УДК 681.322

*Ігор Олександрович Ляшенко*

# ФЕДЕРАЛЬНІ КРИТЕРІЇ БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ

## Постановка проблеми. Аналіз останніх досліджень і публікацій

Реалізація вимог щодо забезпечення безперервного, якісного та оперативного управління військами (силами) під час підготовки та в ході ведення бойових дій в умовах сьогодення вимагає створення та розвиток сучасної ефективної автоматизованої системи управління. Ця система управління повинна буде функціонувати в умовах обробки значного об'єму невизначеної та нечіткої інформації про умови обстановки, противника та свої війська.

Цілком зрозуміло, що противник намагатиметься будь-яким способом вразити систему управління військами (інформаційно-управляюча система спеціального призначення): нанести вогневе ураження, придушити радіоелектронними засобами, провести кібернетичні атаки. Останній спосіб, на думку фахівців [1-4]. Тому питанню безпеки інформаційно-управляючих систем приділяється значна увага у всьому світі.

Особливого значення цьому питанню надають на етапі розробки інформаційно-управляючих систем, оскільки захист та функціонування цих систем потрібно розглядати одночасно та в комплексі.

При створенні підсистеми захисту інформаційно-управляючих систем спеціального призначення користуються спеціальними стандартами інформаційної безпеки, метою яких створення підґрунтя взаємодії між виробниками, користувачами та експертами по кваліфікації продуктів інформаційних технологій.

## Формулювання мети статті. Виклад основного матеріалу

Пропонується доцільним здійснити аналіз існуючих стандартів дослідивши структуру, вимоги та критерії та ефективність їх практичного застосування.

Для прикладу розглянемо федеральні критерії безпеки інформаційних технологій.

"Федеральні критерії безпеки інформаційних технологій" (Federal Criteria for Information Technology Security) розроблялися як одна із складових "Американського федерального стандарту з обробки інформації" (Federal Information Processing Standard), покликаного замінити "Помаранчеву книгу". Авторами стандарту виступили Національний інститут стандартів і технологій США (National Institute of Standards and Technology) та Агентство національної безпеки США (National Security Agency).

Цей документ грунтується на результатах численних досліджень у сфері забезпечення безпеки інформаційних технологій 80-х — початку 90-х років, а також на аналізі досвіду використання "Помаранчевої книги".

"Федеральні критерії безпеки інформаційних технологій" (далі просто "Федеральні критерії" охоплюють практично повний спектр проблем пов'язаних із захистом і забезпеченням безпеки, оскільки включають усі аспекти забезпечення конфіденційності, цілісності та працездатності.

Основними об'єктами застосування вимог безпеки "Федеральних критеріїв" є продукти інформаційних технологій (Information Technology Products) і системи обробки інформації (Information Technology Systems).

Положення "Федеральних критеріїв" торкаються тільки власних засобів забезпечення безпеки ІТ-продуктів, тобто механізмів захисту, вбудованих безпосередньо у ці продукти у вигляді відповідних програмних та апаратних засобів. Для підвищення їх ефективності можуть додатково застосовуватися зовнішні системи захисту та засоби забезпечення безпеки, до яким відносяться як технічні, так і організаційні заходи, правові та юридичні норми. Кінець кінцем безпека ІТ-продукту визначається сукупністю власних засобів забезпечення безпеки та зовнішніх засобів, що є частиною середовища експлуатації.

Ключовим поняттям концепції інформаційної безпеки "Федеральних критеріїв" являється поняття "Профіль захисту". Профіль захисту — це нормативний документ, який регламентує усі аспекти безпеки ІТ-продукту у вигляді вимог до його проектування, технології розробки та кваліфікаційного аналізу. Як правило. один профіль захисту описує декілька близьких по структурі та призначенню ІТ-продуктов. Основна увага в профілі захисту приділяється вимогам до складу засобів захисту та якості їх реалізації, а також їх адекватності передбачуваним загрозам безпеки.

"Федеральні критерії" представляють процес розробки систем обробки інформації, що розпочинається з формулювання вимог споживачами та закінчується введенням в

експлуатацію у вигляді послідовності наступних основних етапів:

розробка й аналіз профілю захисту;

розробка та кваліфікаційний аналіз ІТ-продуктів;

компонування та сертифікація системи обробки інформації в цілому.

“Федеральні критерії” регламентують тільки перший етап цієї схеми – розробку та аналіз профілю захисту. Процес створення ІТ-продуктів і компонування систем обробки інформації залишаються поза рамками цього стандарту.

*Профіль захисту.*

Профіль захисту призначений для визначення та обгрунтування складу та змісту засобів захисту, специфікації технології розробки та регламентації процесу кваліфікаційного аналізу ІТ-продукту. Профіль захисту складається з п’яти розділів:

опис;

обгрунтування;

функціональні вимоги до ІТ-продукту;

вимоги до технології розробки ІТ-продукту;

вимоги до процесу кваліфікаційного аналізу ІТ-продукту.

“Федеральні критерії” містять детальний опис усіх трьох розділів профілю захисту, присвячених вимогам, що включає їх таксономію та ранжирування для кожного розділу. У цьому огляді основна увага приділена функціональним вимогам, оскільки саме в цій області “Федеральні критерії” здійснили значний крок вперед в порівнянні з передуючими стандартами.

“Федеральні критерії” пропонують набір функціональних вимог, реалізація яких дозволяє протистояти найбільш поширеним загрозам безпеці, що відносяться до широкого спектру ІТ-продуктів та областей їх застосування. Ці вимоги розроблені з урахуванням можливості розширення та адаптації до конкретних умов експлуатації ІТ-продуктів і можуть удосконалюватися паралельно процесу розвитку інформаційних технологій.

Функціональні вимоги, приведені в “Федеральних критеріях”, визначають склад і функціональні можливості ядра безпеки – Trasted Computing Base (TCB).

Вимоги, що спрямовані на забезпечення безпеки, відносяться або до внутрішніх елементів TCB, або до його зовнішніх функцій, доступних через спеціальні інтерфейси.

Функціональні вимоги профілю захисту задаються у вигляді загальних станів і непрямим чином визначають множину загроз, яким може успішно протистояти ІТ-продукт.

Таксономія функціональних вимог

Функціональні вимоги “Федеральних критеріїв” розподілені на вісім класів і визначають усі аспекти функціонування TCB. Таксономія класів функціональних вимог приведена на рис. 1. Усі класи мають безпосереднє відношення до забезпечення безпеки функціонування TCB.

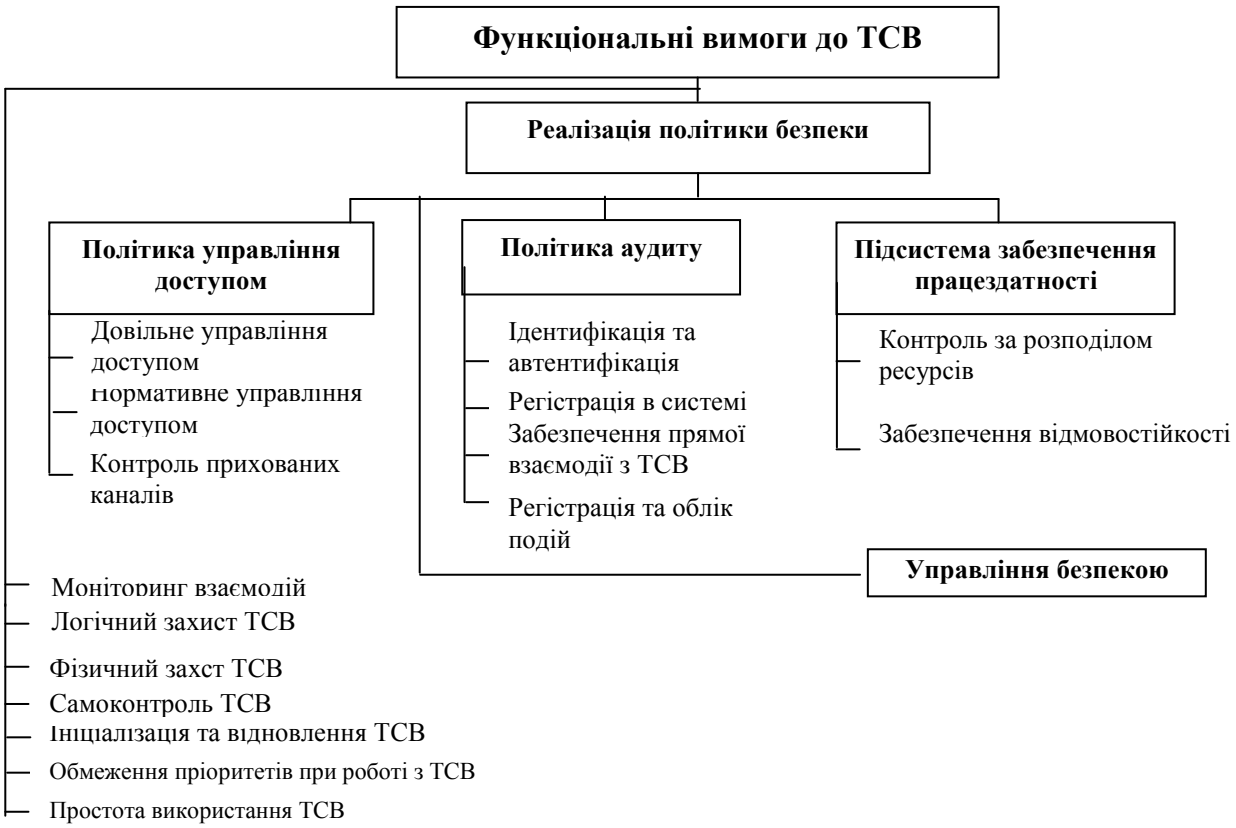


**Рис 1. Таксономія функціональних вимог “Федеральних критеріїв”**

Об’єм і глибина реалізації функціональних вимог залежать від того, який ступінь захищеності повинно забезпечувати TCB конкретного ІТ-продукту, а також від того, які загрози безпеці

можливі в середовищі його експлуатації. Ступінь забезпечення необхідного рівня захищеності залежить від реалізованої політики безпеки, кваліфікації відповідального за безпеку персоналу, правильності адміністрування ТСВ та дотримання рядовими користувачами правил політики безпеки.

## Висновки

"Федеральні критерії безпеки інформаційних технологій" стали першим стандартом інформаційної безпеки, в якому визначаються три незалежні групи вимог: функціональні вимоги до засобів захисту, вимоги до технології розробки та до процесу кваліфікаційного аналізу.

Авторами цього стандарту вперше запропонована концепція профілю захисту документу, що містить опис усіх вимог безпеки як до самого ІТ-продукту, так і до процесу його проектування, розробки, тестування й кваліфікаційного аналізу.

Функціональні вимоги безпеки добре структуровані та описують усі аспекти функціонування ТСВ. Вимоги до технології розробки, які вперше з'явилися в цьому документі, спонукають виробників використовувати сучасні технології програмування, що дозволяють забезпечити безпеку свого продукту. Вимоги до процесу кваліфікаційного аналізу носять досить загальний характер і не містять конкретних методик тестування та дослідження безпеки ІТ-продуктів.

Розробники "Федеральних критеріїв" відмовилися від використовуваного в "Помаранчевій книзі" підходу до оцінки рівня безпеки ІТ-продукту на основі узагальненої універсальної шкали класів безпеки. Замість цього пропонується незалежне ранжирування вимог кожної групи, тобто замість єдиної шкали використовується множина часткових шкал-критеріїв, що характеризують рівень безпеки, що забезпечується. Цей підхід дозволяє розробникам і користувачам ІТ-продукту обрати найбільш прийнятне рішення та точно визначити необхідний і достатній набір вимог для кожного конкретного ІТ-продукту та середовища його експлуатації.

Особливо відмічається, що цей стандарт розглядає усунення недоліків існуючих засобів безпеки як одне із завдань захисту разом з протидією загрозам безпеки та реалізацією моделі безпеки.

Цей стандарт ознаменував появу новою покоління керівних документів в області інформаційної безпеки, а його основні положення послужили базою для розробки "Канадських критеріїв безпеки комп'ютерних систем" і "Єдиних критеріїв безпеки інформаційних технологій".

## *Література*

**1. Toffler**, Alvin and Heidi, War and Anti – War: Survival at the Dawn of the 21st Century. New York: Little, Brown and Company, 1993, 3p. **2. Winn Schwartau**. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's Mouth Press, 1994, 13p. **3. Азов В. О.** реализации в США концепции ведения военных действий в едином информационном пространстве / В. Азов / Зарубежное военное обозрение. – 2004. – №6. – С. 10 – 17. **4. Кларк Р.** Третья мировая война: какой она будет? / Кларк.Р., Нейк Р. / - СПб.: Питер, 2011. – 336 с.: ил.

Рассматривается принцип создания стандарта информационной безопасности информационно-управляющих систем на примере "Федеральных критериев информационной безопасности".

*Ключевые слова:* информационная безопасность, политика безопасности, доступ, стандарт, идентификация, адекватность.

The article highlights the principles of creation for information security standart for control information systems with the example of the "Federal Criteria for Information Technology Security".

*Key words:* informative safety, policy of safety, access, standard, authentication, adequacy.