$y_3^o = 0;$

Отже, при використанні цільової функції (2) і співвідношенні $g_1 : g_2 : g_3 = 0{,}5 : 0{,}3 : 0{,}2$; у випадку, коли напад здійснюється на один з об'єктів і імовірності цих подій як і імовірності виділення нападом ресурсів $z = 1, z = 2, z = 3$ однакові, оптимальний розподіл ресурсів захисту становить $y_1^o : y_2^o : y_3^o = 0{,}87 : 0{,}13 : 0$; у випадку коли напад розподіляє свої ресурси порівну і імовірності виділення нападом ресурсів $z = 1, z = 2, z = 3$ однакові $y_1^o : y_2^o : y_3^o = 0{,}55 : 0{,}45 : 0$; якщо ж останні імовірності співвідносяться як 0,8: 0,15: 0,05 (оцінки експертів), то $y_1^o : y_2^o : y_3^o =$ $= 0{,}64 : 0{,}36 : 0$. Цей результат, очевидно, можна вважати остаточним.

Список літератури

1. Левченко Є.Г. Оптимізація розподілу ресурсів між об'єктами захисту інформації. – К.: НТЖ «Захист інформації», №1, 2007.

2. Гуткин Л.С. Оптимизация радиоэлектронных устройств. М.: Радио, 1975.

3. Левченко Є.Г., Рабчун А.О. Модель Гросса в протистоянні двох сторін у сфері захисту інформації. – НТЖ «Захист інформації», №3, 2009.

Надійшла 12.02.09

УДК 342.738

Хорошко В.О., Артемов В.Ю.

ОКРЕМІ АСПЕКТИ ВПРОВАДЖЕННЯ МІЖНАРОДНИХ СТАНДАРТІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СПЕЦІАЛЬНИХ СЛУЖБАХ УКРАЇНИ

Перехід до системи демократичних цінностей і відкритого суспільства, європейська та євроатлантична спрямованість України примушують державу та суспільство звертатися до системи міжнародних стандартів у такій делікатній галузі як безпека.

При цьому безпека розуміється в широкому сенсі – це і безпека держави, це і безпека особистості, це і безпека суспільної організації держави, це і безпека міждержавних об'єднань, таких як ЄС та НАТО.

До проблеми міжнародного співробітництва в галузі стандартизації зверталися такі відомі зарубіжні та вітчизняні науковці як Асландер Робертс, Олександр Бакалінський, Володимир Галатенко, Володимир Бетелін, Сергій Климчук, Павло Куберт, Віталій Безштанько, Василь Цукран та ін.

Метою даної статті є аналіз міжнародного стандарту з інформаційної безпеки ISO 27001 та його впровадження в спеціальних службах нашої держави.

Чому саме цей стандарт з інформаційної безпеки потрібен спецслужбам? Тому, що інформація стає не лише сферою професійної діяльності мільйонів людей ще тому, що не вугілля, залізо та нафта, а саме вона постійно перетворюється в основне загальнолюдське багатство.

Безумовно, жодне суспільство не може існувати без законодавства та нормативних документів, які регламентують правила, процеси, методи виготовлення і контролю якості товарів, робіт та послуг, а також гарантують безпеку життя, здоров'я і майна людей та навколишнього середовища. Стандартизація якраз і є тією діяльністю, яка виконує ці функції.

Стандартизація - діяльність, що полягає у встановлення положень для загального і багаторазового застосування щодо наявних чи можливих завдань з метою досягнення

оптимального ступеня впорядкування у певній сфері, результатом якої є підвищення ступеня відповідності продукції процесів та послуг їх функціональному призначенню, усуненню бар'єрів у торгівлі і сприянню міжнародному співробітництву.

Відносини, пов'язані з діяльністю у сфері стандартизації та застосування її результатів, регулюються Законом України "Про стандартизацію" від 17.05.01 [1]. Цей Закон встановлює правові та організаційні засади стандартизації в Україні спрямований на забезпечення єдиної політики у цій сфері.

Об'єктом стандартизації є продукція, процеси та послуги, зокрема матеріали, складники. обладнання, системи, їх сумісність, правила, процедури, форми методи чи діяльність.

Метою стандартизації в України є забезпечення безпеки життя та здоров'я людини, тварин, рослин, а також майна та охорони довкілля, створення умов для раціонального використання всіх видів національних ресурсів та відповідності об'єктів стандартизації своєму призначенню, сприяння усуненню технічних бар'єрів у торгівлі [1].

Державна політика у сфері стандартизації базується на таких принципах:

- забезпечення участі фізичних і юридичних осіб в розробленні стандартів та у вільному виборі ними видів стандартів при виробництві чи постачанні, продукції;
- відкритості та прозорості процедур розроблення і прийняття стандартів з урахуванням інтересів усіх зацікавлених сторін, підвищення конкурентоспроможності продукції вітчизняних виробників;
- доступності стандартів та інформації щодо них для користувачів;
- відповідності стандартів законодавству;
- адаптації до сучасних досягнень науки і техніки з урахуванням стану національної економіки;
- пріоритетності прямого впровадження в Україні міжнародних та регіональних стандартів;
- дотриманні міжнародних та європейських правил і процедур стандартизації;
- участі у Міжнародній (регіональній) стандартизації.

Суб'єктами стандартизації є:

- центральний орган виконавчої влади у сфері стандартизації;
- рада стандартизації;
- інші суб'єкти, що займаються стандартизацією.

Залежно від рівня суб'єкта стандартизації, який приймає чи схвалює стандарти, розрізняють:

- національні стандарти, кодекси усталеної практики та класифікатори, прийняті чи схвалені центральним органом виконавчої влади у сфері стандартизації, видані ним каталоги та реєстри загальнодержавного застосування;
- стандарти, кодекси усталеної практики та технічні умови, прийняті чи схвалені іншими суб'єктами, що займаються стандартизацією.

Застосування стандартів чи їх окремих положень є обов'язковим:

- для всіх суб'єктів господарювання, якщо це передбачено в технічних регламентах чи інших нормативно-правових актах;
- для учасників угоди (контракту) щодо розроблення, виготовлення чи постачання продукції, якщо в ній (ньому) є посилання на певні стандарти;
- для виробника чи постачальника продукції, якщо він склав декларацію про відповідність продукції певним стандартам чи застосував позначення цих стандартів у її маркуванні;
- для виробника чи постачальника, якщо його продукція сертифікована щодо дотримання вимог стандартів [1].

Міжнародні стандарти та стандарти інших країн, якщо їх вимоги не суперечать законодавству України, можуть бути застосовані в Україні в установленому порядку шляхом посилання на них у національних та інших стандартах. Таким чином виникає питання, що ж таке ISO? Це міжнародна організація зі стандартизації, котра була створена в 1947 році, штаб-квартира в Женеві. Першочерговою її метою було створення лише систему стандартів, яка б сприяла міжнародній торгівлі. Більшість країн світу мають національні представництва та національні комітети в ISO. ISO не працює наодинці. В своїй діяльності вона взаємодіє з іншими міжнародними організаціями зі стандартизації. В галузі інформаційної безпеки такої організацією є для неї МЕК – Міжнародна електротехнічна комісія, котра була створена ще в 1906 р., метою її є встановлення міжнародних стандартів у всіх галузях, пов'язаних з електрикою, електронікою та радіотехнікою.

Саме з цієї причини правильним та повною назвою нашого стандарту є **ISO/IEC 27001 Information Security Management Standard,** тобто стандарт ІСО та МЕК з управління інформаційною безпекою.

ISO взаємодіє не лише з міжнародними спеціалізованими організаціями в галузі стандартизації, але й з найбільшими національними. Із цієї причини наш стандарт виник не на порожньому місці - він розроблений на основі британського стандарту BS 7799, що призначений для управління інформаційною безпекою організації незалежно від її сфери діяльності.

Даний стандарт припускає, що служба безпеки, ІТ-відділ (відділ інформаційних технологій), керівництво компанії повинно працювати відповідно до загального регламенту, незалежно від того, чи мова йде про захист паперового документообігу або електронних даних.

В останні кілька років ISO 17799, а потім і 27001 почали упевнено просуватися по країнах СНД. У Республіці Бєларусь із 1 листопада 2004 р. став національним державним стандартом. У Молдові, завдяки позиції Національного Банку, всі банки з 2003 року проходять регулярну перевірку на відповідність ISO.

У Росії стандарти безпеки ISO перевтілений в держстандарт, прийняття Держстандарту 17799 відбулося в 2006 році.

Сьогодні стандарт ISO 27001 міцно ввійшов у наше життя, ставши на практиці де-факто стандартом побудови систем управління інформаційною безпекою провідних компаній як в Європі та Азії, так і в країнах СНД. До 2005 року навчальний курс розроблений підприємством Digital Security був єдиний у СНД курсом з цього стандарту. Вартість навчання на цих курсах з від 1000 до 2000 доларів США. До теперішнього часу в країнах СНД пройшло навчання кілька тисяч фахівців різних компаній, при цьому курс неодноразово проводився в таких містах як Київ, Дніпропетровськ, Одеса, Кишинів, Рига, Таллінн, Алмати, Ташкент, Москва.

Цікавим було б розглянути (хоча б загалом) історію стандартів безпеки ISO.

У середині 90-х років Британський інститут стандартів (BSI) за участі комерційних організацій, таких як Shell, National Westminster Bank, Midland Bank, Unilever, British Telecommunications, Marks & Spencer, Logica та ін., зайнявся розробкою стандарту управління інформаційною безпекою, та в 1995 р. був прийнятий національний британський стандарт BS 7799 з управління інформаційною безпекою та її організації незалежно від сфери її діяльності. Перша частина стандарту носила рекомендаційний характер. Друга частина була призначена для сертифікації та містила частину обов'язкових вимог, що не входили в першу частину.

Як і будь-який національний стандарт BS 7799 у період 1995-2000 користувався помірною популярністю лише в рамках країн британської співдружності [2].

Наприкінці 1999 експерти міжнародної організації зі стандартизації ISO прийшли до висновку, що в рамках існуючих стандартів ISO відсутній спеціалізований стандарт

управління інформаційною безпекою. Відповідно, ISO було ухвалене рішення не починати розробку нового стандарту, а за узгодженням із британським інститутом стандартів, взявши за базу BS 7799:1, прийняти стандарт ISO 17799.

Відповідно 2000 рік вдихнув нове життя в BS 7799:1, ставши ISO 17799, одержав вже статус міжнародного стандарту, що кардинально змінило розміщення сил і відношення до стандарту (між локальним і міжнародним стандартом різниця очевидна).

Що ж стосується офіційної сертифікації по ISO 17799, то вона споконвічно не була передбачена (повна аналогія з BS 7799). Була передбачена тільки сертифікація по BS 7799:2, що являв собою низку обов'язкових вимог (не ввійшли в першу частину BS 7799/ISO 17799). Процедура сертифікації по ISO повинна була з'явитися тільки після виходу в рамках ISO стандарту аналога BS 7799:2 (відзначимо, що це трапилося тільки наприкінці 2005 року з виходом сертифікаційного стандарту ISO 27001).

При цьому в Англії була передбачена стандартна процедура сертифікації по BS 7799:2 така ж, як і для всіх інших стандартів ISO. Сертифікатом (компанія, що спеціалізується на сертифікації за різними стандартами від ISO 9001 до ISO 14001, обов'язково акредитована при UKAS (англійська асоціація по стандартизації), наприклад BSI, TUV, URS, DNV й ін.) не має право готовити компанії до сертифікації: цим займаються партнери - незалежні консультанти. У свою чергу консультант не має право займатися сертифікацією.

Лютий 2002 року можна сміливо називати відправною точкою розвитку стандарту ISO 17799 у країнах СНД. У середині 2001 року у світі розпочалася непроста ситуація в галузі стандартизації з інформаційної безпеки. Існували різні стандарти, застосування яких на практиці викликало питання та серйозні сумніви. Крім того, у більшості фахівців переважав винятково технологічний підхід до захищеності (тобто визнавалися лише технічні методи захисту). І питанням організаційно-правового управління безпеці приділялася мінімальна увага. Однак у вузького кола фахівців було сприйняття, що винятково технологічний підхід до захисту інформації - це шлях у нікуди, це ще далеко не все. Тому з'явилося, нарешті, розуміння, що нам всім життєво необхідно ще виробити якийсь єдиний підхід до того, що тепер називається системою управління інформаційною безпекою. І тут у пригоді стає саме ISO 17799, який спеціалізується саме в питаннях управління інформаційною безпекою і став тим відсутньою ланкою, якої так не вистачало на практиці [3].

До кінця 2002 року кількість компаній у світі, що мали сертифікат BS 7799, було приблизно близько 150.

Ставлення фахівців в вітчизняних спецслужбах й більшості фахівців-практиків з безпеки у нашій країні як і у всіх країнах СНД до стандарту в той час, втім як і тепер, визначалося однією фразою: "Ми до цього ще не доросли".

Але незабаром ситуація повністю зміниться, зокрема 2011-20012 років можна назвати роком початку експонентного зросту інтересу фахівців з безпеки бізнесу до стандартів управління безпекою саме в ISO.

Найцікавішою подією 2008 року в СНД стало те, що саме тоді Національний Банк України почав на практиці застосовувати вимоги стандарту, поставивши за обов'язок всім місцевим банкам виконувати його вимоги, створюючи систему управління інформаційною безпекою на основі стандартів безпеки ISO.

Число компаній у світі, що одержали офіційний сертифікат - більше 10 000! Велика увага на трикратний приріст числа сертифікованих компаній в 2009 році - цей рік став тим роком, що показав тенденцію загального практичного інтересу до стандарту у світі й країнах СНД.

Буквально вибуховий інтерес учасників ринку країн СНД до стандарту. Росія, Казахстан, Молдова, Узбекистан, Україна - стандарт став повсюдно застосовуватися на

практиці (або прийшло усвідомлення необхідності його застосування як кращої світової практики).

Вийшла нова значно розширена в порівнянні з 2005 роком редакція стандарту ISO 27001.

Який же висновок? Сьогодні стало зовсім очевидно те, що було зовсім неочевидно ще наскільки років тому - стандарт ISO 27001, заснований на аналізі й управлінні ризиками, зайняв лідируючі позиції в Європі й Азії й став стандартом де-факто в побудові систем управління інформаційною безпекою.

Спостерігаючи за останні роки експонентний ріст інтересу до стандарту, мабуть, що в найближчі роки нас чекає підвищення інтересу як до застосування стандарту на практиці. Сьогодні ISO 27001 - це та об'єктивна реальність, що уже не має альтернативи. Аналіз і управління інформаційними ризиками, система управління інформаційною безпекою на основі ISO 27001 стали основною темою на всіх конференціях з інформаційної безпеки [2].

ISO/IEC 27001 стандарт був розроблений підкомісією по безпеці (SC 27) Об'єднаного Технічного Комітету з Інформаційній Технології (ISO/IEC JTC 1). Новий ISO/IEC 27001 заміняв попередню версію стандарту ISO/IEC 17799:2007, що є тепер застарілою. Основний зміст стандарту зберігся, але багато чого було повністю перероблене, щоб краще відповідати новим інформаційним загрозам і викликам безпеки. Крім того, додано новий розділ, що має назву "Управління інцидентами інформаційної безпеки".

Стандарт ISO/IEC 17799:2007 складався з 13 розділів:

1. Загальна частина
2. Терміни та визначення
3. Політика безпеки
4. Організаційні методи забезпечення інформаційної безпеки
5. Управління ресурсами
6. Користувачі інформаційної системи
7. Фізична безпека
8. Управління комунікаціями та процесами
9. Контроль доступу
10. Придбання, розробка та супровід інформаційних систем
11. Управління інцидентами інформаційної безпеки
12. Управління безперервністю ведення бізнесу
13. Відповідність вимогам

Кожен з розділів має наступну структуру:

Мета – вказує, яка мета повинна бути досягнута.

Управління – вказує, які цілі можуть бути досягнуті.

Керівництво – вказує, як управління може бути реалізовано.

Примітки – подаються корисні зауваження та пояснення.

Новий стандарт 27001 було скорочено майже вдвічі та він складається з 8 розділів. Основними з них є Відповідальність керівництва та Аудит. ISO/IEC 27001 призначений для використання будь-якою організацією (в тому числі і спеціальною службою), що припускає встановити систему ефективного інформаційного захисту або поліпшувати існуючі методи інформаційного захисту.

Разом з тим, все це означає, що всі рекомендації стандарту повинні бути безумовно прийняті в нашій державі та її спецслужбах. Все залежить від конкретних місцевих інформаційних ризиків та вимог.

Таким чином міжнародний стандарт ISO 27001 містить у собі рекомендації з управління інформаційною безпекою, призначені для співробітників, відповідальних за створення, впровадження й підтримку заходів, які забезпечують безпеку на державному підприємстві або недержавній організації. Рекомендації, наведені в проаналізованому

стандарті, слід виконувати з урахуванням діючих українських законів і нормативних вимог. Він повинен послужити основою для розробки стандартів безпеки й ефективних методів управління безпекою в конкретній організації. Крім того, даний стандарт допоможе підтримати взаємну довіру при контактах між українськими організаціями.

Список літератури

1. Законом України "Про стандартизацію" від 17.05.01р. // Правова база НАУ, версія 8.4.40.

2. В.Василюк, С.Климчук. Інформаційна безпека, К.,КНТ, 2008 р., - 190 с.

3. П.Куберт, В.Безштанько, В.Цукран. Международный стандарт ISO 17799. Информационные технологии – практические правила управления информационной безопасностью. // Бизнес и безопасность, № 3/2006 (53).

4. П.Куберт. Обеспечение безопасности при эксплуатации по ISO 17799. // Бизнес и безопасность, № 1/2007 (57).

5. Анализ международного стандарта ISO 15408 информационная технология, методі и средства. // Бизнес и безопасность, № 5/2007 (61).

6. В. Галатенко. Стандарты информационной безопасности., М., НИИСИ РАН, 2006, - 262 с.

Надійшла 12.01.09