УДК 004.056

А.Я. Гладун, канд. техн. наук, с.н.с.
К.О. Хала, м.н.с.

ТАКСОНОМІЯ СТАНДАРТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Резюме. *У статті представлено таксономію (структурну класифікацію) стандартів інформаційної безпеки (далі — ІБ), що є певним системним аналізом стандартів як на думку їх розробників, так і проектувальників та розробників захищених систем. Таксономія стандартів забезпечує застосування системного підходу декомпозиції загальної проблеми керування безпекою до часткових завдань.*

Ключові слова: *інформаційна безпека, стандарт, авторизація, автентифікація, таксономія.*

ВСТУП

Процес розроблення стандартів у сфері інформаційних технологій (ІТ) і, зокрема, в напрямі інформаційної безпеки відбувається безупинно. Послідовно опубліковують проекти та версії стандартів на різних стадіях узгодження та затвердження. Деякі стандарти поетапно поглиблюють і деталізують у вигляді сукупності взаємозалежних груп стандартів щодо концепцій і структури [1].

Поняття "інформаційна безпека" (ІБ) має багато визначень, наприклад, одне з них може бути таким: ІБ — це стан інформації, за якого забезпечується збереження визначених політикою безпеки властивостей інформації. Більш стандартизоване визначення: ІБ — це збереження конфіденційності, цілісності та доступності інформації. Крім того, можуть враховуватися інші властивості ІБ, наприклад, автентичність, відстежуваність, неспростовність і надійність.

ПОСТАНОВКА ПРОБЛЕМИ

Розробляють стандарти для відкритих систем, зокрема у сфері безпеки ІТ, спеціалізовані міжнародні організації і консорціуми, наприклад, ISO/IEC, ITU-T, IEEE, CEN, CENELEC, IAB, WOS, ANSI, W3C, ECMA, X/Open, OSF, OMG та ін.

Критерії оцінювання інформаційної безпеки є методологічною базою для визначення вимог захисту комп'ютерних систем від несанкціонованого доступу, створення захисних систем та оцінювання ступеня захищеності.

За допомогою критеріїв можна порівняти різні механізми захисту інформації та визначити необхідну їх функціональність під час розроблення захищених комп'ютерних систем. Для характеристики основних критеріїв інформаційної безпеки застосовують модель тріади CIA: *CIA Triad*. Ця система передбачає такі основні характеристики інформаційної безпеки: конфіденційність, цілісність, доступність (*Confidentiality, Integrity and Availability* (CIA)). Інформаційні системи аналізують у трьох головних секторах: технічних засобах, програмному забезпеченні та комунікаціях з метою ідентифікації й застосування промислових стандартів інформаційної безпеки як механізмів захисту та запобігання на трьох рівнях (фізичному, особистому і організаційному). По суті процедури або правила запроваджують для інформування адміністраторів, користувачів та операторів щодо використання захисних механізмів із метою гарантування інформаційної безпеки в межах організацій. В Україні також розробляють і використовують критерії інформаційної безпеки. Наприклад, департамент спеціальних телекомунікаційних систем та захисту інформації СБУ ухвалив нормативний документ технічного захисту інформації 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу", подібний до моделі тріади CIA [2; 3].

Метою статті є дослідження стандартів і нормативних документів у сфері інформаційної безпеки, що відіграють першорядну роль у сьогоднішньому динамічному розподіленому інформаційному просторі для задач пересилання, оброблення та збереження інформації.

Значну роботу зі стандартизації питань безпеки ІТ здійснюють спеціалізовані установи й на національному рівні (ДП "УкрНДНЦ"). Усе це дало змогу сформувати значну методичну базу з міжнародних, національних та галузевих стандартів, а також нормативних і настановчих матеріалів, що регламентують діяльність у сфері безпеки ІТ [4–6].

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Архітектура безпеки та її відображення в еталонній моделі взаємозв'язку відкритих систем. Більшість сучасних складних мереже-

вих структур проектують, враховуючи ідеологію Еталонної моделі взаємозв'язку відкритих систем (ВВС), яка дає змогу кінцевому користувачу мережі (або його прикладним процесам) отримувати доступ до інформаційно-обчислювальних ресурсів значно легше, ніж це було раніше [5; 6].

Завданням ВВС є визначення серії стандартів, які дають змогу системам взаємодіяти. Систему, що взаємодіє з іншими системами та відповідає вимогам відповідних стандартів ВВС, називають реальною відкритою системою.

Завданням стандартизації ВВС є визначення серії стандартів, які дають можливість автономним системам взаємодіяти. Будь-яке обладнання, що вступає у взаємодію і відповідає всім вимогам застосовних стандартів протоколу ВВС, є реальним еквівалентом поняття "відкрита система", визначеного в моделі (**табл. 1**).

Водночас концепція відкритості систем створює низку труднощів в організації захисту інформації у інформаційній системі (ІС). Вимоги щодо захисту ресурсів мережі від несанкціонованого доступу (НСД) є обов'язковими під час проектування й реалізації більшості сучасних ІС, що відповідають вимогам еталонної моделі ВВС.

У 1986 р. міжнародні організації прийняли *Архітектуру безпеки ВВС* (*АБВВС*). В архітек-

Таблиця 1

Напрями стандартизації функцій безпеки (еталонна модель ВВС)

Призначення служби	Процедура захисту	Номер рівня ЕМВВС
Автентифікація:		
– однорівневих об'єктів	– шифрування, цифровий підпис – забезпечення автентифікації	3, 4 3, 4, 7
– джерела даних	– шифрування – цифровий підпис	3, 4 3, 4, 7
Контроль доступу	керування доступом	3, 4, 7
Засекреченість:		
– з'єднання	– шифрування – керування трафіком	1–4, 6, 7 3
– в режимі без з'єднання	– шифрування – керування трафіком	2–4, 6, 7 3
– вибіркових полів	– шифрування	6, 7
– потоку даних	– шифрування – заповнення потоку – керування трафіком	1, 6 3, 7 3
Забезпечення цілісності:		
– з'єднання з відновленням	– шифрування, забезпечення цілісності даних	4, 7
– з'єднання без відновлення	– шифрування, забезпечення цілісності даних	3, 4, 7
– вибіркових полів	– шифрування, забезпечення цілісності даних	7
– без встановлення з'єднання	– шифрування – цифровий підпис – забезпечення цілісності даних	3, 4, 7 4 3, 4, 7
– вибіркових полів без з'єднання	– шифрування – цифровий підпис – забезпечення цілісності даних	7 4, 7 7
Забезпечення неможливості відмови від факту:		
– відправлення	– цифровий підпис, забезпечення цілісності даних, підтвердження характеристик даних	7
– доставлення	– цифровий підпис, забезпечення цілісності даних, підтвердження характеристик даних	7

турі ВВС виокремлюють сім рівнів ієрархії: фізичний, канальний, мережевий, транспортний, сеансовий, представницький і прикладний [5]. Однак у АБВВС передбачено реалізацію механізмів захисту переважно на п'яти рівнях. Для захисту інформації на фізичному й канальному рівнях зазвичай вводять такий механізм захисту, як лінійне шифрування. Канальне шифрування забезпечує закриття фізичних каналів зв'язку за допомогою спеціальних шифраторів. Однак застосування лише канального шифрування не дає повного закриття інформації під час її передавання через мережу, оскільки на вузлах комутації пакетів інформація буде перебувати у відкритому вигляді. Тому НСД порушника до апаратури одного вузла приведе до розкриття усього потоку повідомлень, що проходять через цей вузол.

При встановленні віртуального з'єднання між двома абонентами мережі комунікації проходять по незахищених елементах інформаційно-комунікаційних систем (ІКС), і тоді необхідне наскрізне шифрування, коли закривається інформаційна частина повідомлення, а заголовки повідомлень не шифруються. Це дає змогу вільно керувати потоками зашифрованих повідомлень. Наскрізне шифрування організовується на мережевому чи транспортному рівнях згідно з еталонною моделлю ВВС. На прикладному рівні реалізується більшість механізмів захисту, необхідних для повного розв'язання проблем забезпечення безпеки даних в ІКС.

АБ ВВС установлює такі служби безпеки (див. **табл. 1**):

- забезпечення цілісності даних (із установленням з'єднання, без установлення з'єднання та для вибіркових полів повідомлень);
- забезпечення конфіденційності даних (із установленням з'єднання, без установлення з'єднання та для вибіркових полів повідомлень);
- контролю доступу;
- автентифікації (однорівневі об'єкти і джерела даних);
- забезпечення конфіденційності трафіка;
- унеможливлення відмови від факту відправлення повідомлення абонентом-передавачем і приймання повідомлення абонентом-приймачем.

Стан міжнародної нормативно-методичної бази. З метою аналізу поточного стану міжнародної нормативно-методичної бази в сфері безпеки ІТ необхідно використовувати певну класифікацію напрямів стандартизації. Загалом можна виокремити такі напрями [5]:

- загальні принципи керування інформаційною безпекою;
- моделі безпеки ІТ;
- методи та механізми безпеки ІТ (наприклад, методи автентифікації, керування ключами тощо);
- криптографічні алгоритми;
- методи оцінювання безпеки інформаційних систем;
- безпека EDI-технологій;
- безпека міжмережевої взаємодії (міжмережеві екрани);
- сертифікація й атестація об'єктів стандартизації.

Стандартизація задач керування інформаційною безпекою. Аналіз проблеми захисту інформації в інформаційних системах і мережах потребує, зазвичай, деякого комплексного підходу з застосуванням загальнометодологічних концептуальних рішень. Вони дають змогу визначити необхідний системотворчий підхід декомпозиції загальної проблеми керування безпекою до вирішення часткових завдань. Тому сьогодні зростає роль стандартів і регламентуючих матеріалів загальнометодологічного призначення.

На роль такого документа претендує міжнародний стандарт ДСТУ ISO/IEC TR 13335 *Інформаційні технології. Настанови з керування безпекою інформаційних технологій* (*ІТ*). Він складається з п'яти частин: концепції й моделі безпеки ІТ; керування та планування безпеки ІТ; методи керування захистом ІТ; вибір засобів захисту; настанова з керування мережевою безпекою. Вони були прийняті у 2003, 2005 рр. як національні стандарти України [7–9].

Ці документи містять:

- визначення найважливіших понять, безпосередньо пов'язаних із проблемами керування безпекою інформаційних технологій;
- визначення важливих архітектурних рішень щодо створення систем керування безпекою інформаційних технологій (СКБІТ), зокрема, складу елементів, задач, механізмів і методів СКБІТ;
- опис типового життєвого циклу та принципів функціонування СКБІТ;
- опис принципів формування політики (методики) керування безпекою інформаційних технологій;
- методику аналізу висхідних даних для побудови СКБІТ, зокрема методику ідентифікації та аналізу складу об'єктів захисту, уразливих місць інформаційної системи, загроз безпеки та ризиків тощо;
- методику вибору відповідних заходів захисту й оцінювання залишкового ризику;
- принципи побудови керування в СКБІТ та ін. [6–8].

Ще один важливий міжнародний стандарт ISO/TR 13569:2005 — *Financial services — Information security guidelines* (*Фінансові послуги. Настанови щодо інформаційної безпеки*) містить рекомендації з розроблення програмного забезпечення для ІБ для установ у сфері фінансових послуг. У стандарті є опис політики безпеки, організаційних, структурних, правових і нормативних компонентів такої програми. Також обговорюються питання вибору і впровадження контролю безпеки та елементів, необхідних для керування ризиками ІБ у сучасній фінансовій установі. Ці рекомендації базуються на аналізі установ, бізнес-середовища, практики та процедур. До настанови долучено обговорення правових і нормативних питань, дотримання яких має бути розглянуто в процесі розроблення й реалізації програм.

Стандартизація механізмів і моделей безпеки ІТ. Для більшої обґрунтованості програмно-технічних рішень під час побудови СКБІТ, а також визначення її ступеня гарантії, необхідно використовувати за можливості точніші описові моделі як на загальносистемному (архітектурному) рівні, так і на рівні окремих аспектів і засобів СКБІТ.

Побудова моделей дає змогу структурувати та конкретизувати досліджувані об'єкти, усунути неоднозначності в їхньому розумінні, розбити розв'язувану задачу на підзадачі й у остаточному підсумку — виробити необхідні рішення.

Можна виділити такі міжнародні стандарти та інші документи, у яких визначено основні моделі безпеки ІТ:

1. *ДСТУ ISO 7498-2:2004 Системи оброблення інформації. Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 2. Архітектура захисту інформації.*

У ДСТУ ISO/IEC 7498-2:2004 визначено організацію інформаційної безпеки в ІКС згідно з еталонною моделлю ВВС. Стандарт є перекладом міжнародного стандарту ISO 7498-2:1989 (Information processing systems. — Open Systems Interconnection. — Basic Reference Model. — Part 2. Security Architecture). Він визначає загальні архітектурні елементи, що стосуються захисту, які можуть бути відповідно використані, коли необхідний захист даних, переданих між відкритими системами. ДСТУ ISO 7498-2:2004 встановлює в рамках еталонної моделі основні напрями й обмеження щодо удосконалення чинних стандартів або розроблення нових стандартів у сфері ВВС для захисту обміну даних і так забезпечує погоджений підхід щодо захисту інформації.

ДСТУ ISO 7498-2:2004 є розширенням базової еталонної моделі щодо аспектів захисту інформації, які стали загальними архітектурними елементами для протоколів обміну даними, але не розглянуті в базовій еталонній моделі. Цей стандарт незамінний для тих, хто працює в галузі технологій захисту корпоративних мереж, захисту при наданні інформаційних послуг в Інтернеті та інтеграції мобільних і наземних телекомунікаційних систем.

У **табл. 2** перелічено механізми, які окремо або в поєднанні з іншими розглядають як можливі в деяких випадках для забезпечення кожної послуги. Ця таблиця є оглядом таких взаємин і не є вичерпною. Послуги та механізми, наведені тут, описано в п. 5.2 і 5.3ДСТУ ISO 7498-2 (докладніший опис взаємин наведено в розділі 6 цього стандарту) [5].

У цьому стандарті є посилання на такі стандарти: *ДСТУ ISO/IEC 7498-1:2004 (Системи оброблення інформації. Взаємозв'язок відкритих систем. Базова еталонна модель)* та *ДСТУ ISO/IEC 7498-4:2015 (Системи оброблення інформації. Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 4. Основи адміністративного керування)*.

2. Міжнародний стандарт *ISO/IEC 1018 — Information technology — Open Systems Interconnection (Інформаційні технології — Взаємозв'язок відкритих систем)* складається з таких семи частин: загальний опис основ захисту інформації у ВВС; основи автентифікації; керування доступом; безвідмовність одержання; конфіденційність; цілісність; основи перевірки захисту.

3. Міжнародний багаточастинний стандарт *ISO/IEC 15408 Information technology — Security techniques — Evaluation criteria for IT security (Інформаційні технології. Технології безпеки. Загальні критерії оцінювання безпеки інформаційних технологій)* описує інфраструктуру, в якій користувачі комп'ютерної системи можуть висунути свої вимоги, розробники — заявити про властивості безпеки продуктів, а експерти з безпеки — визначити, чи задовольняє продукт заявкам щодо безпеки. Цей стандарт гарантує, що процес опису, розроблення та перевірки продукту проведено в строгому порядку. Прообразом документа слугували "Критерії оцінювання безпеки інформаційних технологій" (англ. *Evaluation Criteria for IT Security*, ECITS), робота над якими почалася в 1990 р. Стандарт дає змогу оцінити повноту системи інформаційної безпеки з технічної точки зору, не розглядаючи при цьому комплекс організаційних заходів щодо забезпечення захисту інформації.

Проблема убезпечення інформаційних технологій займає усе значніше місце в реалізації комп'ютерних систем і мереж у міру того, як

Таблиця 2

Механізми забезпечення послуг згідно з еталонною моделлю ВВС

Механізми послуг	Шифрування	Цифровий підпис	Керування доступом	Цілісність даних	Обмін автентифікацією	Заповнення трафіка	Керування маршрутизацією	Нотаризація
Автентифікація рівноправного логічного об'єкта	Так	Так	*	*	Так	*	*	*
Автентифікація відправника даних	Так	Так	*	*	*	*	*	*
Сервіс керування доступом	*	*	Так	*	*	*	*	*
Конфіденційність у режимі з установленням з'єднання	Так	*	*	*	*	*	Так	*
Конфіденційність у режимі без установлення з'єднання	Так	*	*	*	*	*	Так	*
Конфіденційність вибіркового поля	Так	*	*	*	*	*	*	*
Конфіденційність потоку трафіка	Так	*	*	*	*	Так	Так	*
Цілісність у режимі з установленням з'єднання з відновленням	Так	*	*	Так	*	*	*	*
Цілісність у режимі з установленням з'єднання без відновлення	Так	*	*	Так	*	*	*	*
Цілісність вибіркового поля в режимі з установленням з'єднання	Так	*	*	Так	*	*	*	*
Цілісність у режимі без установлення з'єднання	Так	Так	*	Так	*	*	Так	*
Цілісність вибіркового поля в режимі без установлення з'єднання	Так	Так	*	Так	*	*	*	*
Безвідмовність відправника	*	Так	*	Так	*	*	*	Так
Безвідмовність одержувача	*	Так	*	Так	*	*	*	Так

Позначення: Так — механізм вважають можливим для використання як окремо, так і в поєднанні з іншими механізмами; * — механізм вважають неможливим для використання.

зростає їхня роль в інформатизації суспільства. Безпека інформаційних технологій є комплексною проблемою, яка розв'язується через удосконалення правового регулювання для застосування ІТ, розвиток системи сертифікації, забезпечення відповідних організаційно-технічних умов експлуатації. Ключовим аспектом розв'язку проблеми безпеки ІТ стає вироблення системи вимог, критеріїв і показників для оцінювання рівня безпеки ІТ.

Стандарт ISO/IEC 15408 містить загальні критерії оцінювання безпеки ІТ і складається з трьох частин.

Стандарт ISO/IEC 15408-1 установлює загальний підхід до формування вимог для оцінювання безпеки (функціональні та довірчості), основні конструкції (профіль захисту, завдання щодо безпеки) представлення вимог безпеки в інтересах споживачів, розробників і оцінювачів продуктів і систем ІТ. Вимоги безпеки об'єкта

Таблиця 3

Основні властивості інформації як об'єкта захисту

Характеристика основних властивостей інформації	Опис характеристики
Конфіденційність (*confidentiality*)	Властивість інформації, яка полягає в тому, що вона не може бути отримана неавторизованим користувачем
Цілісність (*integrity*)	Означає неможливість модифікації неавторизованим користувачем
Доступність (*availability*)	Властивість інформації бути отриманою авторизованим користувачем за наявності у нього відповідних повноважень, у необхідний для нього час
Додатково також використовують такі властивості:	
Апелювання (*non-repudiation*)	Можливість довести, що автором є саме заявлена людина (юридична особа) і ніхто інший
Підзвітність (*accountability*)	Властивість інформаційної системи, що дає змогу фіксувати діяльність користувачів, використання ними пасивних об'єктів та однозначно встановлювати авторів певних дій у системі
Достовірність (*reliability*)	Властивість інформації, яка визначає ступінь об'єктивного, точного відображення подій, фактів
Автентичність (*authenticity*)	Властивість, яка гарантує, що суб'єкт або ресурс ідентичні заявленим

оцінки (ОО) згідно з методологією Загальних критеріїв визначають, враховуючи цілі безпеки, які у свою чергу ґрунтуються на аналізі призначення ОО і умов середовища його використання (погроз, припущень, політики безпеки).

Стандарт ISO/IEC 15408-2 містить універсальний систематизований каталог функціональних вимог безпеки й передбачає можливість їх деталізації й розширення за певними правилами.

Стандарт ISO/IEC 15408-3 містить систематизований каталог вимог довірчості, що визначають заходи, яких треба вжити на всіх етапах життєвого циклу продукту або системи ІТ для впевненості в тому, що вони задовольняють пред'явлені до них функціональні вимоги. Тут же містяться оцінювальні рівні довірчості, що визначають шкалу вимог, які дають змогу зі зростаючим ступенем повноти й строгості оцінити проектну, тестову й експлуатаційну документацію, правильність реалізації функцій безпеки ОО, уразливості продукту або системи ІТ, стійкість механізмів захисту й зробити висновок про рівень довірчості до безпеки об'єкта оцінювання.

Стандарт містить два основних види вимог безпеки: функціональні, що висуваються до функцій безпеки і реалізують їхні механізми, і вимоги довірчості, які пред'являють до технології та процесу розроблення й експлуатації.

Для характеристики основних властивостей інформації як об'єкта захисту часто використовується модель CIA (Confidentiality, Integrity, Aavailability) (див. **табл. 3**).

4. Міжнародний стандарт *ISO/IEC 10745: 1995 — Information technology — Open Systems Interconnection — Upper layers security model (Інформаційні технології. Взаємозв'язок відкритих систем. Модель захисту інформації верхніх рівнів)* визначає модель безпеки у верхніх рівнях OSI, що забезпечує основу для розвитку застосувань незалежних сервісів і протоколів, а також визначає аспекти безпеки у верхніх рівнях OSI.

5. Міжнародний стандарт *ISO/IEC 11586-1:1996 — Information technology — Open Systems Interconnection — Generic upper layers security: Overview, models and notation (Інформаційні технології. Взаємозв'язок відкритих систем. Загальні функції захисту верхніх рівнів. Огляд, моделі та позначення)* визначає набір базових засобів для надання допомоги в забезпеченні безпеки послуг для застосувань ВВС.

Стандартизація методів і механізмів безпеки ІТ. На певному етапі задачу захисту інформаційних технологій поділяють на підзада-

чі: забезпечення конфіденційності, цілісності, доступності. Для цих підзадач треба виробляти конкретні рішення щодо організації взаємодії об'єктів і суб'єктів інформаційних систем. До таких рішень належать методи:

- автентифікації суб'єктів і об'єктів інформаційної взаємодії, призначені для надання взаємодіючим сторонам можливості впевнитися, що протилежна сторона дійсно є тим, за кого себе видає;
- шифрування інформації, призначені для захисту у разі перехоплення її третіми особами;
- контролю цілісності, призначені для того, щоб інформацію не було спотворено чи підмінено;
- керування доступом, призначені для розмежування доступу до інформації різних користувачів;
- підвищення надійності та відмовостійкості функціонування системи, призначені для забезпечення гарантій виконання інформаційною системою цільових функцій;
- керування ключами, призначені для організації створення, поширення й використання ключів суб'єктів і об'єктів інформаційної системи, з метою закладення необхідного базису для процедур автентифікації, шифрування, контролю автентичності та керування доступом.

Організації зі стандартизації приділяють велику увагу розробленню типових рішень для безпеки. До них у першу чергу варто віднести такі міжнародні стандарти (серед них є чинні в Україні):

1. Багаточастинний стандарт *ISO/IEC 9798 — Information technology — Security techniques — Entity authentication (Інформаційні технології. Методи та засоби забезпечення безпеки. Автентифікація об'єкта)*. Цей стандарт складається з шести частин: загальні положення; механізми, що використовують алгоритми симетричного шифрування; механізми, що використовують метод цифрового підпису; методи на базі криптографічних контрольних функцій; механізми, що використовують методи нульової обізнаності; механізми, що використовують ручне передавання даних. Стандарт визначає модель автентифікації, загальні вимоги та обмеження для механізмів автентифікації особи, які використовують методи забезпечення безпеки. Ці механізми застосовують, щоб підтвердити, що особа є тим, за кого себе видає. Чинний в Україні.

2. *ISO/IEC 9798-6:2010 — Information technology — Security techniques — Entity authentication — Part 6: Mechanisms using manual data transfer (Інформаційні технології. Методи та засоби забезпечення безпеки. Об'єкт перевірки дійсності. Частина 6. Механізми використовувані для ручного передавання даних)* визначає вісім механізмів автентифікації особи, базованих на ручному передаванні даних між пристроями автентифікації.

3. *ISO/IEC 11577:1995 Information technology — Open Systems Interconnection — Network layer security protocol (Інформаційні технології. Взаємозв'язок відкритих систем. Протокол захисту інформації на мережевому рівні)*.

Тестування конформності (тестування на відповідність) є механізмом, за допомогою якого визначають ступінь відповідності продуктів IT базовим стандартам і профілям. Тестування конформності слугує апаратом, що пов'язує світ продуктів і сервісів IT із системою стандартів.

Наприклад, спосіб використання введеної класифікації вимог щодо конформності ілюструє стандарт міжнародного стандартизованого профілю ISO/IEC ISP 10613-19, в якому обумовлюється функціональність системи ретранслятора (маршрутизатора), що реалізує функції мережевого сервісу моделі BBC у режимі передавання дейтаграм, доповнені засобами мережевої безпеки, надаваної протоколом Network Layer Security Protocol (NLSP — ITU-T X.273|ISO/IEC 11577).

ISO/IEC 11577 визначає протокол, який буде використовувати прикінцева система (End Systems) та проміжна система з метою забезпечення безпеки послуг мережевого рівня, який визначається стандартом CCITT Rec. X.213, ISO/IEC 8348 і ISO 8648. Протокол, що тут визначено, має назву "Протокол безпеки мережевого рівня" — Layer Security Protocol (NLSP).

4. Міжнародний стандарт *ISO/IEC 10736: 1995 Information technology — Telecommunications and information exchange between systems — Transport layer security protocol (Інформаційні технології. Телекомунікації й обмін інформацією між системами. Протокол захисту інформації на транспортному рівні)*. Стандарт визначає безпеку протоколу транспортного рівня, неспецифіковані функції керування та протоколи, необхідні для підтримання цього протоколу безпеки. Стандарт обумовлює протокол, який може бути використано для створення безпеки асоціації. Задає один алгоритм автентифікації і розподілу ключів, що базується на відкритих ключах системи шифрування.

5. Багаточастинний стандарт *ISO/IEC 13888 — Information technology — Security techniques — Non-repudiation (Інформаційні технології. Методи й засоби забезпечення безпеки. Механізми запобігання відмовам)*. Цей стандарт має три

частини: загальні відомості; механізми з використанням симетричних методів; механізми з використанням асиметричних методів. Чинний в Україні.

6. *ISO/IEC 9594-8:2014 — Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks (Взаємозв'язок відкритих систем. Каталог. Частина 8. Основи автентифікації)*. Стандарт ISO/IEC 9594-8 формулює основні складові сертифікатів відкритих ключів, але недостатньо точно для інтероперабельних реалізацій. Чинний в Україні з 01.01.2016 р. як ДСТУ ISO/IEC 9594-8:2014.

7. *ISO/IEC 11568 — Banking — Key management (retail) (Банківська справа. Керування ключами)*. Цей стандарт містить чотири частини: введення. Керування ключами; методи керування ключами для симетричних шифрів; життєвий цикл ключа для симетричних шифрів; асиметричні криптосистеми. Управління ключами і життєвий цикл.

8. *ISO/IEC 13492:2007 Financial services — Key management related data element — Application and usage of ISO 8583 data elements 53 and 96 (Фінансові послуги. Управління ключами, що пов'язані з елементом даних. Застосування і використання елементів даних 53 і 96 ISO 8583)*.

9. *Багаточастинний стандарт ISO/IEC 11770 — Information technology — Security techniques — Key management (Інформаційні технології. Методи захисту. Керування ключами захисту)*. Цей стандарт містить п'ять частин: структура; механізми, що використовують симетричні методи; механізми, що використовують асиметричні методи розроблення; механізми на базі нестійких секретів; група керування ключами.

10. *ISO/IEC 10164-7:1992 — Information technology — Open Systems Interconnection — Systems Management — Part 7: Security alarm reporting function (Інформаційні технології. Взаємозв'язок відкритих систем. Адміністративне керування системи. Частина 7. Функції повідомлення про порушення інформаційної безпеки)*. Чинний в Україні.

11. *ISO/IEC 11586 — Information technology — Open Systems Interconnection — Generic upper layers security (Інформаційні технології. Взаємозв'язок відкритих систем. Загальні функції захисту верхніх рівнів)*. Цей стандарт містить шість частин: загальний опис, моделі й нотація; визначення послуг сервісного елемента обміну інформацією захисту; специфікація протоколу сервісного елемента обміну інформацією захисту; специфікація синтаксису захищеного передавання; проформа про відповідність протокольної реалізації сервісного елемента обміну інформацією захисту; проформа синтаксису захищеного передавання про відповідність протокольної реалізації.

У стандартах цього рівня, зазвичай, не вказують конкретні криптографічні алгоритми, а декларують, що може бути використано будь-який криптоалгоритм, при цьому мають на увазі використання певних зарубіжних криптографічних алгоритмів. Тому в разі використання деяких стандартів може знадобитися їхня адаптація до вітчизняних криптоалгоритмів.

Стандартизація національних криптографічних алгоритмів. Мінекономрозвитку України у 2014 р. наказом ухвалило національні європейські та міжнародні нормативні документи, які будуть сприяти гармонізації вимог у сфері розвитку та забезпечення інтероперабельності системи електронного цифрового підпису. Йдеться про найпоширеніші в світі криптографічні алгоритми та протоколи: RSA, DSA, KCDSA, ECDSA, EC KCDSA,EC-GDSA тощо. Окремо було прийнято два національних стандарти: ДСТУ 7624:2014 "*Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення*"; ДСТУ 7564:2014 "*Інформаційні технології. Криптографічний захист інформації. Функція гешування*" на алгоритм симетричного блокового перетворення та на функції хешування [10].

Стандарт *ДСТУ 7624:2014* розроблено для поступової заміни міждержавного стандарту ДСТУ ГОСТ 28147:2009 (на базі ГОСТ 28147-89, який визначає симетричний блочний алгоритм криптографічного перетворення), а ДСТУ 7564:2014 — для поступової заміни міждержавного стандарту ГОСТ 34.311:1995 (визначає функцію гешування та має посилання на ГОСТ 28147-89), які не відповідають сучасним вимогам до швидкодії і потенційним викликам щодо криптографічної стійкості [9–10].

Стандарт *ДСТУ 7624:2014* визначає сучасний алгоритм симетричного блокового перетворення для забезпечення конфіденційності та цілісності інформації під час її оброблення і встановлює режими його роботи (застосування).

Криптографічні перетворення, що їх застосовують в алгоритмі, відповідають сучасним вимогам щодо рівня криптографічної стійкості та швидкодії. Алгоритм розроблено з урахуванням наявних і потенційних загроз, подальшого інтенсивного розвитку інформаційних технологій і необхідності активного використання протягом декількох наступних десятиліть.

Застосування стандарту ISO/IEC 15408: 2008 для оцінювання безпеки IT. Безпека IT значною мірою визначається досконалістю від-

повідної нормативно-методичної бази. Міжнародний стандарт *ISO/IEC 15408-2008 Information technology — Security techniques — Evaluation criteria for IT security (Інформаційні технології. Методи убезпечення. Критерії оцінювання безпеки інформаційних технологій)* є результатом узагальнення досвіду різних держав з розробки й практичного використання критеріїв оцінювання безпеки ІТ [11–13]. Базовими документами, які лягли в основу загальних критеріїв, є Оранжева книга (TCSEC) 1985 р., Європейські критерії (ITSEC) 1991 р., Канадські критерії 1993 р., Федеральні критерії США 1993 р.

У "Загальних критеріях" (ЗК) проведена класифікація широкого набору функціональних вимог і вимог довіри до безпеки, визначені структури їх групування й принципи цільового використання. Основні відмінні риси ЗК:

1. Насамперед, ЗК — це певна методологія й система формування вимог і оцінювання безпеки ІТ. Системність простежується, починаючи від термінології й рівнів абстракції подання вимог аж до їхнього застосування під час оцінювання безпеки на всіх етапах життєвого циклу продуктів і систем ІТ.

2. Загальні критерії характеризуються найбільш повною сукупністю вимог до безпеки ІТ.

3. У ЗК проведено чіткий поділ вимог безпеки на функціональні вимоги й вимоги довіри до безпеки. Функціональні вимоги (11 класів, 66 сімейств, 135 компонентів) стосуються функцій безпеки (ідентифікації, автентифікації, керування доступом, аудиту тощо), а вимоги довіри (8 класів, 44 сімейства, 93 компоненти) — досягнення впевненості в коректності реалізації й ефективності функцій безпеки через оцінювання технології розроблення, тестування, аналізу вразливостей експлуатаційної документації, постачання та супроводу продуктів і систем ІТ.

4. Загальні критерії охоплюють шкалу довіри до безпеки (оціночні рівні довіри — ОРД), яку можна використовувати для одержання різного ступеня впевненості в безпеці продуктів і систем ІТ.

5. Систематизація й класифікація вимог за ієрархією "клас — сімейство — компонент — елемент" з унікальними ідентифікаторами вимог забезпечує зручність їх використання.

6. Компоненти вимог у сімействах і класах ранжуються за ступенем повноти й строгості, а вимоги довіри згруповані в пакети вимог.

7. Гнучкість у підході до вимог безпеки для різних типів продуктів і систем ІТ і умов їх застосування забезпечується можливістю цілеспрямованого формування необхідних наборів вимог у вигляді певних стандартизованих структур (пакетів вимог, профілів захисту й завдань щодо безпеки).

8. Загальні критерії мають відкритість і розширюваність, тобто дають змогу уточнювати наявні й уводити додаткові вимоги.

Як показують оцінки фахівців у сфері ІБ за рівнем систематизації, повноти і можливостях деталізації вимог, універсальності й гнучкості в застосуванні ЗК представляють найбільш досконалий з наявних сьогодні стандартів. Причому, що дуже важливо, з огляду на особливості побудови він має майже не обмежені можливості для розвитку і є базовим стандартом, що містить методологію завдання вимог і оцінювання безпеки ІТ, а також систематизований каталог вимог безпеки. Як функціональні стандарти, у яких формулюють вимоги до безпеки визначених типів продуктів і систем ІТ, використовують профілі захисту (ПЗ), створювані за методологією та на основі каталогу вимог ЗК. У ПЗ може бути включено й будь-які інші вимоги, які є необхідними для забезпечення безпеки конкретного типу продуктів або систем ІТ.

На основі дослідження цього стандарту можна дійти висновку, що ЗК дають змогу підвищити довіру до засобів захисту і самої інформації, захист якої відбувається на основі трьох базових якостей:

1. Можливості гнучкого обґрунтування вимог до засобів захисту інформації з урахуванням їх призначення й умов застосування.

2. Більш повного й обґрунтованого набору вимог безпеки.

3. Методологія оцінювання, що забезпечує об'єктивність і порівняння результатів.

ВИСНОВКИ

Головним завданням стандартів з ІБ є узгодженість позицій і запитів виробників, споживачів та аналітиків класифікаторів ІТ-продуктів. Кожна з категорій фахівців оцінює стандарти, вимоги й критерії за своїми власними параметрами. Для споживачів найбільшу роль відіграє простота критеріїв та однозначність параметрів вибору захищеної системи, а для найбільш кваліфікованої частини споживачів — гнучкість вимог і можливість їх застосування до специфічних ІТ-продуктів і середовища експлуатації. Виробники потребують від стандартів максимальної конкретності та загальних вимог і критеріїв з сучасними обчислювальними архітектурами та з поширеними операційними системами.

Експерти з ІБ потребують стандартів, які детально регламентують процедуру кваліфікаційного аналізу, та чітких, простих, однозначних і легких критеріїв. Очевидно, що такий ідеал є

недосяжним, і реальність потребує від кожної сторони певних компромісів.

Представлена таксономія (структурна класифікація) стандартів з ІБ надає певний суб'єктивний аналіз стандартів на думку як розробників, так і проектувальників захищених систем з метою уведення загальних "об'єктивних" критеріїв зіставлення. Таксономія стандартів забезпечує застосування системного підходу декомпозиції загальної проблеми керування безпекою до розв'язку часткових завдань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Гладун А.Я*. Онтологічній підхід до проблем підвищення якості розроблення національних стандартів України / А.Я. Гладун, Ю.В. Рогушина // Стандартизація, сертифікація, якість. — 2016. — № 2. — С. 19–28.
2. *Гладун А.Я*. Data Maning: Пошук знань в даних / А.Я. Гладун, Ю.В. Рогушина; ред. С. Кузнецов. — К. : ТОВ "ВД "АДЕФ-Україна", 2016. — 452 с.
3. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. — Вид. офіц. — Вперше введ. 1999-07-01. — К. : Держспоживстандарт України, 1999. — IV, 61 с. (Нормативній документ Системи технічного захисту інформації).
4. *Гладун А.Я*. Семантичні технології: принципи та практики: монографія / А.Я. Гладун, Ю.В. Рогушина; ред. С. Кузнецов. — К. : ТОВ "ВД "АДЕФ-Україна", 2016. — 387 с.
5. Системи оброблення інформації. Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 2. Архітектура захисту інформації (ISO 7498-2: 1989, IDT): ДСТУ ISO 7498-2:2004. — Вид. офіц. — Вперше введ. 2006-04-01. — К. : Держспоживстандарт України, 2006. — IV. — 40 с. (Національний стандарт України).
6. Системи обробки інформації — Взаємозв'язок відкритих систем — Базова еталонна модель — Частина 4: Структура управління: ISO / IEC 7498-4: 1989 — ISO / IEC. — Перше редагування. 1989-11-16. — Міжнародна організація зі стандартизації, 2006. — I. — 9 с. (Міжнародний стандарт).
7. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 2. Керування та планування безпеки IT (ISO/IEC TR 13335-2:1997, IDT): ДСТУ ISO/IEC TR 13335-2:2003. — Вид. офіц. — Вперше введ. 2004-10-01. — К. : Держспоживстандарт України, 2005. — IV. — 16 с. (Національний стандарт України).
8. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 3. Методи керування захистом IT (ISO/IEC TR 13335-3:1998, IDT): ДСТУ ISO/IEC TR 13335-3:2003. — Вид. офіц. — Вперше введ. 2004-10-01. — К. : Держспоживстандарт України, 2005. — IV. — 16 с. (Національний стандарт України).
9. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 5. Настанова з керування мережною безпекою (ISO/IEC TR 13335-5:2001, IDT): ДСТУ ISO/IEC TR 13335-5:2005. — Вид. офіц. — Вперше введ. 2006-07-01. — К. : Держспоживстандарт України, 2007. — VIII. — 21 с. (Національний стандарт України).
10. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення: ДСТУ 7624:2014. — Вид. офіц. — Вперше введ. 2015-07-01. — К. : Держспоживстандарт України, 2015. — III. — 226 с. (Національний стандарт України).
11. Інформаційні технології. Криптографічний захист інформації. Функція хешування: ДСТУ 7564: 2014. — Вид. офіц. — Вперше введ. 2015-04-01. — К. : Держспоживстандарт України 2015, III. — 37 с. (Національний стандарт України).
12. Інформаційні технології — Методи убезпечення — Критерії оцінення безпеки IT — Частина 2: Функціональні компоненти безпеки: ISO / IEC 15408-2 2008 — ISO / IEC. — Перше редагування. 2008-08-19; Остання зміна. 2014-12-01. — Міжнародна організація по стандартизації, 2008 — III. — 218 с. (Міжнародний стандарт).
13. Інформаційні технології — Методи убезпечення — Критерії оцінення безпеки IT — Частина 3: Компоненти убезпечення: ISO / IEC 15408-2 2008 — ISO / IEC. — Перше редагування. 2008-08-19; Остання зміна. 2014-12-01. — Міжнародна організація по стандартизації, 2008 — III. — 174 с. (Міжнародний стандарт).

REFERENCES

1. *Hladun A.Ia., Rohushyna Yu.V*. (2016) Ontolohichnii pidkhid do problem pidvyshchennia yakosti rozroblennia natsionalnykh standartiv Ukrainy [Ontological approach to improving the quality of development of national standards of Ukraine]. Standartyzatsiia, sertyfikatsiia, yakist [Standardization, Certification, Quality], no. 2, pp. 19–28.
2. *Hladun A.Ia., Rohushyna Yu.V*. (2016) Data Maning: Poshuk znan v danykh [Search for knowledge in these], Ed. S. Kuznetsov. Kyiv: TOV "VD "ADEF-Ukraina", 452 p.
3. Kryterii otsinky zakhyshchenosti informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu: ND TZI 2.5-004-99 [Criteria for evaluating information security in computer systems from unauthorized access: Sun Heat 2.5-004-99. — Kind. official. — For the first time intr. 07/01/1999]. Kyiv: Derzhspozhyvstandart Ukrainy [State Committee of Ukraine], 1999. IV, 61 p. Normatyvnii dokument Systemy tekhnichnoho zakhystu informatsii [Normative documents of technical protection of information].
4. *Hladun A.Ia., Rohushyna Yu.V*. (2016) Semantychni tekhnolohii: pryntsypy ta praktyky: monohrafiia [Principles and Practice. monograph]. Kyiv: TOV "VD "ADEF-Ukraina", 387 p.
5. Systemy obroblennia informatsii. Vzaiemozviazok vidkrytykh system. Bazova etalonna model. Chastyna 2. Arkhitektura zakhystu informatsii (ISO 7498-2: 1989, IDT): DSTU ISO 7498-2:2004. — 2006-04-01 [Information processing systems. Open Systems Interconnection. Basic reference model. Part 2. Architecture of information security (ISO 7498-2: 1989, IDT): GOST ISO 7498-2: 2004. — Kind. official. — For the first time intr. 2006-04-01]. Kyiv: Derzhspozhyvstandart Ukrainy [State Committee of Ukraine], 2006. IV, 40 p. Natsionalnyi standart Ukrainy [National standard of Ukraine].
6. Systemy obrobky informatsii — Vzaiemozviazok vidkrytykh system — Bazova etalonna model — Chastyna 4: Struktura upravlinnia: ISO/IEC 7498-4: 1989 — ISO/IEC. — 1989-11-16 [Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 4: Management framework: ISO/IEC 7498-4:1989 — ISO/IEC. — First edit. 1989-11-16]. Mizhnarodna orhanizatsiia zi

standartyzatsii [International Organization for Standardization], 2006. I, 9 p. Mizhnarodnyi standart [International standard].
7. Informatsiini tekhnolohii. Nastanovy z keruvannia bezpekoiu informatsiinykh tekhnolohii (IT). Chastyna 2. Keruvannia ta planuvannia bezpeky IT (ISO/IEC TR 13335-2:1997, IDT): DSTU ISO/IEC TR 13335-2:2003. — 2004-10-01 [Information Technology. Guide to Security Management Information Technology (IT). Part 2: Managing and planning IT Security (ISO/IEC TR 13335-2: 1997, IDT): GOST ISO/IEC TR 13335-2: 2003. — Kind. official. — For the first time intr. 2004-10-01]. Kyiv: Derzhspozhyvstandart Ukrainy [State Committee of Ukraine], 2005. IV, 16 p. Natsionalnyi standart Ukrainy [National standard of Ukraine].
8. Informatsiini tekhnolohii. Nastanovy z keruvannia bezpekoiu informatsiinykh tekhnolohii (IT). Chastyna 3. Metody keruvannia zakhystom IT (ISO/IEC TR 13335-3:1998, IDT): DSTU ISO/IEC TR 13335-3: 2003 [Information technology. Guide to Security Management Information Technology (IT). Part 3. Methods of protection of IT management (ISO/IEC TR 13335-3:1998, IDT): GOST ISO / IEC TR 13335-3: 2003. — Kind. official. — For the first time intr. 2004-10-01]. Kyiv: Derzhspozhyvstandart Ukrainy [State Committee of Ukraine], 2005. IV, 16 p. Natsionalnyi standart Ukrainy [National standard of Ukraine].
9. Informatsiini tekhnolohii. Nastanovy z keruvannia bezpekoiu informatsiinykh tekhnolohii (IT). Chastyna 5. Nastanova z keruvannia merezhnoiu bezpekoiu (ISO/IEC TR 13335-5:2001, IDT): DSTU ISO/IEC TR 13335-5:2005. — 2006-07-01 [Information technology. Guide to Security Management Information Technology (IT). Part 5. Guidance on managing network security (ISO / IEC TR 13335-5: 2001, IDT): GOST ISO/IEC TR 13335-5: 2005. — Kind. official. — For the first time intr. 2006-07-01]. Kyiv: Derzhspozhyvstandart Ukrainy [State Committee of Ukraine], 2007. VIII, 21 p. Natsionalnyi standart Ukrainy [National standard of Ukraine].
10. Informatsiini tekhnolohii. Kryptohrafichnyi zakhyst informatsii. Alhorytm symetrychnoho blokovoho peretvorennia: DSTU 7624:2014. — 2015-07-01. [Information technology. Cryptographic protection. The algorithm is a symmetric block transformation: ISO 7624: 2014. — Kind. official. — For the first time intr. 07/01/2015]. Kyiv: Derzhspozhyvstandart Ukrainy [State Committee of Ukraine], 2015. III, 226 p. Natsionalnyi standart Ukrainy [National standard of Ukraine].
11. Informatsiini tekhnolohii. Kryptohrafichnyi zakhyst informatsii. Funktsiia kheshuvannia: DSTU 7564: 2014. — 2015-04-01. [Information technology. Cryptographic protection. Hash function: ISO 7564: 2014. — Kind. official. — For the first time intr. 04/01/2015]. Kyiv: Derzhspozhyvstandart Ukrainy [State Committee of Ukraine], 2015. III, 37 p. Natsionalnyi standart Ukrainy [National standard of Ukraine].
12. Informatsiini tekhnolohii — Metody ubezpechennia — Kryterii otsinennia bezpeky IT — Chastyna 2: Funktsionalni komponenty bezpeky: ISO/IEC 15408-2:2008 — ISO / IEC. — 2008-08-19; 2014-12-01 [Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components: ISO/IEC 15408-2: 2008 — ISO/IEC. — First edit. 2008-08-19; Last edit. 2014-12-01]. Mizhnarodna orhanizatsiia po standartyzatsii [International Organization for Standardization], 2008. III, 218 p. Mizhnarodnyi standart [International standard].
13. Informatsiini tekhnolohii — Metody ubezpechennia — Kryterii otsinennia bezpeky IT — Chastyna 3: Komponenty ubezpechennia: ISO/IEC 15408-2 2008 — ISO/IEC. — 2008-08-19; 2014-12-01. [Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components: ISO/IEC 15408-2:2008 — ISO/IEC. — First edit. 2008-08-19; Last edit. 2014-12-01]. Mizhnarodna orhanizatsiia po standartyzatsii [International Organization for Standardization], 2008. III, 174 p. Mizhnarodnyi standart [International standard].

A.Ia. Hladun, PhD in Engineering, Senior Researcher
K.O. Khala, Junior Researcher

TAXONOMY OF INFORMATION SECURITY STANDARDS

Abstract. *This paper presents a taxonomy (structural classification) of standards for information security (hereafter — IS), which represents a certain systematic analysis of standards both in terms of standard makers and from the point of view of designers and developers of secure systems. The taxonomy of standards provides a systematic approach of decomposition of general security management problems for solving specific problems.*

Key words: *information security, standard, авторизація, authentication, taxonomy.*

А.Я. Гладун, канд. техн. наук, с.н.с.
Е.А. Хала, м.н.с.

ТАКСОНОМИЯ СТАНДАРТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Резюме. *В статье рассмотрена таксономия (структурная классификация) стандартов ИБ, которая представляет определенный системный анализ стандартов как с точки зрения их разработчиков, так и проектировщиков и разработчиков защищенных систем. Таксономия стандартов обеспечивает применение системного подхода декомпозиции общей проблемы управления безопасностью к решению частных задач.*

Ключевые слова: *информационная безопасность, стандарт, авторизация, аутентификация, таксономия.*

ІНФОРМАЦІЯ ПРО АВТОРІВ

Гладун Анатолій Ясонович — канд. тех. наук, с.н.с. Міжнародного науково-навчального центру інформаційних технологій та систем НАН та МОН України, пр-т Акад. Глушкова, 40, м. Київ, Україна, 03680; (044) 502-63-66; glanat@yahoo.com; ORCID: 0000-0002-4133-8169
Хала Катерина Олександрівна — м.н.с. МННЦІТС НАН та МОН України, пр-т Акад. Глушкова, 40, м. Київ, Україна, 03680; (044) 502-63-66; cecerongreat@ukr.net; ORCID: 0000-0002-9477-970X

INFORMATION ABOUT THE AUTHORS

Hladun A.Ia. — PhD in Engineering, Senior Researcher, International Research and Training Center for Information Technologies and Systems under NAS and MES of Ukraine, 40, Acad. Glushkova Ave., Kyiv, Ukraine, 03680; +38(044) 502-63-66; glanat@yahoo.com; ORCID: 0000-0002-4133-8169
Khala K.O. — Junior Researcher, IRTCITS under NAS and MES of Ukraine, 40, Acad. Glushkova Ave., Kyiv, Ukraine, 03680; +38(044) 502-63-66; cecerongreat@ukr.net; ORCID: 0000-0002-9477-970X

ИНФОРМАЦИЯ ОБ АВТОРАХ

Гладун А.Я. — канд. техн. наук, с.н.с. Международного научно-учебного центра информационных технологий и систем НАН и МОН Украины, пр-т Акад. Глушкова, 40, г. Киев, Украина, 03680; +38(044) 502-63-66; glanat@yahoo.com, ORCID: 0000-0002-4133-8169
Хала Е.А. — м.н.с. МНУЦИТС НАН и МОН Украины, пр-т Акад. Глушкова, 40, г. Киев, Украина, 03680; +38(044) 502-63-66; cecerongreat@ukr.net; ORCID: 0000-0002-9477-970X

УДК 681.330.888

О.Й. Рішан, канд. техн. наук, доцент
А.С. Гура, магістрант

РОЗРОБКА СТРУКТУРНОЇ СХЕМИ ТА СПОСОБУ ПІДВИЩЕННЯ ТОЧНОСТІ ВИМІРЮВАНЬ УЛЬТРАЗВУКОВОГО ПРИСТРОЮ КОНТРОЛЮ ШИРИНИ СТРІЧКИ У ПОВІТРІ

Резюме. *У статті наведені результати розробки та дослідження способу підвищення точності вимірювань при реалізації ультразвукового тіньового методу в пристрої контролю ширини стрічкових напівфабрикатів у повітрі. Особливістю використання тіньового методу в повітрі є неізольованість акустичних зон первинних вимірювальних перетворювачів ширини (ПВПШ) пристрою від навколишнього середовища і відповідно вплив цього середовища на зони вимірювання, який проявляється в зміні інтенсивності ультразвукових коливань на вимірювальних приймачах при постійній ширині стрічки і, відповідно, зміні вихідних сигналів приймачів і збільшенні похибки вимірювання. Оцінено додаткові складові похибки: випадкова похибка флуктуації, яка виникає при зміні швидкості повітряних потоків (турбулентність) в акустичній зоні вимірювання положення краю стрічки та похибка від впливу зміни температури в акустичній зоні вимірювання. Для зменшення додаткових складових основної похибки вимірювання при тіньовому методі розроблений спосіб їх компенсації, що реалізується в ПВПШ пристрою за допомогою додаткового приймача коригування, який розташований поряд із вимірювальним приймачем і в одній площині з ним, але не перекривається краєм стрічки, і введенням сигналу цього додаткового приймача в ланцюг від'ємного зворотного зв'язку регулювання напруги живлення пакета випромінювачів, завдяки чому цей сигнал підтримується незмінним і рівним заданому.*

Ключові слова: *ультразвуковий тіньовий метод вимірювання ширини стрічки у повітрі, неізольованість акустичних зон вимірювання від навколишнього середовища, додаткові складові основної похибки вимірювання, приймач коригування.*

ПОСТАНОВКА ПРОБЛЕМИ

Для вимірювання ширини стрічкових напівфабрикатів у повітрі, які можуть бути або оптично прозорими, або легко піддаватись деформуванню, наприклад, листи для пакування виробів у харчовій промисловості тощо, досліджено ультразвуковий тіньовий диференціальний метод [1].

Головною умовою реалізації такого методу є необхідність великої різниці між акустичними