УДК 35.078

Н. Б. Мєзєнцева,
кандидат наук з державного управління,
старший науковий співробітник військової частини А1906

ІНТЕГРАЦІЯ УКРАЇНИ В ЄВРОПЕЙСЬКІ СИСТЕМИ В АСПЕКТІ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

У статті розглядається роль інформаційних технологій та IT-стандартизації в контексті інтеграції України в європейські системи. Проаналізовані складові інформаційної безпеки, досліджені питання гармонізації українського законодавства в галузі інформаційних технологій з відповідними стандартами Європейського Союзу.

In the article the role of information technologies and IT-standardization in the context of integration of Ukraine is examined in the European systems. The constituents of informative safety are analysed, investigational questions of harmonization of the Ukrainian legislation in industry of information technologies with the proper standards of European Union.

Ключові слова: інформаційний простір, інформаційні ресурси, інформаційна інфраструктура, інформаційні технології, інформаційна безпека.

Key words: informative space, informative resources, informative infrastructure, information technologies, informative safety.

ВСТУП

Сучасні умови глобальної світової інтеграції призводять до жорсткої міжнародної конкуренції в інформаційному просторі та підвищують роль IT-стандартизації. Інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології значною мірою визначають рівень і темпи соціально-економічного, науково-технічного і культурного розвитку держави.

Побудова високотехнологічного виробництва, надання послуг, керування державою тощо у сучасному світі неможливі без застосування передових IT-технологій. Такі досягнення України, як вступ в СОТ і зростання міжнародного авторитету українських IT-фірм, демонструють наявність потенціалу розвитку та зміцнення економіки України у XXI столітті, в якому інформаційні технології стали основою розбудови та процвітання нового суспільства — інформаційного.

МЕТА СТАТТІ

Метою даної статті є аналіз міжнародного досвіду стандартизації щодо сучасних інформаційних технологій та виявлення особливостей і проблем використання цього досвіду в Україні.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

У контексті інтеграції України в європейські системи доцільно розглянути аспект інформаційних технологій як основоположних інструментів сучасної взаємодії, оскільки саме Україні необхідно адаптувати свої стандарти до вимог ЄС.

Українські дослідники питань транскордонної взаємодії, зокрема в сфері інформаційних технологій, О.Л. Перевозчикова, А.О. Мелащенко для уникнення проблем, переважно пов'язаних із втратою ресурсів (часу, кадрів, коштів), наголошують на необхідності концентрації зусиль на гармонізації стандартів ЄС у прикладних сферах та інших різновидів міжнародних стандартів у міжгалузевих сферах.

Звертаючись у зазначеній проблематиці до міжнародного досвіду, потрібно відзначити на загальноєвропейському рівні роботу об'єднаного комітету із IT-стандартизації JTC 1 ISO/IEC, який розробив найбільшу кількість IT-стандартів. Детальніший аналіз засвідчує, що основна кількість розроблених IT-стандартів припадає на 2006—2009 роки. Важливо також констатувати міждисциплінарний характер інформаційних технологій та їх поширення у всіх без винятку сферах людської діяльності. У зв'язку з цим IT потребують загальновизнаних процедур інновацій, зокрема стандартизації.

Зауважимо, що в європейських країнах із чинними міжнародними стандартами працюють технічні комітети європейських інституцій стандартизації (ETSI, CEN/CENELEC тощо). Таким чином, саме в прикладних сферах сконцентровано специфіку реалізації, через це серед європейських стандартів немає гармонізованих за "правилами IDT", здебільшого застосовними в Україні, з іншими міжнародними стандартами.

Але серед європейських відсутні стандарти оцінювання якості програмного продукту, мережної безпеки, безпеки систем, подання даних тощо, тобто в Євросо-

юзі використовують міжнародні фундаментальні методики та практики, загальні для ІТ.

В Європейському Союзі загалом ІТ-стандартизацію розглядають через вимоги набору Директив, які напряму впливають на гармонізацію локального законодавства країн-членів ЄС. ІТ-стандарти є спільними для всіх країн-членів. Нині в Україні щодо ІТ чинні наступні Директиви Євросоюзу:

1) Директива 95/46/ЄС про захист даних (стаття 17);

2) Директива 1999/93/ЄС про комунікаційне середовище електронних підписів;

3) Директива 2002/21/ЄС про пакет комунікаційного середовища;

4) Директива 98/34/ЄС про процедури надання інформації щодо технічних стандартів і норм;

5) Директива 2001/115/ЄС про спрощення, модернізацію й гармонізацію умов, установлених для виставлення рахунку на ПДВ;

6) Директива 2003/58/ЄС, що виправляє Директиву 68/151/ЕЄС;

7) Директива 2003/127/ЄС, що виправляє Директиву 1999/37/ЄС про реєстраційні документи транспортних засобів;

8) Директива 2006/43/ЄС про встановлений законом аудит річних звітів і консолідованих рахунків;

9) Директива 2004/17/ЄС з координації закупочних процедур на обробку сутностей у секторах води, енергії, транспорту і поштових послуг;

10) Директива 2005/51/ЄС, що виправляє Додатки XX і VIII Директиви 2004/17/ЄС;

11) Директива 2004/18/ЄС з координації процедур оплати публічних контрактів на роботи, постачання та послуги;

12) Директива 2009/72/ЄС про спільні правила внутрішнього ринку електрики і відміняє Директиву 2003/54/ЄС;

13) Директива 2009/73/ЄС про спільні правила внутрішнього ринку природнього газу і відміняє Директиву2003/55/ЄС;

14) Директива 2006/123/ЄС про послуги на внутрішньому ринку.

Стосовно технічної регламентації інформаційної безпеки, необхідно звернути увагу на міжнародний стандарт "інформаційна безпека — збереження конфіденційності, цілісності та доступності інформації". Крім того, у міжнародній практиці прийнято враховувати такі властивості інформації, як автентичність, підзвітність, неспростовність та надійність.

Конфіденційність — властивість, яка гарантує, що інформація недоступна або не розкрита неавторизованим особам, суб'єктам або процесам.

Цілісність — властивість захисту точності та повноти активів.

Доступність — властивість інформації, що дає можливість використовувати її на вимогу авторизованого суб'єкта.

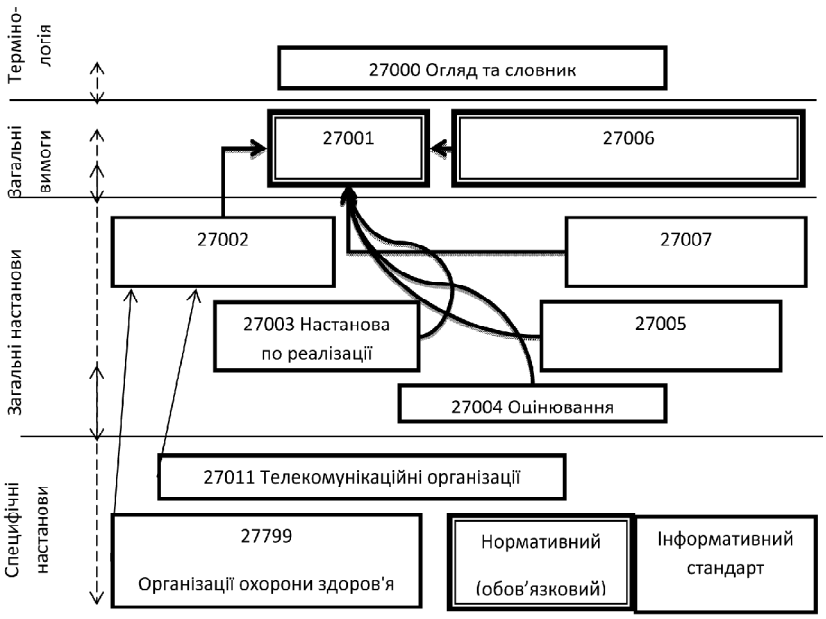

Рис. 1. Взаємозв'язок між стандартами ISMS

Автентичність — властивість, яка гарантує, що суб'єкт є тим, ким він / вона заявлені.

Підзвітність — відповідальність суб'єктів за свої дії та рішення.

Неспростовність — можливість довести виникнення заявлених подій або дій та осіб, які породили їх, з метою вирішення суперечок про виникнення або не виникнення певних подій та участь суб'єктів у цих подіях.

Надійність — властивість передбачуваних послідовностей поведінки і результатів" [9].

Фактично інформаційну безпеку можна розділити на дві складові:

1) організаційну складову легко уявити як модель для створення, впровадження, експлуатації, моніторингу, аналізу, підтримки та покращення захисту інформаційних активів для досягнення бізнес-цілей, заснованих на оцінці ризиків та допустимих організацією рівнів ризиків, призначених для ефективної обробки та управління ризиками;

2) технологічна складова гарантує надійну та якісну реалізацію визначених функцій безпеки, точніше функцій, які використовуються для досягнення встановлених вимог безпеки.

Організаційна складова інформаційної безпеки. ISMS (Information Security Management System) — модель для створення, впровадження, експлуатації, моніторингу, аналізу, підтримки та покращення захисту інформаційних активів для досягнення бізнес-цілей, заснованих на оцінці потенційних загроз і допустимих ризиків, призначених для ефективної обробки та управління ризиками. Аналіз вимог щодо захисту інформаційних ресурсів та застосування відповідних заходів контролю для забезпечення захисту цих інформаційних ресурсів за потреби реалізується в ISMS.

Основоположні принципи, які сприяють успішній реалізації ISMS:

а) усвідомлення необхідності захисту інформації;

б) покладання відповідальності за інформаційну безпеку;

в) включення зобов'язань керівництва та інтересів зацікавлених сторін;

г) зміцнення соціальних цінностей;

д) оцінка ризику призначення відповідних контрольних заходів для досягнення прийнятного рівня ризику;

е) заходи безпеки, визначені в якості найважливіших елементів інформаційних мереж і систем;

г) активне попередження та виявлення інцидентів інформаційної безпеки;

д) забезпечення комплексного підходу до управління інформаційною безпекою;

ж) постійний перегляд ризиків інформаційної безпеки та створення модифікації (за необхідності).

Сімейства ISMS-стандартів складають взаємопов'язані стандарти, чинні (вже опубліковані) або на стадії розробки, і містять ряд суттєвих структурних компонентів, орієнтованих на норми стандартів, що описують відповідність СУІБ вимогам (ISO / IEC 27001) та органу з сертифікації вимог (ISO/IEC 27006) для тих, що засвідчують відповідність з ISO/IEC 27001. Інші стандарти мають забезпечити керівництво з різних аспектів реалізації СУІБ, звертаючись по загальним процесам, пов'язаним з контролем над керівними принципами, а також галузеві керівництва. Відносини між сім'єю СУІБ стандартів показані на рис. 1.

Стандарти, які забезпечують пряму підтримку, — це докладні настанови та інтерпретація загальних процесів PDCA і вимог, зазначених в ISO/IEC 27001, це: ISO/IEC 27000, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005 і ISO/IEC 27007, ISO/IEC 27006 — вони описують вимоги до органів, що забезпечують сертифікацію ISMS. ISO/IEC 27011 та ISO 27799 описують конкретні сектори для застосування ISMS.

Сімейства ISMS-стандартів стосуються багатьох інших ISO та ISO/IEC стандартів. Їх можна класифікувати наступним чином:

а) описові і термінологічні стандарти;

б) стандарти, що визначають вимоги;

в) стандарти, що описують загальні принципи;

г) стандарти, що описують галузеві настанови.

Технологічна складова інформаційної безпеки. Відповідний технічний стандарт ISO/IEC 15408-1 підготував Підкомітет SC 27 "Інформаційні технології. Методи IT-захисту" Об'єднаного технічного комітету ISO/IEC JTC 1. Ідентичний текст ISO/IEC 15408 видано у рамках загального проекту підтримки критеріїв організацій як Загальні критерії оцінювання IT-безпеки. Загальне XML-джерело обох публікацій можна знайти в http://www.oc.ccn.cni.es/xml

Третій випуск замінив другий випуск ISO/IEC 15408-1:2005, який було технічно переглянуто і доопрацьовано. ISO/IEC 15408 складають три частини:

— Частина 1. Вступ і загальна модель;

— Частина 2. Функціональні компоненти безпеки;

— Частина 3. Компоненти гарантій безпеки.

ISO/IEC 15408 допускає еквівалентність результатів кількох незалежних оцінювань безпеки. Досягнення еквівалентності ISO/IEC 15408 забезпечує єдиний набір вимог для функцій безпеки IT-продуктів і оцінювання заходів, вжитих до цих IT-продуктів протягом оцінювання безпеки. IT-продукти можна реалізувати як апаратне, вбудоване або програмне забезпечення.

Процес оцінювання встановлює рівень довіри, що гарантує виконання вимог за допомогою наявності функцій безпеки в IT-продуктах і вжитих заходах до IT-продуктів. Результати оцінювання допомагають споживачам оцінити достатній рівень захищеності IT-продуктів. ISO/IEC 15408 використовується як настанова для розробки, оцінювання та придбання IT-продуктів з функціональністю безпеки.

ISO/IEC 15408 гнучкий, допускає використання набору методів оцінювання для множини властивостей безпеки набору IT-продуктів. Користувачі цього міжнародного стандарту повинні акуратно використовувати його гнучкість. Наприклад, використання ISO/IEC 15408 разом з некоректними методами оцінювання, недоцільними властивостями безпеки чи недоречними IT-продуктами може призвести до невірних результатів оцінювання.

Отже, факт оцінювання IT-продукту має значення тільки в контексті доведених властивостей безпеки та задіяних методів оцінювання. Органам оцінювання рекомендовано ретельно перевіряти продукти, властивості та методи для гарантії одержання значимих результатів. Також покупцям оцінених продуктів рекомендовано ретельно оцінити корисність оцінених продуктів для застосування їх у конкретних ситуаціях і потребах.

ISO/IEC 15408 сконцентровано на захисті активів від несанкціонованого розкриття, модифікації або неможливості використання. Ці категорії захисту зазвичай називають: конфіденційністю, цілісністю та доступністю. Також ISO/IEC 15408 застосовний до інших аспектів IT-безпеки. ISO/IEC 15408 можна використовувати для оцінювання людських ризиків (зловмисних або інших дій) і ризиків, не пов'язаних з діяльністю людини. Крім IT-безпеки, ISO/IEC 15408 застосовний в інших сферах IT.

Певні теми, через їхню специфічність або через слабкий зв'язок з IT-безпекою, перебувають поза сферою ISO/IEC 15408.

a) ISO/IEC 15408 не містить критерії оцінювання безпеки адміністративних заходів щодо безпеки, не пов'язаних безпосередньо з IT-функціями безпеки. Визнано, що значного рівня IT-безпеки можливо досягти за допомогою чи підтримуючи адміністративні заходи, наприклад, контроль організаційних, персональних, фізичних і процедурних факторів.

b) Не охоплено оцінювання таких техніко-фізичних аспектів IT-безпеки, як електромагнітне випромінювання, хоча багато понять застосовні до цієї сфери.

c) ISO/IEC 15408 не описує методологію оцінювання відповідності, у рамках якої необхідно застосовувати критерії. Цю методологію описано в ISO/IEC 18045.

d) ISO/IEC 15408 не враховує адміністративні та правові рамки, у яких будуть задіяні критерії органами з оцінювання відповідності. Однак передбачено, що ISO/IEC 15408 будуть використовувати для оцінювання в зазначених рамках.

e) Процедури використання результатів оцінювання відповідності для акредитації не регламентує

Таблиця 1. Перелік стандартів для створення Технічного регламенту ІТ-захисту

№	Номер стандарту	Назва стандарту	Потрібна дія
1.	ДСТУ ISO/IEC TR 13335-1:2004	Інформаційні технології. Посібник з управління безпекою інформаційних технологій. Частина 1. Управління та планування безпекою ІТ	Чинний, потребує перегляду
2.	ДСТУ ISO/IEC TR 13335-2:2004	Інформаційні технології. Посібник з управління безпекою інформаційних технологій. Частина 2. Управління та планування безпекою ІТ	Чинний, потребує перегляду
3.	ДСТУ ISO/IEC TR 13335-3:2004	Інформаційні технології. Посібник з управління безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій	Чинний, потребує перегляду
4.	ДСТУ ISO/IEC 11770-1:2006	Інформаційні технології. Методи захисту. Керування ключами. Частина 1. Середовище	Те саме
5.	ДСТУ ISO/IEC 11770-2:2006	Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми, базовані на використанні симетричних методів	Чинний, потребує перегляду
6.	ДСТУ ISO/IEC 11770-3:2006	Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми, базовані на використанні асиметричних методів	Чинний, потребує перегляду
7.	ISO/IEC 11770-4:2006	Information technology - Security techniques - Key management - Part 4: Mechanisms based on weak secrets	
8.	ISO/IEC 15408-1:2009	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model	С проект ДСТУ
9.	ISO/IEC 15408-2:2008	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components	Є проект ДСТУ
10.	ISO/IEC 15408-3:2008	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components	С проект ДСТУ
11.	ISO/IEC 18014-1:2008	Information technology - Security techniques - Time-stamping services - Part 1: Framework	Перегляд ДСТУ
12.	ISO/IEC 18014-2:2009	Information technology - Security techniques - Time-stamping services -- Part 2: Mechanisms producing independent tokens	Перегляд ДСТУ
13.	ISO/IEC 18014-3:2009	Information technology - Security techniques - Time-stamping services - Part 3: Mechanisms producing linked tokens	Перегляд ДСТУ
14.	ISO/IEC 18028-2:2006	Information technology - Security techniques - IT network security - Part 2: Network security architecture	
15.	ISO/IEC 18028-3:2005	Information technology -- Security techniques -- IT network security -- Part 3: Securing communications between networks using security gateways	
16.	ISO/IEC 18028-4:2005	Information technology -- Security techniques -- IT network security -- Part 4: Securing remote access	
17.	ISO/IEC 18028-5:2006	Information technology -- Security techniques -- IT network security -- Part 5: Securing communications across networks using virtual private networks	
18.	ISO/IEC 18031:2005	Information technology -- Security techniques -- Random bit generation	
19.	ISO/IEC 18032:2005	Information technology -- Security techniques -- Prime number generation	
20.	ISO/IEC 18033-1:2005	Information technology -- Security techniques -- Encryption algorithms -- Part 1: General	
21.	ISO/IEC 18033-2:2006	Information technology -- Security techniques -- Encryption algorithms -- Part 2: Asymmetric ciphers	
22.	ISO/IEC 18033-3:2005	Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers	
23.	ISO/IEC 18033-4:2005	Information technology -- Security techniques -- Encryption algorithms -- Part 4: Stream ciphers	
24.	ISO/IEC 27000:2009	Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary	
25.	ISO/IEC 27001:2005	Information technology -- Security techniques -- Information security management systems -- Requirements	
26.	ISO/IEC 27002:2005	Information technology -- Security techniques -- Code of practice for information security management	
27.	ISO/IEC 27004:2009	Information technology -- Security techniques -- Information security management – Measurement	
28.	ISO/IEC 27005:2008	Information technology -- Security techniques -- Information security risk management	
29.	ISO/IEC 27006:2007	Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems	
30.	ISO/IEC 27011:2008	Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	
31.	ДСТУ ISO/IEC 13335-1:2004	Інформаційні технології. Методи захисту. Керування інформацією й безпекою технології комунікацій. Частина 1. Поняття й моделі для інформації й керування безпекою технології комунікацій	Чинний
32.	ДСТУ ISO/IEC 15946-1:2008	Інформаційні технології. Методи захисту. Криптографічні методи, засновані на еліптичних кривих. Частина 1. Загальні положення	Чинний
33.	ДСТУ ISO/IEC 9798-1:1997	Інформаційні технології. Методи. Автентифікації сутності. Частина 1. Загальні положення	Чинний
34.	ДСТУ ISO/IEC 9798-3:1998	Інформаційні технології. Методи захисту. Автентифікація сутності. Частина 3. Механізми , що використовують методи цифрового підпису	Чинний

ISO/IEC 15408. Акредитація — адміністративний процес, який дозволяє органу акредитації використовувати ІТ-продукт (або набір продуктів), включаючи його не-ІТ-компоненти. Результати процесу оцінювання відповідності є передумовою процесу акредитації. Оскільки інші методи використовуються для оцінювання властивостей, які не стосуються ІТ-безпеки, таким чином їхнє співвідношення необхідно оцінювати окремо.

f) Оцінювання відповідності суб'єкта критерію властивостей криптографічних алгоритмів не охоплює ISO/IEC 15408. Застосовують незалежну оцінку математичних властивостей криптографії, схему оцінювання відповідності, яку використовує ISO/IEC 15408, щоб врахувати результат незалежного оцінювання.

Філософія стандарту ISO/IEC 15408 полягає в тому, що загрози безпеки та зобов'язання політики організаційної безпеки мають бути чітко сформульовані. А запропоновані заходи безпеки мають бути вочевидь достатніми для досягнення їхньої мети.

Окрім зазначеного, необхідно вжити заходів, які зменшують імовірність уразливості. Додатково необхід-

но вжити заходів, які полегшують наступну ідентифікацію уразливості.

Філософія ISO/IEC 15408 має за мету забезпечити гарантії, базовані на оцінюванні (активному дослідженні) ІТ-продукту, якому потрібно довіряти. Оцінювання було традиційним засобом забезпечення гарантій і підставою для попередніх висновків про критерії оцінювання. У ISO/IEC 15408 запропоновано визначати законність висновків отриманих на ІТ-продукт досвідченим оцінювачам з акцентом на сфері застосування, глибині та суворості.

ISO/IEC 15408 не виключає й не коментує відносні переваги інших засобів отримання гарантій. Дослідження триває щодо альтернативних способів одержання гарантій.

Значимість уразливості грунтується на передбаченні існування агентів загроз, які активно прагнуть порушити політику безпеки для отримання незаконного прибутку або здійснення інших хибних намірів, і це — небезпечні дії. Агенти загроз можуть також випадково викликати уразливість безпеки, наносячи шкоду організації. Істотний ризик відмови ІТ виникає через потребу обробити важливу інформацію та брак придатних продуктів, яким достатньо довіряють. Тому цілком імовірно, що порушення правил ІТ-безпеки може призвести до суттєвих втрат.

Порушення правил ІТ-безпеки виникають внаслідок навмисних дій або ненавмисного виклику уразливості ІТ.

Таким чином, існує, необхідність здійснити заходи для запобігання уразливості, що виникає в ІТ-продуктах. Уразливість має бути:

a) усунутою — тобто необхідно вжити заходи, щоб показати й видалити або нейтралізувати всю заподіяну уразливість;

b) мінімізованою — тобто необхідно вжити заходи, щоб зменшити до прийнятного залишкового рівня потенційний вплив будь-якої шкоди;

c) перевіреною — тобто необхідно вжити заходи, щоб гарантувати, що будь-яка спроба заподіяти шкоду буде виявлена таким чином, щоб можна було здійснити дії для обмеження ушкоджень.

Уразливість може виникнути:

a) через нехтування вимогами безпеки, тобто ІТ-продукт може мати всі необхідні функції й особливості але містити уразливість, яка не може бути відповідним або ефективним способом усунута через скорочений обсяг вимог безпеки;

b) у результаті неякісної розробки, тобто ІТ-продукт не відповідає своїй специфікації або уразливість виникла в результаті неякісних стандартів розробки або неправильного вибору проекту;

c) у зв'язку з неправильним оперативним управлінням, тобто ІТ-продукт створено коректно за коректною специфікацією, але уразливість виникла в результаті неадекватного управління після операції.

Гарантії ISO/IEC 15408. Гарантія — підстави для впевненості, що ІТ-продукт забезпечує свої цілі безпеки. Гарантію можна одержати від посилання на такі джерела, як необгрунтовані твердження, що передують конкретному певному досвіду. Але ISO/IEC 15408 забезпечує гарантії через активне дослідження. Активне дослідження — оцінювання ІТ-продукту для визначення його властивостей безпеки.

Оцінювання є традиційним засобом одержання гарантій і підставою ISO/IEC 15408 підходу.

Методики оцінювання можуть включати, але не обмежуються наступним:

a) аналіз і перевірка процесу(ів) і процедур;

b) перевірка застосованих процесу(ів) і процедур;

c) аналіз відношення між поданням проекту TOE;

d) аналіз спроектованого подання TOE відносно вимог;

e) перевірка доказів;

f) аналіз документів настанов;

g) аналіз функціональних тестів розробника й наданих результатів;

h) незалежне функціональне тестування;

i) аналіз уразливості (включаючи гіпотезу недоліків);

j) тестування проникнення.

ВИСНОВКИ

Зазначені стандарти мають фундаментальний характер. Вони є визнаним міжнародним співтовариством ІТ-базисом.

Здебільшого ІТ-стандарти потребують гармонізації, оскільки застосовуватимуться у судових розглядах як джерело норм, правил, еталонів, зразків і вимог до якості ІТ-продуктів, що потенційно могли нанести шкоду чи матеріальні збитки. Щоб пересічний суддя міг скористатися нормами цих стандартів, за законодавством України вони мають бути викладені державною мовою.

Таким чином, нижче наведений перелік стандартів, що в сукупності могли б скласти Технічний регламент ІТ-захисту, рекомендований для прийняття в Україні.

Література:

1. Конституція України.

2. Директива 1999/93/ЄС Європарламента й Ради від 13 грудня 1999 р. про комунікаційне середовище електронних підписів.

3. Закон України від 01.12.2005 № 3164 "Про стандарти, технічні регламенти та процедури оцінки відповідності".

4. Мелащенко А.О., Перевозчикова О.Л. Кроссертификация Украины // Проблеми програмування. — 2010. — № 2—3. — С. 299—307.

5. Закон України від 22.05.2003 № 852-15 "Про електронний цифровий підпис".

6. Директива 2002/21/ЄС Європарламенту і Ради про спільні правові рамки для електронних комунікаційних мереж та послуг.

7. Баховець О.Б., Грінченко Т.О., Гуляєв К.Д., Полумієнко С.К., Рибаков Л.О., Тюрин В.В. Передумови становлення інформаційного суспільства в Україні / за ред. Довгого С.О. — К.: Азимут-Україна, 2008. — 205 с.

8. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевіряння.

9. ISO/TS 15000:2004 Electronic business eXtensible Markup Language (ebXML) (у 5-ти частинах).

Стаття надійшла до редакції 04.02.2013 р.