УДК 004.056

ЕВОЛЮЦІЯ МЕТОДОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ НА ПРИКЛАДІ АНАЛІЗУ СТАНДАРТІВ БЕЗПЕКИ

О. Є. Архипов[1], Т. П. Теплицька[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

Розглянуто стандарти та нормативні документи присвячені забезпеченню інформаційної безпеки. У процесі дослідження було виділено дві основні гілки розвитку даних документів. Від «Помаранчевої книги» до «Загальних критеріїв» – перша гілка, стандарти для систем управління інформаційною безпекою – друга. Розглянуто нормативну базу українського законодавства у сфері інформаційної безпеки. Наведено характерні особливості зазначених документів та проведено аналіз розвитку стандартів по кожній із гілок.

Ключові слова: еволюція, стандарти, інформаційна безпека, ризик

Вступ

З розвитком інформаційних технологій, комп'ютерних мереж все більш актуальною стає проблема захисту інформаційних ресурсів, що обробляються у таких системах, адже втрата таких ресурсів організацією може стати причиною появи у ній фінансових проблем. Оскільки єдиним дієвим механізмом протидії загрозам інформаційної безпеки є вдало побудована система захисту інформації (СЗІ), виникає потреба формуванні вимог до такої системи. Для вирішення цього питання раціональним є дослідження стандартів інформаційної безпеки.

1. Розвиток перших стандартів у сфері інформаційної безпеки

Першим в історії оціночним стандартом в області інформаційної безпеки є документ під назвою «Критерії оцінки захисту комп'ютерної системи», більш відомий за назвою «Помаранчева книга». Стандарт, розроблений Міністерством оборони США в 1983 році, в першу чергу, спрямований на захист комп'ютерних систем військового призначення. Головне завдання даного документу полягало у оцінювання та класифікації комп'ютерних систем, що використовувались при зберіганні, обробці та розмежуванні доступу до інформації.

У критеріях пропонуються три категорії вимог безпеки – політика безпеки, аудит і коректність, в рамках яких сформульовані шість базових вимог безпеки: політика безпеки, мітки – в рамках політики безпеки; ідентифікація та автентифікація, реєстрація та облік – в рамках аудиту; контроль коректності функціонування засобів захисту, безперервність захисту – в рамках коректності [1].

Однією з головних особливостей «Помаранчевої книги» є проста для сприйняття та використання класифікація оцінюваних систем. В залежності від реалізованого ступеня захищеності система може бути віднесена до однієї з чотирьох груп, кожна з яких має від одного до трьох класів. Однак, такий підхід доцільно використовувати лише для оцінювання систем одного призначення.

Ще однією важливою особливістю TCSEC є введення поняття «диспетчер доступу» («монітор звернень»), що виконує роль посередника між суб'єктом та об'єктом при спробі першого отримати доступ до другого. Даний механізм в сукупності з іншими вимогами, що освітлені у критеріях, зосереджуються на питаннях збереження конфіденційності та частково цілісності інформації. Натомість питання доступності в даному стандарті майже не освітлюються, що є одним із головних його недоліків.

Одним із документів, для яких основою послугувала «Помаранчева книга», є «Європейські критерії безпеки інформаційних технологій», що були опубліковані у 1991 році. У даному документі, окрім збереження конфіденційності та цілісності, розглядаються питання забезпечення працездатності систем, реалізоване шляхом протидії загрозам, які ведуть до відмови в обслуговуванні.

Серед відмінностей «Європейських критеріїв» від TCSEC варто зазначити введення поняття адекватності засобів захисту, яка включає в себе їх ефективність та коректність, та використання класів-шаблонів замість єдиної універсальної шкали оцінювання рівня захищеності [2].

До введених шаблонів, окрім визначених у «Помаранчевій книзі», увійшли класи, призначені для оцінювання систем різного призначення: систем управління базами даних, систем управління технологічними процесами, розподілених систем обробки інформації. У даному стандарті кількість наведених класів-шаблонів дуже обмежена (лише 10 класів), що

виявилося недостатнім. Вирішенням цієї проблеми стало введення профілів захисту.

Вперше концепція профілю захисту застосовується у документі під назвою «Федеральні критерії безпеки інформаційних технологій». Згідно цього стандарту розроблення і аналіз профілів захисту є першим етапом розроблення продукту ІТ. Профіль захисту містить опис, обґрунтування, функціональні вимоги до реалізації засобів захисту продукту ІТ, вимоги до технології розроблення продукту ІТ, вимоги до процесу кваліфікаційного аналізу. У даному документі зазначено, що після розробки та аналізу профілю захисту повинні слідувати етапи розробки і кваліфікаційного аналізу ІТ-продуктів та компонування й сертифікація системи оброблення інформації. Однак у цьому документі належним чином розкрито лише перший етап, що стосується розробки профілю захисту.

В 1990 році Міжнародна організація зі стандартизації за участю Національниого інституту стандартів і технологій та Агентства національної безпеки (США), Установи безпеки комунікацій (Канада), Агентства інформаційної безпеки (Німеччина), Агентства національної безпеки комунікації) (Голландія), Органів виконання Програми безпеки і сертифікації, почали роботу над розробкою єдиних міжнародних критеріїв оцінки безпеки інформаційних технологій для загального використання. Даний документ було прийнято в 1999 році як міжнародний стандарт ISO 15408 «Загальні критерії оцінки безпеки ІТ». «Загальні критерії» були прийняті у 30 країнах світу.

«Загальні критерії» мають безліч переваг у порівнянні зі своїми попередниками, що детально описані у [3]. Вперше документ такого рівня містить розділи, адресовані споживачам, виробникам і експертам по кваліфікації ІТ-продуктів. На відміну від профілю захисту «Федеральних критеріїв», який орієнтований виключно на середу застосування ІТ-продукту, профіль захисту «Загальних критеріїв» призначений безпосередньо для задоволення запитів споживачів, пропонуючи для цього відповідні механізми (проект захисту), що дає можливість вибудувати на їх основі динамічну технологію створення безпечних інформаційних систем.

Особливу увагу цей стандарт приділяє адекватності реалізації функціональних вимог, яка забезпечується як незалежним тестуванням і аналізом ІТ-продукту, так і застосуванням відповідних технологій на всіх етапах його проектування і реалізації. Крім того, «Загальні критерії» розглядають гарантованість реалізації захисту як найважливіший компонент інформаційної безпеки і передбачають багатоетапний контроль на кожній стадії розробки ІТ-продукту, що дозволяє підтвердити відповідність отриманих результатів поставленим цілям. Таким чином, вимоги «Загальних критеріїв» охоплюють практично всі аспекти безпеки ІТ-продуктів і технології їх створення, а також містять всі вихідні матеріали, необхідні споживачам і розробникам для формування профілів захисту [3].

Однак, з моменту створення даного стандарту, окрім позитивних відгуків, у його адресу було проголошено і деяку критику. Так, у роботі [4] зазначено, що головними недоліками оцінювання систем за «Загальними критеріями» є довго тривалість такої оцінки та її надто висока вартість. Сертифікація по даному стандарту може тривати близько року, впродовж якого може бути розроблена нова версія системи, що також буде потребувати оцінювання[5]. До того ж процес оцінювання по «Загальним критеріям» переважно зосереджений на перевірці відповідної документації, що призводить до зменшення уваги до фактичних характеристик самого продукту [4]. Зважаючи на те, що в основі усіх сучасних стандартів, спрямованих на забезпечення інформаційної безпеки, лежить ризик-орієнований підхід, варто зазначити, що для розробки методики оцінки ризиків ІБ цей стандарт практично не використовується [6].

2. Розвиток стандартів для систем управління інформаційною безпекою

Найголовнішим стандартом в області управління інформаційною безпекою можна вважати BS 7799, адже саме цей документ покладено в основу сучасних ISO/IEC 27001[7], ISO/IEC 27002[8], ISO/IEC 27005[9]. У його першій частині – BS 7799 Part-1 «Практичні правила управління інформаційною безпекою», опублікованій у 1995 році, було описано 127 механізмів контролю, що необхідні для побудови системи управління інформаційною безпекою (СУІБ). У 1998 році було розроблено другу частину стандарту, що мала назву BS 7799 Part-2 «Системи управління інформаційною безпекою». В цьому документі було наведено перелік обов'язкових вимог для сертифікації. Згодом, в 1999 році, BS 7799 Part-1 та Part-2 було гармонізовано з міжнародним стандартом ISO 9001, в якому висунуто вимоги до систем менеджменту якості підприємств та організацій, з метою підвищення задоволеності споживача. Для цього в даному документі вводяться поняття внутрішнього аудиту, процесного підходу, коригувальних та запобіжних дій. У 2000 році першу частину BS 7799 було прийнято як міжнародний стандарт ISO 17799, а в 2005 році стандарт отримав назву ISO/IEC 27002 «Інформаційні технології. Методи забезпечення безпеки. Практичні правила управління інформаційною безпекою».

BS 7799 Part-2 у 2005 році було прийнято як міжнародний стандарт ISO/IEC 27001 «Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги»[7]. Застосування даного стандарту можливе для організацій різних сфер діяльності: телекомунікації, інформаційні технології, державні послуги, страхування і т.д. Стандарт містить перелік обов'язкових вимог для сертифікації. ISO/IEC 27001, як і ISO 9001, для постійного покращення системи управління ІБ застосовує цикл «Plan-Do-Check-Akt». Такий підхід дозволяє ввести модель для розробки, впровадження, функціонування, постійного моніторингу, аналізу,

підтримання в робочому стані і поліпшення СУІБ. У стандарті наведено огляд таких складових управління ІБ: політика безпеки, інформаційна структура безпеки, класифікація інформаційних ресурсів, фізична і зовнішня безпека, управління доступом, забезпечення безперервності бізнесу, відповідність вимогам законодавства. Згідно цього стандарту найважливішим компонентом СУІБ є підсистема управління ризиками. Саме на основі оцінки ризиків приймається більшість рішень щодо політики безпеки в організації. Варто зазначити, що навіть не всі заходи контролю з зазначеного вище переліку вимог є обов'язковими для успішної сертифікації по ISO/IEC 27001 у разі наявності документально підтвердженого рішення керівництва, заснованого на оцінці ризиків[10]. Таким чином, для відповідності стандарту найголовнішими вимогами є розуміння того, які інформаційні активи має організація, а також впровадження заснованого на оцінці ризиків рівня заходів контролю.

У 2005 році було випущено третю частину британського стандарту BS 7799 Part-3[11], в якому було розглянуто питання управління інформаційними ризиками. У даному стандарті поняття ризику сформульовано як комбінацію ймовірності події та її наслідків. Управління ризиками визначається як скоординовані безперевні дії з управління та контролю ризиків в організації. Цей стандарт розкриває основні етапи оцінки ризиків для системи управління ІБ, а саме:

- аналіз ризиків (інвентаризація активів організації та складання для кожного з них переліку значущих загроз та вразливостей у системі);
- оцінювання ризиків(допускається використання як кількісних, так і якісних методик оцінки ризиків);
- аналіз можливих заходів та засобів з мінімізації ризиків.

Усі перераховані вище етапи оцінки ризиків розкрито також у міжнародному стандарті ISO/IEC 27005 «Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки»[9], випущеному в 2005 році. Даний стандарт базується на міжнародному досвіді у сфері управління ризиками. Він прийшов на зміну міжнародним стандартам серії ISO/IEC 13335[12], що містить огляд загальних понять, настанов та моделей управління безпекою інформаційно-телекомунікаційних систем. В ISO/IEC 13335 запропоновано чотири підходи до аналізу ризику, що відрізняються деталізацією та глибиною проведеного аналізу. Ці підходи дозволяють підтримувати необхідний рівень балансу між точністю та трудомісткістю оцінки ризиків. Крім того, на зміст ISO/IEC 27005 вплинула розробка ISO/IEC 31000 «Ризик-менеджмент. Принципи та настанови», в бібліографічному переліку якого зазначено вищезгадану серію стандартів ISO 9000. ISO/IEC 31000 розкриває питання управління та контролю якістю у різних сферах діяльності, в тому числі і у сфері інформаційної безпеки.

Стандарт ISO/IEC 27005, як і вищезазначені ISO/IEC 27001 та ISO/IEC 27002, регламентує використання циклу «Plan-Do-Check-Akt». В стандарті зазначено, що одним із найважливіших етапів побудови системи управління ІБ є оцінка ризиків, можливих у конкретній СУІБ. Як вже зазначалось вище, у даному стандарті розкрито усі етапи проведення оцінки ризиків. Характерною особливістю для цього документу є надання організації права вільного вибору методики оцінки ризиків. Зазначається, що обрана методика повинна задовольняти переліку вимог, а саме: порівнюваність результатів з результатами інших методик, документованість та раціональність. При розробці методики оцінки ризиків ІБ доцільним є використання переліків активів, загроз, вразливостей, що містяться у додатках до стандарту.

2.1. Нормативна база українського законодавства в області інформаційної безпеки

Розглядаючи існуючу нормативну базу у сфері інформаційної безпеки в Україні варто звернути увагу на наступні документи: ДСТУ 3396.0-96[13], ДСТУ 3396.1-96[14], ДСТУ 3396.2-97[15], серія НД ТЗІ[16], [17], [18], [19], [20].

Зважаючи на доцільність застосування ризик-орієнтованого підходу до усіх процесів по забезпеченню інформаційної безпеки, варто відзначити, що у перших трьох документах із зазначеного переліку, які були першими вітчизняними документами, що стосувались захисту інформації поняття ризику та оцінки ризиків не освітлювалось. Ці питання почали розглядатися у серії документів по захисту інформації в комп'ютерних системах від несанкціонованого доступу.

У НД ТЗІ 1.1-003-99 поняття ризику сформульовано як функція ймовірності реалізації певної загрози, виду і величини завданих збитків. Однак у даному документі не розкрито термін оцінки ризиків. Проте в інших нормативних документах зазначене поняття широко використовується. Так, наприклад, у НД ТЗІ 1.4-001-00, як одне з завдань, яке необхідно розв'язати при розробці політики безпеки, зазначено оцінку ризиків. Результати проведеної оцінки можуть бути застосовані, наприклад, при класифікації оброблюваної в системі інформації.

У НД ТЗІ 3.7-001-99 зазначається, що функціональний профіль захищеності інформації в конкретній АС може бути визначений в результаті проведення аналізу загроз та оцінки ризиків. У переліку основних робіт при формуванні технічного завдання, що міститься у даному документі, зазначено необхідність визначення експертної оцінки очікуваних втрат у разі здійснення загроз.

Варто відзначити, що у 2003-2005 роках було прийнято державні стандарти України, що базуються на перекладі вищезгаданого стандарту ISO/IEC 13335. Проте термінологія, що наведена у цьому стандарті дещо відрізняється від наведеної у серії

НД ТЗІ, а підходи, запропоновані в ISO/IEC 13335 майже не застосовуються на практиці.

Таким чином, аналізуючи наявну в Україні систему нормативного забезпечення у сфері інформаційної безпеки, можна зробити висновок про необхідність її перегляду та розвитку, одним із найважливіших етапів якого є гармонізація існуючих вітчизняних документів із досвідом міжнародних стандартів.

Висновки

Розглянуті вище два основних напрямки розвитку систем інформаційної безпеки вирішують подібні проблеми по-різному. Дуже важливий методологічний недолік «Помаранчевої книги», що в певній мірі зберігається і в групі похідних від неї стандартів – орієнтація на інтереси оцінювача(«Контролера»), а не власника системи. Альтернативою такого підходу є стандарти для систем управління ІБ, в яких побудова і реалізація СУІБ планується, виходячи із завдань забезпечення бізнесу, відповідно до цілей і місії організації і витікаючими вимогами до її безпеки, залежними від використовуваних інформаційних процедур, розмірів і структури організації. Таким чином, розглянуті напрямки в практичній діяльності призводять дорізноманітних компромісних варіантів реалізації систем безпеки інформації на національному, міжнаціональному, різних професійно-орієнтованих рівнях, в залежності від конкретних соціально-економічних умов, ідейно-політичних цілей і завдань, що стоять перед зацікавленими сторонами.

Перелік використаних джерел

1. Юдін О. К., Богуш В. М. Інформаційна безпека держави // — Харків: Консум. — 2004. — С. 315–376.
2. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. // – К.: Видавнича група BHV. — 2009. — С. 142–175.
3. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. // – М.: Горячая линия – Телеком. — 2000. — 452 с.
4. C. Zhou and S. Ramacciotti. Common criteria: Its limitations and advice on improvement. // Information Systems Security Association ISSA Journal. — 2011. — pages 24–28.
5. Samuel Paul Kaluvuri, Michele Bezzi, and Yves Roudier.
   Quantitative Analysis of Common Criteria Certification Practice — 2012. — Available at: `http://www.eurecom.fr/en/publication/4438/download/rs-publi-4438.pdf`.
6. Other ISMS Standarts
   ISO27k infosec management standards — 2012. — Available at: `http://www.iso27001security.com/html/others.html`.
7. Information technology — Security techniques — Information security management systems — Requirements: ISO/IEC 27001:2005. // — Geneve. — 2005. — 42 p.
8. Информационные технологии. Свод правил по управлению защитой информации : ISO/IEC 27002:2005. // — М.: “Технонорматив”. — 2007. — 183 с.
9. Information technology — Security techniques — Information security risk management: ISO/IEC 27005:2008. // — Geneve. — 2008. — 64 p.
10. Айвазова К.Б. , Мацків О.І. Аналіз перспективних стандартів забезпечення інформаційної безпеки // Available at: `http://dspace.oneu.edu.ua/jspui/bitstream.pdf`.
11. BS 7799-3 Information security management systems. Guidelines for information security risk management. // 2006. —
12. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий: ГОСТ Р ИСО/МЭК ТО 13335-3-2007. // — М.: ФГУП «СТАНДАРТИНФОРМ». — 2007. — 84 с.
13. Information technology — Security techniques — Information security management systems — Requirements: ISO/IEC 27001:2005. // — Geneve. — 2005. — 42 p.
14. Захист інформації. Технічний захист інформації. Порядок проведення робіт: ДСТУ 3396.1-96. // — К.: Держстандарт України. — 1996. — 6 с.
15. Захист інформації. Технічний захист інформації. Терміни та визначення: ДСТУ 3396.2-97. // — К.: Держстандарт України. — 1997. — 10 с.
16. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99. // — К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. — 1999. — 21 с.
17. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. // — К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. — 1999. — 30 с.
18. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. // — К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. — 1999. — 58 с.
19. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі: НД ТЗІ 3.7-001-99. // — К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. — 1999. — 14 с.
20. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі: НД ТЗІ 3.7-003-05. // — К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. — 2005. — 25 с.