classification of social networking services and the simultaneous use of several networking services by the same actor. The contributor suggests the definitions for the “social networking services” term and the “actor” term. The contribution is about analyzing the social networking services and classifying them hierarchically. Considered a wide class of assets to meet the needs of actors in communication, content, expression, socialization and so on. These types of social networking services provide integration of different types of content sharing and coordination of interaction between the actors themselves. The classification approach suggested in the contribution has the certain advantages of its consistency, capacity and accuracy. It specifies interactions between the actors of virtual communities thus enabling an efficient system of national cybersecurity. The results will be used to formalize approaches to develop control actions on the virtual community.

Keywords: social networking services, actors, threat, hierarchy classification, national cybersecutity.

Катерина Валеріївна Молодецька, кандидат технічних наук, доцент, доцент кафедри комп’ютерних технологій і моделювання систем, Житомирський національний агроекологічний університет, Житомир, Україна.
E-mail: kmolodetska@gmail.com.

Катерина Валерьевна Молодецкая, кандидат технических наук, доцент, доцент кафедры компьютерных технологий и моделирования систем, Житомирский национальный агроэкологический университет, Житомир, Украина.

Kateryna Molodetska, candidate of technical sciences, assistant professor, assistant professor at the information technology and simulation academic department, Zhytomyr National Agro-Ecological University, Zhytomyr, Ukraine.

УДК 006.057/.032

ЮЛІЯ КОЖЕДУБ

СУЧАСНІ АСПЕКТИ ОНОВЛЕННЯ МІЖНАРОДНИХ СТАНДАРТІВ СЕРІЇ ISO/IEC 27000

У статті наведено та проаналізовано нові відомості щодо сучасних аспектів стандартизації методів безпеки інформаційних технологій, висвітлено роботу експертів технічних комітетів стандартизації зі створення й оновлення міжнародних стандартів на системи управління інформаційною безпекою, подано приклади, озвучені експертами стандартизації стосовно технічних пропозицій та методів розв’язання проблем щодо інформаційної безпеки за допомогою зводів практичних правил, реалізованих у серії міжнародних стандартів. У статті з’ясовано, що першопричиною кропіткої роботи технічних експертів стандартизації над оновленням міжнародних стандартів серії ISO/IEC 27000 стало оновлення основоположних стандартів серії ISO/IEC 9000. Результатом цієї праці було приведення у відповідність положень стандартів серії ISO/IEC 27000 та напрацювання спеціалістів з методів безпеки інформаційних технологій до фундаментальних основ систем управління, принципи яких закладено й озвучено новітніми стандартами.

Ключові слова: стандарти, стандартизація, інформаційні технології, методи безпеки інформаційних технологій, системи управління інформаційною безпекою, технічний комітет.

Постановка проблеми. Користувачам міжнародних стандартів відомо, що над створенням стандарту працюють багато експертів – спеціалістів, фахівців, знавців у даній

сфері діяльності та стандартизації. Ці експерти представлені багатьма країнами світу, де створено та функціонують технічні комітети стандартизації. Робота над стандартами відбувається планово й за правилами, запропонованими міжнародними організаціями, що представлені ISO, IEC та ITU. Збір, оброблення, узагальнення пропозицій, листування, проведення нарад і зустрічей, на яких опрацьовують та узагальнюють висновки з даних зауважень до технічних рішень, виявлених проблем, що потім врешті-решт стають положеннями стандарту. Одним реченням можна пояснити роботу експертів-стандартизаторів, але не відобразити масштаб проведеної роботи про сотні пунктів пропозицій, тисячі листів, отриманих від експертів з понад 150 країн світу, що є членами Міжнародної організації зі стандартизації, з висновками, що містять погодження чи заперечення, або нову покращену пропозицію на надіслану позицію положення стандарту.

Аналіз останніх досліджень і публікацій. Державна служба спеціального зв'язку та захисту інформації України (далі – Держспецзв'язок) разом з командою CERT-UA і спільно з Київським відділенням міжнародної організації ISACA проводять дослідження застосовності стандарту ISO/IEC 27001:2013 для впровадження систем управління інформаційною безпекою органів державної влади та об'єктів критичної інфраструктури. Дорученням віце-прем'єр-міністра України від 29 квітня 2015 р., центральним органам виконавчої влади запропоновано взяти участь у опитуванні щодо наявних політик та практик з інформаційної безпеки [1].

На виконання розпорядження Уряду від 05.11.2014 р. № 1135-р "Про затвердження Плану заходів щодо захисту державних інформаційних ресурсів", 7 квітня 2015 року Держспецзв'язок звернувся до Кабінету Міністрів України з пропозицією впровадження системного підходу до управління інформаційною безпекою державних органів шляхом побудови загальнодержавної системи управління інформаційною безпекою.

У своєму листі Держспецзв'язок зазначає, що системи управління інформаційною безпекою, створені за стандартом ISO/IEC 27001:2013, впроваджені і успішно функціонують на деяких об'єктах критичної інформаційної інфраструктури України, зокрема, у фінансовому секторі, газовидобувній галузі та енергетичному комплексі. Руку допомоги на цьому шляху пропонує Грузія, що також почала впровадження стандарту ISO/IEC 27001:2013 в органах державної влади й, яка вже успішно пройшла сертифікаційний аудит на відповідність міжнародним стандартам системи управління інформаційної безпеки.

Постановка завдання. Світовий досвід та досвід європейських країн свідчить, що системи управління інформаційною безпекою дають змогу забезпечити конфіденційність, цілісність і доступність інформації у них, провадити оцінку інформаційних ризиків та контролювати стан захищеності системи, оцінювати та впевнюватись у тому, що всі процеси на підприємстві/установі відповідають вимогам із забезпечення безпеки інформації. Впровадження системи управління інформаційною безпекою, які відповідають міжнародному стандарту ISO/IEC 27001:2013, дасть змогу суттєво зменшити втрати від кіберзагроз в органах державної влади і на об'єктах критичної інформаційної інфраструктури нашої держави.

Метою статті є доведення сучасних аспектів оновлення цілої низки міжнародних стандартів, зокрема, й міжнародних стандартів серії ISO/IEC 27000, що відбулось через змінення основних фундаментальних положень, викладених у міжнародних стандартах серії ISO/IEC 9000, і це стало рушійною силою для їх оновлення. Ці положення – "три кити" систем управління, це: процесний підхід, цикл PDCA та мислення на основі ризиків, відомі давно фахівцям з систем управління, проте вони набули нової сили, отримали продовження та поширення на нові сфери діяльності людей.

Виклад основного матеріалу дослідження. Фахівців з систем управління інформаційної безпеки не дивує той факт, що групу експертів, яка розробляє міжнародні стандарти з методів безпеки інформаційних технологій, нагороджено премією Лоуренса Д. Єйчера за видатні досягнення в технічній роботі [2]. Премію було оголошено на 38-й Генеральній Асамблеї ISO, що проходила в серпні 2015 року в Сеулі, Південна Корея. За словами президента ISO доктора Чжан Сяогана, спільний технічний комітет ISO/IEC JTC1 "Інформаційні технології", підкомітет SC 27 "Методи безпеки ІТ", було вибрано "провідними світовими експертами, міжнародного рівня стандартами і довершеністю щодо просування та консультацій".

Премію Лідерство було створено в 2002 році як данину покійному Генеральному секретарю Міжнародної організації зі стандартизації Лоуренсу Д. Єйчеру, який очолював з 1986 по 2002 рік цю організацію. Її присуджують, щоб визнати довершеність і інновації у технічній роботі технічних комітетів та/чи підкомітетів.

Під час церемонії нагородження виконуючий обов'язки Генерального секретаря ISO Кевін Маккінлі сказав, що ISO/IEC 27001 став спільною мовою для організацій, щоб захистити свою інформацію і на сьогодні він є провідним стандартом для міжнародної сертифікації у сфері інформаційної безпеки.

Пан Маккінлі високо оцінив зусилля, що були зроблені спільним технічним комітетом ISO/IEC JTC1 щодо забезпечення міцних зв'язків із зацікавленими сторонами в сфері інформаційних технологій, зокрема під час проведення семінарів для місцевих підприємств, під час засідань її робочих груп, обміну й отримання зворотного зв'язку про майбутні потреби в галузі стандартизації. Ця робота також полягала у формуванні зв'язків з іншими організаціями і загалом з промисловістю, що забезпечує наявність відповідного провідного світового досвіду для систем управління інформаційною безпекою.

Слід зазначити, що це вдруге, коли спільний технічний комітет ISO/IEC JTC1 отримав нагороду, що особливо підкреслює важливість спільної роботи зі створення сучасних, комплексних й випереджувальних стандартів.

Наразі підкомітет SC 27 "Методи безпеки IT" веде DIN, Німеччина, очолює його Вальтер Фамий, секретарем є Кристина Пассія. Під час нагородження Голова підкомітету SC 27 Вальтер Фамий подякував більше ніж 70 членам ISO з усіх п'яти континентів, які підтримували роботу підкомітету, багато з яких присвятили свій час, надали ресурсів, призначили експертів для участі в процесі розвитку міжнародних стандартів. Він зазначив, що ця зростаюча підтримка відображає зростаючу потребу в стандартах з інформаційної безпеки, оскільки "ми переносимо більшу частину людської діяльності з фізичного світу в віртуальний простір".

Професор Едвард Хамфріс, керівник робочої групи, відповідальної за стандарти системи управління інформаційною безпекою ISO, підкреслює: "З метою забезпечення безпеки в сучасному цифровому полі, всі організації, незалежно від розміру, повинні ввести в дію систему управління як відправну точку щодо управління кібер-ризиками. ISO/IEC 27001 було розроблено, щоб допомогти організаціям зробити саме це. Міжнародний стандарт – це "спільна мова", коли йдеться про оцінювання, оброблення й управління інформаційними ризиками". Професор Едвард Хамфріс, як і один з очільників ISO пан Кевін Маккінлі, так саме наголошує, що міжнародні стандарти серії ISO/IEC 27000 є спільною мовою для фахівців щодо методів захисту інформаційних технологій. Зокрема, це стосується й управління кібербезпекою.

Кібер-атаки є одними з найбільших чинників ризику з якими організація може зіткнутися сьогодні. Наявність стандартів і систем захисту в організації, щоб зберегти інформацію в безпеці, ніколи не була такою важливою, ніж в сучасному цифровому світі. Саме тому серія міжнародних стандартів ISO/IEC 27000 щодо методів безпеки інформаційних технологій постійно оновлюється для забезпечення організацій доданою вартістю й впевненістю в собі [3].

У глобальному дослідженні, проведеному ISACA в 129 країнах, лише 38 % респондентів вважають, що вони були готові до кібер-атаки, навіть незважаючи на те, що 83 % опитаних вважають, що їх інформаційні активи входять до числа трьох найбільших загроз, що стоять перед організаціями сьогодні, зважаючи на значну кількість особистої і конфіденційної інформації, що її оброблюють в електронному вигляді, а тому багато поставлено на карту, якщо ця інформація підпаде під загрозу.

Як організації можуть виявляти та запобігати кібер-атакам у їх мережі, системах і додатках? На це питання допоможе відповісти ISO/IEC 27039. Краща практика показує, що вони повинні бути в змозі знати коли, як і що відбувається під час вторгнення в їх мережі,

системи або додатки. Вони також повинні бути готові визначити, яку вразливість було використано і яких елементів контролю має бути реалізовано, щоб унеможливити подібні вторгнення в майбутньому. Один із способів зробити це через системи виявлення і запобігання вторгненням (англ. Intrusion Detection and Prevention Systems (IDPS)).

Міжнародний стандарт ISO/IEC 27039 надає рекомендації з підготовки та розгортання систем виявлення і запобігання вторгненням, що охоплюють такі важливі аспекти, як вибір, розгортання та експлуатацію. Стандарт особливо корисний в умовах сучасного ринку, де є багато доступних комерційних і відкритих джерел з продуктами систем виявлення і запобігання вторгненням, і, послуг, заснованих на різних технологіях і підходах. ISO/IEC 27039 допоможе організаціям протягом усього процесу.

Іншим прикладом, що стандартизація миттєво відповідає викликам сучасних інформаційних технологій є новий Звід практичних правил для управління інформаційною безпекою для хмарних послуг ISO/IEC 27017, який щойно було опубліковано.

“Хмара” є одним з найбільш широко використовуваних інновацій в сучасному мінливому світі комерції та бізнесу. Оскільки ”хмара” – це швидко поширювана й надприбуткова послуга, то користувачі вимагають гарантій того, що дані зберігаються й обробляються в ”хмарі” безпечно. Через саму свою природу, ринок хмарних послуг є глобальним, їх постачальники розосереджено по широким географічним районам, а дані зазвичай передаються через національні кордони. Міжнародна настанова щодо хмарних послуг ISO/IEC 27017 є ключовою подією.

За словами Сатору Ямасакі, який був одним з редакторів, що працював над стандартом, ISO/IEC 27017 допоможе постачальникам послуг дійти загального порозуміння зі своїми клієнтами щодо належного контролю безпеки і вона є для них настановою щодо застосування. Цей міжнародний стандарт для управління безпекою хмари сприятиме розвитку і розширенню безпечних хмарних обчислювальних систем.

Ці нові керівні принципи є результатом спільної ініціативи головних розробників в світі міжнародних стандартів – IEC, ISO та ITU, щоб гарантувати максимальну ступінь охоплення підприємств і організацій в світі. Слід пояснити, що стандарти означені як ”ISO/IEC”, розроблено у співдружності двох міжнародних організацій, що діють на основі Віденської домовленості про співпрацю у всіх важливих сферах діяльності, де стандартизація сприймається як високий ступінь організації, контролю й управління. Приєднання Міжнародного Союзу Телекомунікацій (ITU) означає високу зацікавленість в означеній роботі щодо стандартизації вимог до безпечності хмарних технологій.

Наступним прикладом реалізації стандартизованих положень, що поєднує систему управління інформаційною безпекою з системою управління послугами є міжнародний стандарт ISO/IEC 27013, оскільки усе більше організацій вибирають об’єднання системи управління інформаційною безпекою за ISO/IEC 27001 з системою управління послугами за ISO/IEC 20000-1. Така інтегрована система буде означати, що організація може ефективно управляти якістю своїх послуг, що є зворотний зв’язок між клієнтами і є інструменти вирішення проблем, зберігаючи за цього інформацію в безпеці.

Міжнародний стандарт ISO/IEC 27013 пропонує системний підхід для полегшення інтеграції системи управління інформаційною безпекою з системою управління послугами, що призводить до зниження витрат на реалізацію і уникнення дублювання зусиль, як, наприклад, під час аудитування можна провадити лише один аудит, замість двох, що його необхідно виконати для сертифікації системи.

Коли організація ділиться інформацією з іншою організацією, як вони можуть бути впевнені, що їх передаванні чи пересиланні дані будуть в цілості та захищеності? Міжнародний стандарт ISO/IEC 27010 є конкретним секторним доповненням (основними наскрізними й рамковими стандартами є: ISO/IEC 27000, що є оглядовим й термінологічним, ISO/IEC 27001, де подано вимоги до системи управління інформаційною безпекою та

ISO/IEC 27002, який практично пояснює як може бути упроваджено систему управління інформаційною безпекою) відповідно до серії ISO/IEC 27000 і є тим інструментом, який спрямовує ініціацію, впровадження, підтримання та вдосконалення інформаційної безпеки в міжорганізаційні та міжгалузеві зв'язки організацій. Цей стандарт охоплює загальні принципи про те, як виконати ці вимоги, використовуючи встановлені повідомлення та інші технічні методи. Цей стандарт, як очікується, стимулюватиме зростання глобальних спільнот інформаційного обміну.

Доктор Майк Неш, редактор ISO/IEC 27010, пояснює: "ISO/IEC 27010 в основному адаптує і застосовує ISO/IEC 27001 та ISO/IEC 27002 для взаємозв'язку між різними організаціями. Маючи такий стандарт на місці, він надає організації впевненості в тому, що інформація, якою вона поділилася з іншою організацією, не буде ненавмисно розкрита". Стандарт має особливе значення для захисту важливої національної інфраструктури, де надійний обмін конфіденційною інформацією має першорядне значення. Цей стандарт також буде широко використовуватись командами реагування на інциденти інформаційної безпеки, більш відомими в світі як CERT.

На завершення слід сказати про аудити й сертифікацію систем управління інформаційною безпекою за ISO/IEC 27001, тому що все більше і більше організацій звертаються до сертифікаційних аудитів третьою стороною, щоб продемонструвати, що вони мають у себе на місці надійну систему управління інформаційною безпекою, що відповідає вимогам основоположного рамкового стандарту ISO/IEC 27001. Міжнародний стандарт ISO/IEC 27006 встановлює вимоги до органів з сертифікації і реєстраційних органів щодо акредитації, і у такий спосіб вони можуть запропонувати послуги з сертифікації за ISO/IEC 27001.

"ISO/IEC 27006 є еталоном для акредитації органів з сертифікації, які пропонують послуги за ISO/IEC 27001", пояснює професор Хамфріс, додавши: "Це важливо, оскільки акредитація органів з сертифікації забезпечує додаткову впевненість в процесі аудиту і достовірності, що виданий сертифікат є нагородою".

Згідно зі звітом "ISO Survey 2014" [4-6] загальна кількість виданих сертифікатів на системи управління інформаційною безпекою у 2014 році становить 23792 шт., у цьому самому році Україна мала 9 сертифікатів. Найбільше серед європейських країн має Італія – 970 сертифікатів, а лідером у світі є Японія – вражаючі 7181 сертифікатів. Звіт, поданий ISO, відображає статистичні дані починаючи з кінця 2006 року по 2014 рік не лише на сертифікати на системи управління інформаційною безпекою, але і на інші системи управління, що їх застосовано у різних галузях промисловості різних країн усіх континентів.

Висновки. Підсумовуючи зазначене вище, скажемо, що врахування змін, внесених у методологію міжнародних стандартів на системи управління, призвело до технічного перегляду, коригування, змінення положень міжнародних стандартів серії ISO/IEC 27000. Окрім того, три фундаментальні принципи: процесний підхід в поєднанні з циклом PDCA і мисленням, основаним на ризику – стали каркасом, розробленим Міжнародною організацією зі стандартизації, що дають змогу організаціям, підприємствам, установам, фірмам створити, впровадити, використовувати, узгодити або інтегрувати свою систему управління з вимогами інших стандартів на системи управління. Перегляд стандартів пов'язано з подальшим поширенням зокрема й процесного підходу на ширші сфери життя людей відповідно до структури стандартів верхнього рівня (*High Level Structure standards*) за такими напрямками: якість, безпека та безпечність, загальне керівництво, навколишнє середовище та енергетика, промисловість, послуги, інформаційні технології. Багаторічне використання міжнародних стандартів на системи управління та застосування їх у практику повсякденного життя дало змогу відкинути зайве і дійти такого простого "трикутника": процесний підхід – це основа основ; цикл PDCA або цикл Шухарта-Демінга з чотирма простими діями, але це прагнення до досконалості, постійне поліпшення, наче "філософія правильності"; мислення, основане на

ризиках, ризики ”введені”, ”вбудовані в стандарти”, тому що ризики є невідворотними від будь-якої діяльності людини, її життя і, можливо, її змістом.

Широке коло зацікавлених сторін приймають участь у створенні стандартів. Досвід, накопичений спеціалістами акумульовано у високоінтелектуальному продукті – міжнародний стандарт, що слугує багатьом як еталон. Процедура консенсусу, основана на досягненні порозуміння у проблемних й спірних питаннях, що її відпрацьовано багаторічною практикою, є запорукою успіху застосування міжнародних стандартів у сферах промисловості та діяльності людини, зокрема у сфері забезпечення безпеки інформаційних технологій в усьому світі. Україна вже має накопичений досвід застосування систем управління інформаційною безпекою й продовжує цей шлях.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] “Держспецзв’язок пропонує впровадити загальнодержавну систему управління інформаційною безпекою”. [Електронний ресурс]. Доступно: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=129963&cat_id=119123. Дата звернення: Січ., 5, 2016.

[2] K. Bird, “IT security experts win technical excellence award”. [Online]. Available: http://www.iso.org/iso/home/news_index/news_archive/news.htm?Refid=Ref2005. Accessed on: Dec., 21, 2015.

[3] M. Lazarte, “Security toolbox protects organizations from cyber-attacks”. [Online]. Available: http://www.iso.org/iso/home/news_index/news_archive/news.htm?Refid=Ref2032. Accessed on: Dec., 21, 2015.

[4] “ISO Survey 2014”. [Online]. Available: http://www.iso.org/iso/iso_survey_executive-summary.pdf?v2014. Accessed on: Dec., 7, 2015.

[5] International Organization for Standardization. 2008. *ISO/TC 176/SC 2/N 544R3, ISO 9000 Introduction and Support Package: Guidance on the Concept and Use of the Process Approach for management systems*. [Online]. Available: http://www.iso.org. Accessed on: Jan., 15, 2016.

[6] International Organization for Standardization. *ISO/FDIS 9001:2015 (E), Quality management systems. Requirements*. [Online]. Available: http://www.afnor.fr. Accessed on: Jan., 15, 2016.

Стаття надійшла до редакції 24 лютого 2016 року.

REFERENCES

[1] “State Service of Special Communication and Protection proposes to implement a national system of information security management”. [Online]. Available: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=129963&cat_id=119123. Accessed on: Jan., 5, 2016.

[2] K. Bird, “IT security experts win technical excellence award”. [Online]. Available: http://www.iso.org/iso/home/news_index/news_archive/news.htm?Refid=Ref2005. Accessed on: Dec., 21, 2015.

[3] M. Lazarte, “Security toolbox protects organizations from cyber-attacks”. [Online]. Available: http://www.iso.org/iso/home/news_index/news_archive/news.htm?Refid=Ref2032. Accessed on: Dec., 21, 2015.

[4] “ISO Survey 2014”. [Online]. Available: http://www.iso.org/iso/iso_survey_executive-summary.pdf?v2014. Accessed on: Dec., 7, 2015.

[5] International Organization for Standardization. 2008. *ISO/TC 176/SC 2/N 544R3, ISO 9000, Introduction and Support Package: Guidance on the Concept and Use of the Process Approach for management systems*. [Online]. Available: http://www.iso.org. Accessed on: Jan., 15, 2016.

[6] International Organization for Standardization. 2015. *ISO/FDIS 9001, Quality management systems. Requirements*. [Online]. Available: http://www.afnor.fr. Accessed on: Jan., 15, 2016.

ЮЛИЯ КОЖЕДУБ

СОВРЕМЕННЫЕ АСПЕКТЫ ОБНОВЛЕНИЯ МЕЖДУНАРОДНЫХ СТАНДАРТОВ СЕРИИ ISO/IEC 27000

В статье приведены и проанализированы новые сведения о современных аспектах стандартизации методов безопасности информационных технологий, освещена работа экспертов технических комитетов стандартизации по созданию и обновлению международных стандартов на системы управления информационной безопасностью, подано примеры, озвученные экспертами стандартизации о технических предложениях и методах решения проблем по информационной безопасности с помощью сводов практических правил, реализованных в серии международных стандартов. В статье установлено, что первопричиной кропотливой работы технических экспертов стандартизации над обновлением международных стандартов серии ISO/IEC 27000 было обновление основных стандартов серии ISO/IEC 9000. Результатом этой работы стало приведение в соответствие положений стандартов серии ISO/IEC 27000 и наработка специалистов по методам безопасности информационных технологий с фундаментальными основами систем управления, принципы которых заложены и озвучены новейшими стандартами.

Ключевые слова: стандарты, стандартизация, информационные технологии, методы безопасности информационных технологий, системы управления информационной безопасностью, технический комитет.

YULIIA KOZHEDUB

MODERN ASPECTS OF UPDATING INTERNATIONAL STANDARDS OF SERIES ISO/IEC 27000

The paper presents and analyzes new information about the modern aspects of standardization of information technology security techniques, covered the work of experts of technical standardization committees for the creation and updating of international standards on information security management system, sets an example, experts talk about the standardizing technical proposals and methods for solving problems in information security with help of years of practice, implemented in a series of international standards, found that the root cause of hard work Standardization Technical Experts on updating ISO/IEC 27000 was to update ISO/IEC 9000. This work resulted in harmonizing the provisions of standards ISO/IEC 27000 series and the new work experts on information technology security techniques with the fundamentals of management systems, which principles are laid and announced by the latest standards. These principles are known and constitute the methodological basis of international standards on the management system, namely, the process approach, the PDCA cycle and thinking on the risk based. The provisions of the revised standards and the standards that will be published by the ISO in the future, lies in the fact that the process approach – is the systematic identification and management processes, as well as their interaction in order to achieve the desired results in accordance with established policies and strategic direction organization. Process control and system as a whole can be achieved using the PDCA cycle with the general emphasis thinking on the risk based, aimed at seizing opportunities and prevent unwanted results.

Keywords: standards, standardization, information technology, information technology security methods, information security management systems, the technical committee.

Юлія Василівна Кожедуб, кандидат технічних наук, доцент кафедри управління, Державний заклад ”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 кафедры управления, Государственное учреждение ”Институт специальной связи и защиты информации Национального технического университета Украины ”Киевский политехнический институт”, Киев, Украина.

Yuliia Kozhedub, candidate of technical sciences, associate professor at the management academic department, State institution ”Institute of special communication and information protection of National technical university of Ukraine ”Kyiv polytechnic institute”, Kyiv, Ukraine.