УДК 681.3.06

Матковський А.П., к.т.н., с.н.с.

СТАНДАРТИ ТА КРИТЕРІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Робота присвячена питанню захисту комп'ютерної інформації. Порівнюються існуючі стандарти інформаційної безпеки. Відносно докладно розглядаються Єдині міжнародні критерії CCITS

Вступ

В наш час бурхливого розвитку інформаційних технологій (ІТ) зростають загрози несанкціонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем. Відповідно, все більше уваги приділяється питанням захисту інформації. Основою для вирішення цих питань є Конституція України, Закони України «Про інформацію», «Про захист інформації в автоматизованих системах», «Про державну таємницю», «Про науково-технічну інформацію», «Про Концепцію Національної програми інформатизації», інші нормативно-правові акти, а також міжнародні угоди України, що стосуються сфери інформаційних відносин та безпеки інформації [1, с. 210].

В літературі розглядаються досить докладно стандарти інформаційної безпеки, причому відмічається, що теорія інформаційної безпеки відстає від бурхливого розвитку засобів обробки інформації [2, с. 9].

В даній роботі розглядається поняття захищеної системи обробки інформації, порівнюються різні стандарти інформаційної безпеки, зокрема Єдині міжнародні критерії *CCITSE*. Наведені методи створення безпечних систем обробки інформації.

Захищена система обробки інформації для певних умов експлуатації забезпечує конфіденційність і цілісність оброблюваної інформації і підтримує свою працездатність в умовах дії на неї заданої множини загроз. [3, с. 15].

Щоб створити захищену систему обробки інформації необхідно і достатньо виконати три завдання.

1. Автоматизувати процес обробки конфіденційної інформації.

Для цього треба:

– визначити формальний механізм, який адекватно виражає задану схему інформаційних потоків і правила управління ними;

– побудувати модель безпеки, що відображає заданий порядок обробки інформації, і формальний доказ її безпеки

– реалізувати систему обробки інформації у відповідності із запропонованою моделлю;

– довести адекватність допустимих в автоматизованій системі потоків інформації і правил управління доступом початковій схемі інформаційних потоків і правил управління ними.

2. Усунути передумови, що обумовлюють успішну реалізацію загроз.

Існують два методи протидії загрозам безпеці:

– створення засобів захисту від кожного виду загроз. До переваг даного методу слід віднести те, що засоби захисту не залежать безпосередньо від призначення системи і не вимагають модифікації у міру її розвитку. Недоліком такого підходу є необхідність проаналізувати всі типи загроз і виробити ефективні механізми протидії для кожного типу;

– усунення причин, які обумовлюють успішну реалізацію загроз. Переваги цього методу в тому, що він не залежить від розвитку загроз, оскільки ліквідовує причину, а не наслідок, тому він ефективніший, ніж створення засобів захисту від кожного виду загроз. Як недоліки даного методу можна вказати необхідність модернізації деяких аспектів процесу проектування і створення захищених систем обробки інформації шляхом застосування технологій проектування і розробки, направлених на усунення вказаних причин успішної реалізації загроз.

3. Реалізувати вимоги стандартів ін-

формаційної безпеки.

Безпека є якісною характеристикою системи, її не можна виміряти в яких-небудь одиницях, більш того, не можна навіть з однозначним результатом порівнювати безпеку двох систем – одна володітиме кращим захистом в одному випадку, інша – в іншому. Для узгодження всіх точок зору на проблему створення захищених систем розроблені і продовжують розроблятися стандарти інформаційної безпеки. Ці документи регламентують основні поняття і концепції інформаційної безпеки на державному або міждержавному рівні. Головна задача стандартів інформаційної безпеки ― створити основу для взаємодії між трьома основними категоріями споживачів: ІТ-користувачів, розробників та експертів кваліфікаційного аналізу захищених комп'ютерних систем [1. с. 211].

Для користувачів велике значення має простота критеріїв безпеки для вибору захищених продуктів ІТ (ІТ-продуктів), а також гнучкість вимог і можливість застосування їх до специфічних ІТ-продуктів та середовищ експлуатації.

Розробники вимагають від стандартів (критеріїв) максимальної конкретності, однозначності та сумісності декларованих у них вимог і часткових критеріїв із сучасними конфігураціями комп'ютерних систем та операційними системами, що в них використовуються.

Для експерта велике значення має детальність регламентуючих процедур кваліфікаційного аналізу, чіткість, простота, однозначність і легкість у використанні декларованих часткових критеріїв безпеки.

Таким чином, перед стандартами інформаційної безпеки стоїть непросте завдання: – примирити ці три точки зору і створити ефективний механізм взаємодії всіх сторін. Як узагальнені показники, що характеризують стандарти інформаційної безпеки і мають значення для всіх трьох сторін, пропонується використовувати універсальність, гнучкість, гарантованість, реалізованість і актуальність.

Універсальність стандарту визначається множиною типів обчислювальних систем і областю ІТ, до яких можуть бути коректно застосовані його положення.

Гнучкість стандарту – це можливість і зручність його застосування до ІТ, що постійно розвиваються та час його "старіння".

Гарантованість визначається потужністю передбачених стандартом методів і засобів підтвердження результатів кваліфікаційного аналізу.

Реалізованість – це можливість адекватної реалізації вимог і критеріїв стандарту на практиці, з урахуванням витрат на цей процес.

Актуальність відображає відповідність вимог і критеріїв стандарту множині загроз безпеці, що постійно розвивається, та новітнім методам і засобам, використовуваним зловмисниками. Класифікація стандартів інформаційної безпеки наведена в таб. 1.

Таблиця 1. Зіставлення стандартів інформаційної безпеки.

Стандарти безпеки	Показники якості стандартів інформаційної безпеки				
	Універсальність	Гнучкість	Гарантованість	Реалізованість	Актуальність
Оранжева книга ([4], 1983.)	обмежена	обмежена	обмежена	висока (крім вищого класу А)	помірна
Європейські критерії ([5], 1986.)	помірна	помірна	помірна	висока	помірна

Документи ДТК ([6-8], 1992.)	обмежена	обмежена	відсутня	висока	обмежена
Федеральні критерії ([9], 1992.)	висока	відмінна	достатня	висока	висока
Канадські критерії ([10], 1993.)	помірна	достатня	достатня	достатня	достатня
Єдині критерії ([11], 1999.)	надмірна	надмірна	надмірна	надмірна	надмірна

Відповідності стандартів запропонованим показникам визначається за наступною якісною шкалою:

– обмежена – недостатня відповідність, при застосуванні стандарту виникають істотні труднощі;

– помірна – мінімальна відповідність, при застосуванні стандарту в більшості випадків істотних труднощів не виникає;

– достатня – задовільна відповідність, при застосуванні стандарту в більшості випадків не виникає ніяких труднощів, проте ефективність пропонованих рішень не гарантується;

– висока – стандарт пропонує спеціальні механізми і процедури, направлені на поліпшення даного показника, застосування яких дозволяє отримувати достатньо ефективні рішення;

– надмірна – поліпшення даного показника розглядалося авторами стандарту як одна з основних цілей його розробки, що забезпечує ефективність застосування запропонованих рішень.

Єдині критерії безпеки інформаційних технологій (*CCITSE*) "Єдині критерії" регламентують всі стадії розробки, кваліфікаційного аналізу і експлуатації ІТ-продуктів. Ці критерії пропонують достатньо складну і бюрократичну концепцію процесу розробки і кваліфікаційного аналізу ІТ-продуктів, що вимагає від споживачів і виробників величезної кількості роботи по складанню і оформленню вельми об'ємних і докладних нормативних документів. Наведемо деякі базові поняття "Єдиних критеріїв":

Задачі захисту – поняття, що виражає потребу споживачів ІТ-продукту в протистоянні заданій множині загроз безпеки або в необхідності реалізації політики безпеки.

Профіль захисту – спеціальний нормативний документ, що є сукупністю "Задач захисту", функціональних вимог, вимог адекватності і їх обґрунтування. Служить керівництвом для розробника ІТ-продукту при створенні "Проекту захисту".

Проект захисту – спеціальний нормативний документ, що є сукупністю "Задач захисту", функціональних вимог, вимог адекватності, загальних специфікацій засобів захисту і їх обґрунтування. В ході кваліфікаційного аналізу служить як опис ІТ-продукту.

Основними документами, що описують всі аспекти безпеки ІТ-продукту, з погляду користувачів і розробників є відповідно "Профіль захисту" і "Проект за-

хисту".

Профіль захисту

"Профіль захисту" визначає вимоги безпеки до певної категорії ІТ-продуктів, не уточнюючи методи і засоби їх реалізації. За допомогою "Профілів захисту" споживачі формулюють свої вимоги до виробників.

Розглянемо вміст розділів "Профілю захисту" *CCITSE*.

Вступ – містить інформацію, необхідну для пошуку "Профілю захисту" в бібліотеці (каталозі) профілів.

Ідентифікатор "Профілю захисту" – це унікальне ім'я, придатне для його пошуку серед подібних до нього профілів і посилання на нього.

Огляд змісту – містить коротку анотацію "Профілю захисту", на підставі якого споживач може зробити висновок про відповідність даного профілю його запитам.

Опис ІТ-продукту містить його коротку характеристику, функціональне призначення, принципи роботи, методи використання і т.д. Ця інформація не підлягає аналізу і сертифікації, але надається для пояснення вимог безпеки і визначення їх відповідності задачам, що вирішуються за допомогою ІТ-продукту, а також для загального розуміння його структури і принципів роботи.

Середовище експлуатації. Цей розділ містить опис середовища функціонування ІТ-продукту з погляду безпеки.

Умови експлуатації – містить опис умов експлуатації ІТ-продукту і повинен дати вичерпну характеристику середовища його експлуатації з погляду безпеки, зокрема обмеження на умови його застосування.

Загрози безпеки – опис потенційних загроз безпеки, що діють в середовищі експлуатації, яким повинен протистояти захист ІТ-продукту. Для кожної загрози повинні бути вказані її джерело, метод і об'єкт дії.

Політика безпеки – описання регламентування та пояснення правил безпеки, які мають бути реалізовані в ІТ-продукті.

Задачі захисту – відображення потреби користувачів в протидії вказаним загрозам безпеки і/або реалізації, політики безпеки.

Задачі захисту ІТ-продукту ─ відображення потреби користувачів в протидії загрозам безпеки і/або реалізації політики безпеки.

Інші задачі захисту – відображення необхідності участі засобів захисту ІТ-продукту в протидії загрозам безпеці і/або реалізацій політики безпеки спільно з іншими компонентами інформаційних технологій.

Вимоги безпеки. У цьому розділі "Профілю захисту" містяться вимоги безпеки, яким повинен задовольняти ІТ-продукт для вирішення задач захисту.

Розділ функціональних вимог повинен містити тільки типові вимоги, згідно з критеріями *CCITSE*, деталізація яких дає можливість продемонструвати їх відповідність задачам захисту. Функціональні, вимоги можуть наказувати або забороняти використання конкретних методів і засобів захисту.

Розділ вимог адекватності містить посилання на типові вимоги рівнів адекватності *CCITSE* (7 класів і 25 вимог та 7 рівнів адекватності). але допускає і визначення додаткові вимог адекватності.

Розділ вимог до середовища експлуатації є необов'язковим і може містити вимоги до середовища експлуатації ІТ-продуктів (функціональні, адекватні). На відміну від попередніх розділів, використання типових вимог критеріїв *CCITSE* є бажаним, але необов'язковим.

Додаткові відомості – необов'язковий розділ, що містить будь-яку додаткову інформацію, яка може бути корисна для проектування, розробки, кваліфікаційного аналізу і сертифікації ІТ-продукту.

Обґрунтування повинне демонструвати, що "Профіль захисту" містить повну і пов'язану множину вимог, і що ІТ-продукт, який задовольняє їм ефективно протистоятиме загрозам безпеки середовища експлуатації.

Обґрунтування задач захисту – містить демонстрацію того, що задачі захисту, запропоновані в профілі, відповідають параметрам середовища експлуатації, і їх рішення дозволить ефективно протистояти загрозам безпеці і реалізувати політику безпеки.

Обґрунтування вимог безпеки – показує, що вимоги безпеки дозволяють ефективно вирішити задачі захисту, оскільки:

– сукупність цілей, що переслідуються окремими функціональними вимогами, відповідає встановленим задачам захисту;

– вимоги безпеки є узгодженими, тобто не суперечать, а взаємно підсилюються;

– усі взаємозв'язки між вимогами (функціональними, адекватності, до середовища експлуатації) враховані або шляхом вказівки їх у вимогах, або шляхом декларування вимог до середовища експлуатації;

– обраний набір вимог і рівень адекватності (один з семи стандартизованих рівнів за *CCITSE*) можуть бути обґрунтовані та гарантовані.

"Профіль захисту" служить основою для розробника і виробника ІТ-продукту, в процесі створення "Проекту захисту", який є технічним проектом для розробки ІТ-продукту і представляє його в ході кваліфікаційного аналізу.

Проект захисту

"Проект захисту" містить вимоги і задачі захисту ІТ-продукту, а також описує рівень функціональних можливостей реалізованих в нім засобів захисту, їх обґрунтування і підтвердження ступеня їх адекватності. "Проект захисту" є основою для розробника системи, а з іншого боку ─ є еталоном системи в ході кваліфікаційного аналізу. Структура "Проекту захисту" представлена на мал. 1. Багато розділів "Проекту захисту" співпадають з однойменними розділами "Профілю захисту", тому не будемо на них докладно зупинятись.

Розглянувши "Єдині критерії безпеки інформаційних технологій" можна зробити такі висновки:

Виробники (розробники), можуть використовувати рекомендації Єдиних критеріїв *CCITSE* в ході проектування, розробки ІТ-продуктів, а також при підготовці до кваліфікаційного аналізу та сертифікації. Цей документ дає можливість виробникам (розробникам) на підставі запитів користувачів визначити набір вимог, яким має задовольняти розроблюваний ними ІТ-продукт.

Запропоновані "Єдиними критеріями" механізми "Профілю захисту" і "Проекту захисту" дозволяють споживачам і виробникам повною мірою сформулювати вимоги безпеки і задачі захисту, а з іншого боку дають можливість експертам по кваліфікації проаналізувати взаємну відповідність між вимогами, потребами споживачів, задачами захисту і засобами захисту ІТ-продукту.

Єдині критерії *CCITSE* декларують сім стандартних рівнів адекватності, які відображають можливості засобів контролю та верифікації в ході розробки, кваліфікаційного аналізу та сертифікації ІТ-продукту.

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.

Таким чином, вимоги "Єдиних критеріїв" охоплюють практично всі аспекти безпеки ІТ-продуктів і технології їх створення, а також є практично всеосяжною енциклопедією інформаційної безпеки, тому їх можна використовувати як довідник по безпеці інформаційних технологій.

Даний стандарт робить реальною перспективу створення єдиного безпечного інформаційного простору, в якому сертифікація безпеки систем обробки інформації здійснюватиметься на глобальному рівні.

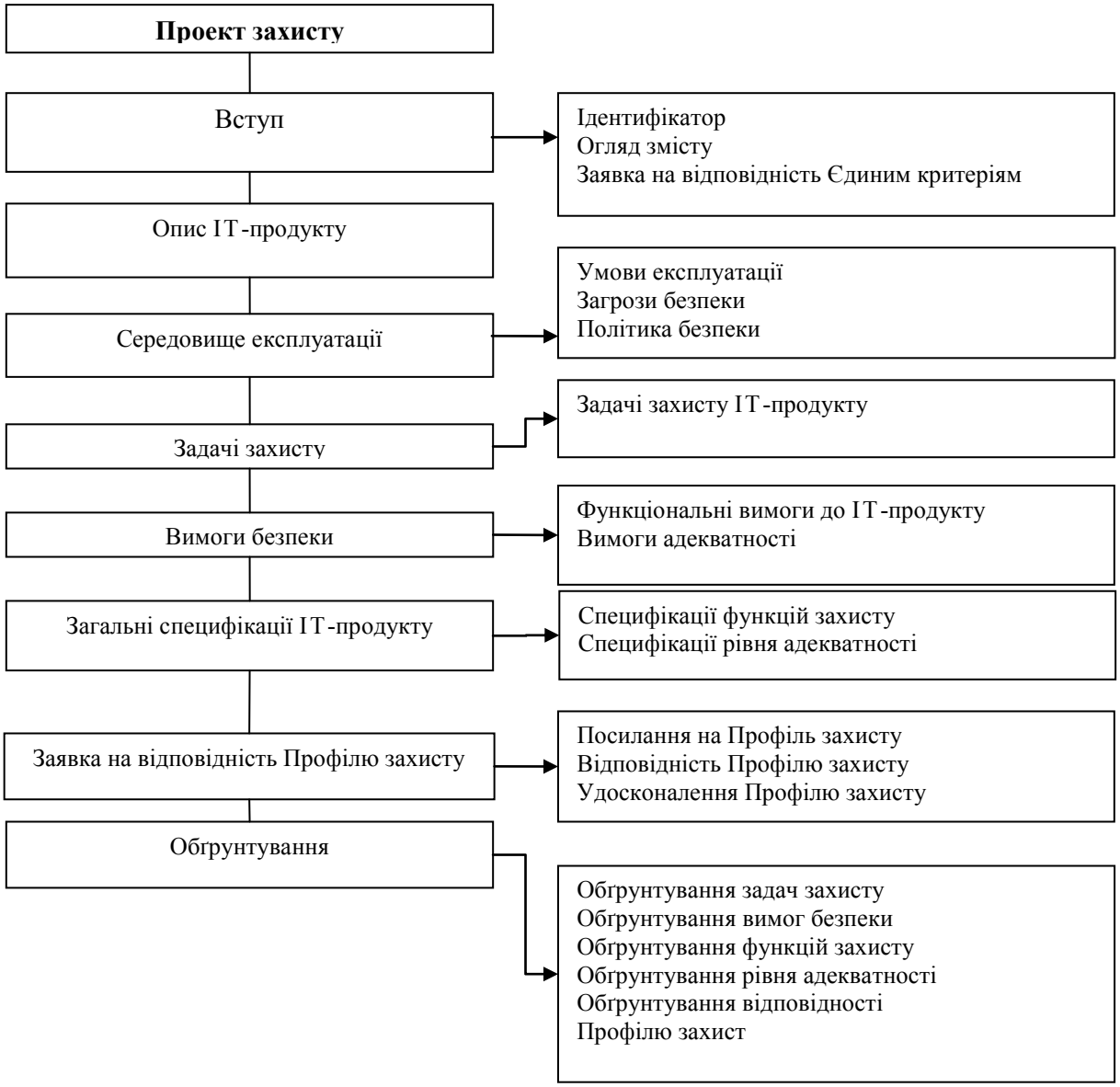

Рис. 1. Структура Проекту захисту згідно "Єдиним критеріям".

Висновок

Поданий матеріал дозволяє визначили задачі, які повинні бути вирішені в ході створення захищеної системи: ефективне протистояння загрозам безпеки, що діють в середовищі її експлуатації, коректна реалізація політики безпеки, а також сформулювати завдання кожного з учасників процесу створення захищених систем (споживачі, виробники, експерти по сертифікації).

Список літератури

1. *Вертузаєв М.С.* Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. посібник / За ред. С.Г.Лаптєва. – К.: Вид-во Європ. ун-ту, 2001. – 321 с.

2. *Косарев В.М.* Информационная безопасность: организация защиты программ и данных: Учебное пособие. – Днепропетровск: Изд-во ДУЭП, 2003. – 152 с.

3. *Зегжда Д.П.* Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с., ил.

4. Trusted Computer System Evaluation Criteria. US Department of Defense 5200.28-STD, 1983.

5. Information Technology Security Evaluation Criteria. Harmonized Criteria of France-Germany-Netherlands-United Kingdom. – Department of Trade and Industry, London, 1991.

6. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники от несанкционированного доступа к информации. Москва. 1992 г.

7. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Москва, 1992г.

8. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Москва, 1992 г.

9. Federal Criteria for Information Technology Security. National Institute of Standards and Technology & National Security Agency. Version 1.0. December 1992.

10. Canadian Trusted Computer Product Evaluation Criteria. Canadian System Security Centre Communication Security Establishment, Government of Canada. Version 3.0e. January 1993.

11. Common Criteria for Information Technology Security Evaluation. National Institute of Standards and Technology & National Security Agency (USA), Communication Security Establishment (Canada), Communications -Electronics Security Group (United Kingdom), Bundesamt fur Sichereit in der Informationstechnik (Germany), Service Central de la Securite des Systemes d'Information (France), National Communications Security Agency (Netherlands). Version 2.1, August 1999.

Подано до редакції 30.11.2010