**Григорій Олексійович Кравцов,** кандидат технічних наук, докторант, Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України, Київ, Україна.

**Ігор Васильович Коцюба,** аспірант, Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України, Київ, Україна.

**Владимир Владимирович Мохор,** доктор технических наук, профессор, заведующий кафедрой, Государственное учреждение «Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт», Киев, Украина.

**Григорий Алексеевич Кравцов,** кандидат технических наук, докторант, Институт проблем моделирования в энергетике им. Г. Е. Пухова Национальной академии наук Украины, Киев, Украина.

**Игорь Васильевич Коцюба,** аспирант, Институт проблем моделирования в энергетике им. Г. Е. Пухова Национальной академии наук Украины, Киев, Украина.

УДК 004.91:65.012.45

ЮЛІЯ КОЖЕДУБ

# СТВОРЕННЯ ДОКУМЕНТАЦІЇ ДЛЯ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Запропоновано нову систему створення документації для систем управління інформаційною безпекою, що відображає особливості, притаманні системам управління інформаційної безпеки організації. Відображено аспекти, пов’язані з персоналом та їх поводженням з документами, що стосуються інформаційної безпеки підприємств та/чи організацій.

**Ключові слова:** документація, міжнародні стандарти, системи управління, управління організацією, персонал.

**Постановка проблеми.** Зважаючи на широке поширення систем управління на різні сфери життя й діяльності людини, і відносячи себе до шанувальників вище зазначених систем, висвітлюється власний погляд на означене питання.

Розроблення документів для потреб систем управління, зокрема для систем управління інформаційною безпекою, є важливе, якщо не найголовніше, питання функціонування організації і отримання прибутків, сталого його розвитку й безперервності бізнес-процесів.

Слід завжди пам’ятати, що усі дії персоналу у певній організації мають бути задокументовані. Їх записано у численній низці документів, що регламентують роботу як окремої людини (посадової особи), так і усієї організації, не забуваючи про проміжні документи, що стосуються роботи відділу, сектору, департаменту тощо. В такому разі унеможливлюються аврали, збої в роботі, термінові усунення неполадок на висхідному етапі, затримки у виконанні плану реалізації або зриви у постачанні продукції чи наданні послуг. Зрозуміло, що за відповідного розумного планування й виконання дій персонал зможе постійно звертатись до цих документів, де детально й реально відображено певні процедурні

дії щодо виконання службових чи функційних обов'язків. Особливо це є важливим для щойно узятих на роботу працівників, які приступають до виконання своїх обов'язків. Ось тому розроблення документації це тривалий й творчий процес до якого залучаються усі (наголошуємо на цьому) працівники персоналу, остаточно завершених редакцій таких документів зазвичай небагато, оскільки після аудитування значну кількість документів треба перевірити й відкоригувати.

**Аналіз останніх публікацій.** Означена тематика широко представлена відомими авторами, такими як: Поліщук Н. М., Якимюк Ю. П., Лазько І. В., Качанов С. О., Сергієнко М. Г., Сморжанюк Т. П., Шрам Т. В., Рогальський Ф. Б., Домарєв В. В., Домарєв Д. В., Слободянюк Н. Ю., Палеха Ю. І., які мають значні напрацювання, про що свідчать їх наукові роботи, підручники та посібники щодо управлінського документування та/чи документального забезпечення управління, проте зовсім незначною є частка робіт присвячена створенню документації для систем управління.

**Формулювання цілей статті, постановка завдання.** Результатом документування є документ, який фіксує на матеріальному носієві інформацію з встановленими реквізитами, що дають змогу її ідентифікувати в подальшому. Зазвичай документ це складний об'єкт, що відображає цілісність інформації і матеріального носія. З'ясувати його суть – це задача, яку можна вирішити за допомогою системного підходу – методологічного напрямку в науці, що має на меті розроблення інструментів, засобів, методів дослідження складно організованих об'єктів – систем. Документ, як система, має значну кількість закономірно пов'язаних одне з одним елементів і частин, і це є цілісним утворенням. Чим більше таких елементів, що функційно взаємопов'язані й взаємодіють між собою, тим є складнішою система. Про це йдетиметься у цій статті. Є багато запропонованих методик для управління документами протягом усього їхнього життєвого циклу, що традиційно застосовувались на підприємствах та організаціях. Наприклад, міжнародні стандарти серії IEC 82045 Document management (Управління документами) Міжнародної електротехнічної комісії або ISO 16016 Technical product documentation (Технічна документація на продукцію), розроблений Міжнародною організацією зі стандартизації, або ISO/TR 10013 Guidelines for quality management system documentation (Настанови щодо розроблення документації системи управління якістю), що конкретно застосовна до систем управління. Проте особливі вимоги щодо забезпечення безпеки інформації є надзвичайно важливими і потребують більшої уваги з боку розробників такої документації. Власне, стаття є пропозицією для менеджерів з систем управління інформаційною безпекою щодо створення, впровадження та покращення діяльності роботи організації/підприємства, де застосовують заходи безпеки до інформаційних активів.

**Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів.** Звичайно відомо, що персонал організації це компетентні, професійно підготовлені люди, що мають відповідну освіту й фах, постійно набувають досвіду й займаються самоосвітою, яким і не потрібні інструкції за якими вони виконують свою діяльність. За таких умов можна обмежити до необхідного мінімуму систему документації для системи управління, і водночас, вимоги до компетентності персоналу збільшуються, зростають професійний контент, як то знання іноземних мов і суміжних спеціальностей, високий рівень юридичної й економічної підготовленості й постійна перепідготовка, що адаптує до сучасних умов ведення бізнесу. Ми хочемо також добавити, що окрім професійних навичок сучасний світ потребує наявності загальнолюдяних якостей у працівників організації й здатності працювати в колективі (відсутність індивідуалізму). Розуміючи, що це є спірним питанням, викладення нашої думки буде окремою статтею і на цьому обмежиться.

Подальші дії мають бути такими [1, 2]: треба проаналізувати наявні документи, що відтворюють (описують, деталізують, пропонують оптимальний шлях реалізації) виробничі процеси, і, якщо вони є застарілими, тобто такими, що вже не відповідають вимогам споживача, замовника (а це відомо з опитування й проміжного контролю, що його має бути проведено, щоб досягнути поставлених цілей), то треба їх допрацювати або скасувати такі. Таке описування можна узяти з інших документів, що здавалось й не мають відношення до

системи управління, проте свідчитиме про системний підхід до управління (наприклад, технологічний регламент, технічні умови тощо). Якщо ж документи відповідають вимогам і їх актуалізовано (перевірено й підтверджено їх дієвість), то їх треба максимально використовувати у повсякденній діяльності.

Наші рекомендації є такими: описувати виробничі процеси в документах слід з мінімально необхідними подробицями, звертаючи увагу на рівень підготовленості персоналу.

Документи розпочинають створювати подаючи документальний й формалізований опис виробничих процесів, який за потреби можна (найкраще, треба) оптимізувати. Такі дії щодо оптимізації можуть бути закладені у самій політиці, як намагання постійного поліпшування, щоб досягнути результативності й ефективності у діяльності організації.

Розроблена і така, що функціонує документація є конче необхідною для успішного управління організації і додає їй цінності, оскільки документація уможливлює поширення бізнес намірів і відповідає за узгодженість дій. Її застосування створює передумови для досягнення відповідності вимогам партнерів, споживачів чи замовника, організацію належної підготовленості персоналу, повторюваності дій і простежуваності подій, забезпечення об’єктивних результатів щодо досяжності поставлених цілей, оцінювання результативності й ефективності, постійної застосовності системи управління до змінюваних умов ведення сучасного бізнесу.

Зрозумілою є така вимога, що кожна організація сама визначає об’єм її документації і у який спосіб її потрібно поширювати: електронною поштою чи на паперовому носії. Звичайно, це залежить від виду діяльності, усталених практик, установлених правил, кількості персоналу, складності і форми самої організації (наявність скажімо філій, дочірніх компаній, географічно віддалених офісів), вимог партнерів, замовників чи споживачів, відповідних обов’язкових вимог (будівельних, санітарних, юридичних, технічних, технологічних, тобто таких, що законодавчо встановлені в цій країні).

Отже, крім засадничих основ, викладених нами вище, потрібно також урегулювати таке питання як: копіювання документів системи управління. Треба створити правила копіювання, це є важливим для певних документів, що не можуть бути доступними для кожного працівника, адже можлива й саме така ситуація, ось тоді потрібно копіювати виокремлені частини документів, щоб унеможливити отримання й відтворення конкурентами повної інформації про діяльність організації. Для пришвидшення та полегшення новоприбулим працівникам роботи пропонуємо видавати і перевидавати (після оновлення) окремі збірники документів, що їх треба вивчити й освоїти.

Так саме не менш важливим є питання доведення під розпис до окремих виконавців або до відома усім іншим положення документів системи управління. Як і у який спосіб це буде відбуватись – на розсуд організації. Зазначимо таке, така процедура підвищуватиме відповідальність й дотримання високої виконавської дисципліни, що є невід’ємним правилом у діяльності організації.

Серед інших зазначимо й таке питання як: збережуваність документів і легка й доступна ідентифікація за формалізованою ознакою (далі пропонується система щодо запису певного документа у системі управління).

Щоб унеможливити застосовування застарілого чи скасованого документа пропонується створити процедуру ведення Реєстру документів для системи управління. Так, типи документів можуть бути: внутрішніми й зовнішніми, що також є прерогативою керівництва, що їх затвердить.

Доцільно взяти за правило таке: документуємо те, що робимо і робимо те, що документуємо! Що це дасть? Можливість аналізувати невдачі або, навпаки, – можливість повторення успіху.

Необхідно продумувати усе на папері, щоб зберегти час! Як відмічалося раніше – достатність документації залежатиме від потреб самої організації. Нарешті, треба створити процедуру стосовно регламентування документів організації: це ведення Реєстру, розділення на внутрішню й зовнішню, дробування її на кадрову, фінансову, технологічну тощо систему документування.

Усе викладене вище стосується будь-якої системи управління, проте є певні особливості, притаманні системам управління інформаційної безпеки.

Засади стосовно інформаційної безпеки, закладені у політиці (їх наборі), мають бути впроваджені у численній низці документів нижчого рівня, які пропонується улаштувати у такий спосіб.

Встановлені у політиці (їх пропонується розробити дві: Політика інформаційної безпеки та Політика системи управління інформаційної політики. Перша – закритий документ для внутрішнього обігу, друга – доступна кожному, де наведені зрозумілі позиції, які конкретизовані та деталізовані, й є наскрізною для решти документів нижчого порядку зазначеної системи) основні цілі, принципи щодо інформаційної безпеки та інформаційні активи як напрямок діяльності організації.

Запровадити модулі базисів [3] або головних напрямків діяльності організації. Їх визначити як модулі A, B, C, D, E. Помаркувати ці модулі пропонується так: модуль А – законодавча база (законодавство), модуль В – нормативні документи, модуль С – наукові основи, модуль D – технічне оснащення, модуль Е – організаційна структура.

Ці модулі базисів будуть основними визначниками для розроблених документів системи управління інформаційною безпекою.

Наступний елемент системи документації є модулі напрямків роботи організації або модулі стандарту, а саме: рознесення документів за відомою класифікацією, що її наведено в міжнародному стандарті ISO/IEC 27001:2013 [4]. Цей елемент встановлює заходи та засоби щодо інформаційної безпеки. Таких модулів напрямків роботи у старій версії цього міжнародного документа одинадцять. У додатку А, починаючи з А.5 до А.15, наведено заходи та методи контролю щодо убезпечення інформаційних активів:

1. А.5 Політика безпеки.
2. А.6 Організація інформаційної безпеки.
3. А.7 Управління активами.
4. А.8 Правила безпеки, пов’язані з персоналом.
5. А.9 Фізична та екологічна безпека.
6. А.10 Управління засобами комунікацій та їх функціюванням.
7. А.11 Контроль доступу.
8. А.12 Розроблення, впровадження та обслуговування інформаційних систем.
9. А.13 Управління інцидентами інформаційної безпеки.
10. А.14 Управління безперервністю бізнесу.
11. А.15 Відповідність вимогам.

На основі міжнародного документа було розроблено національний стандарт ДСТУ ISO/IEC 27001:2010 Інформаційні технології. Методи та засоби досягнення інформаційної безпеки системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, IDT) [5], що його слід застосовувати як путівник для менеджерів з систем управління інформаційною безпекою.

Й, нарешті, модуль «Методи, заходи та засоби», що є третім й останнім елементом системи – це документи системи, що їх нумерують порядковими номерами, починаючи з одиниці. Саме тут будуть інструкції, правила, алгоритми дій, письмові описи процесів діяльності організації. На цьому найнижчому, але самому вагомому рівні буде створено документацію, це є деталізувальний модуль системи управління інформаційною безпекою.

**Висновки з даного дослідження і перспективи подальших досліджень у даному напрямку.** Разом з відомими методиками створення й управління документами, пропонованими нормативними документами, опублікованими міжнародними організаціями, що не відкидають нові сучасні й удосконалені досвідом і практикою «системників», подається як зразок система документування, яку можна застосовувати не лише для систем управління інформаційною безпекою, але й для інших систем управління, що їх застосовують на сьогоднішній день для поліпшення функціонування підприємств і організацій.

Наведені правила є доступними та простими. Їх застосування у повсякденній діяльності організації створюватиме комфортні умови роботи персоналу, усуватиме перепони на шляху порозуміння для досягнення успішного й високоякісного управління діяльністю організації.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Quality management systems. Fundamentals and vocabulary [Electronic resource] : ISO 9000:2015. – Access mode : https://www.iso.org/obp/ui/#!iso:std:45481:en. – Access data : August 2015. – The title of the screen.

2. Quality management systems. Requirements [Electronic resource] : ISO 9001:2015. – Access mode : https://www.iso.org/obp/ui/#!iso:std:62085:en. – Access data : September 2015. – The title of the screen.

3. Домарєв В. В. Управління інформаційною безпекою в банківських установах. Теорія і практика впровадження стандартів серії ISO 27k : навчальне видання / В. В. Домарєв, Д. В. Домарєв. – Донецьк : WS Велстар, 2012. – 146 с.: – ISBN 978-966-2759-00-6.

4. Information technology. Security techniques. Information security management systems. Requirements [Electronic resource] : ISO/IEC 27001:2013. – Access mode : https://www.iso.org/obp/ui/#!iso:std:54534:en. – Access data : September 2015. – The title of the screen.

5. Інформаційні технології. Методи та засоби досягнення інформаційної безпеки системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, IDT) : ДСТУ ISO/IEC 27001:2010. – [Чинний від 2010-01-01]. – К. : Держспоживстандарт України, 2010. – 31 с. – (Національний стандарт України).

Стаття надійшла до редакції 16.10.2015.

## REFERENCE

1. International Organization for Standardization (2015), ISO/IEC 9000:2015, *Quality management systems. Fundamentals and vocabulary*, available at: https://www.iso.org/obp/ui/#!iso:std:45481:en (accessed 17 August 2015).

2. International Organization for Standardization (2015), ISO/IEC 9001:2015, *Quality management systems. Requirements*, available at : https://www.iso.org/obp/ui/#!iso:std:62085:en (accessed 08 September 2015).

3. Domarev, V.V., Domarev, D.V. (2012), *Upravlinnia informatsiinoiu bezpekoiu v bankivskykh ustanovakh. Teoriia i praktyka vprovadzhennia standartiv serii ISO 27k* [Management of information security in banks. Theory and practical implementation of standards series ISO 27k], Donetsk: WS «Velstar» Publ., 146 p., ISBN 978-966-2759-00-6.

4. International Organization for Standardization (2013), ISO/IEC 27001:2013, *Information technology. Security techniques. Information security management systems. Requirements*, available at : https://www.iso.org/obp/ui/#!iso:std:54534:en (accessed 08 September 2015).

5. State Committee for Standardization (2010), DSTU ISO/IEC 27001:2010, *Informatsiini tekhnolohii. Metody ta zasoby dosiahnennia informatsiinoi bezpeky systemy keruvannia informatsiinoiu bezpekoiu. Vymohy* [Information Technology. Methods and means of achieving information security management system of information security. Requirements], Kyiv, 26 p.

ЮЛИЯ КОЖЕДУБ

## СОЗДАНИЕ ДОКУМЕНТАЦИИ ДЛЯ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Предложена новая система создания документации для систем управления информационной безопасности, которая отображает особенности, присущие системам

управления информационной безопасности организации. Отображено аспекты, связанные з персоналам и их обхождением с документами, касательно информационной безопасности предприятий и/или организаций.

**Ключевые слова:** документация, международные стандарты, системы управления, управление организацией, персонал.

YULIYA KOZHEDUB

**CREATE DOCUMENTATION FOR INFORMATION SECURITY MANAGEMENT SYSTEMS**

A new system for creating documentation for information security management systems, reflecting the peculiarities inherent in information security management system of the organization. Showing aspects of personnel and their handling of documents related to information security companies and / or organizations.

**Keywords:** documentation, international standards, system management, management organization, personnel.

**Юлія Василівна Кожедуб**, кандидат технічних наук, доцент, 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, Государственное учреждение «Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт», Киев, Украина.

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

УДК 004.056.5:621.39

ЮРИЙ ХЛАПОНИН

**ВЫЯВЛЕНИЕ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ ЗА СЧЕТ ПОБОЧНОГО ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ И НАВЕДЕНИЯ ПУТЕМ ОБРАБОТКИ ОБЛАСТИ СПЕКТРА СВЕРХВЫСОКИХ ЧАСТОТ**

Проведен анализ образования канала утечки информации за счет побочных электромагнитных излучений и наводок (ПЭМИН) для различных компонентов персонального компьютера (ПК). Для стандартного компьютерного монитора перехват информации возможен на частотах до 50 гармоники тактовой частоты. Излучение может происходить в широком диапазоне частот (от единиц Гц до ГГц), а дальность реального перехвата информации достигать сотен метров. Показано, что информативность сигналов ПЭМИН существенная на частотах единиц ГГц, и возникает вопрос о необходимости специальных исследований на частотах нескольких ГГц, хотя методика этого не требует.

Показано, что вопреки распространенному мнению заземление не играет определяющей роли в защите информации от утечки каналом ПЭМИН. Заземление необходимо только по требованиям электробезопасности. В некоторых случаях при