information security systems. The study also was based on international instruments that they used experts in the field of information security. Generally accepted international practice of standardization and scientific approaches used during the creation of IT projects in the field of information security are the main factors that meet the requirements for protection of vital interests of man and citizen, society and the state, which provided for the sustainable development of society.

Keywords: information security, information, IT projects, international standards, process approach, system approach.

Юлія Василівна Кожедуб, кандидат технічних наук, доцент, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут», Київ, Україна.

E-mail : JuliaKozhedub@email.ua

Юлия Васильевна Кожедуб, кандидат технических наук, доцент, Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт», Киев, Украина.

Yuliya Kozhedub, candidate of technical sciences, assossiate professor, Institute of special communication and information security of National technical university of Ukraine «Kyiv polytechnic institute», Kyiv, Ukraine.