УДК 681.322

*Ігор Олександрович Ляшенко*

# КРИТЕРІЇ БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ МІНІСТЕРСТВА ОБОРОНИ США (“ПОМАРАНЧЕВА КНИГА”)

## Постановка проблеми у загальному вигляді

Друга половина XX – початок XXI століть характеризуються бурхливим зростанням досліджень та досягнень в галузі штучного інтелекту та інтелектуальних систем. Для подальшого технічного прогресу вкрай необхідно розвивати та впроваджувати автоматизовані інтелектуальні та роботизовані системи, які в змозі виконувати будь-які дії за будь-яких умов та в будь-якому просторі – на суші чи в повітряному, космічному, водному й підводному, а на сьогоднішній день – і в кібернетичному просторі.

Цілком зрозуміло, що найбільш активно автоматизовані інтелектуальні та роботизовані системи, в першу чергу, розробляються та впроваджуються у військовій сфері.

## Проблемне питання

У ЗС України в 2001 році затверджено концепцію створення єдиної автоматизованої системи управління. Її призначення – досягнення якісно нового рівня системи управління для підвищення ефективності керівництва життєдіяльністю, розвитком, підготовкою та застосуванням ЗС України як в мирний час, так і в особливий період.

Однак, на сьогоднішній день в Україні, а в її Збройних Силах тим більш, немає власних стандартів щодо побудови інформаційно-управляючих систем спеціального призначення. Одним з основних з набору стандартів при цьому є стандарт інформаційної безпеки.

## Мета статті

Пропонується розглянути існуючі стандарти інформаційної безпеки провідних країн світу на прикладі “Критеріїв безпеки комп'ютерних систем міністерства оборони США” (Trusted Computer System Evaluation Criteria. US Department of Defense 200.28-STD).

## Виклад основного матеріалу

Головним завданням стандартів інформаційної безпеки є створення основи взаємодії між виробниками, споживачами та експертами з кваліфікації продуктів інформаційних технологій. Кожна з цих груп має свої інтереси і свої погляди на проблему інформаційної безпеки.

А саме — споживачі, по-перше, зацікавлені в методиці, що дозволяє обґрунтовано обрати продукт, що відповідає їх потребам та вирішує їх проблеми, для чого їм потрібна шкала оцінки безпеки, і, по-друге, потребують інструменту, за допомогою якого вони могли б формулювати свої вимоги виробникам. Відповідно і вимоги споживачі хотіли б формулювати приблизно в наступній формі: захист обробки абсолютно секретної інформації. Цей неконструктивний підхід сам по собі не такий страшний, набагато гірше інше – багато споживачів не розуміють, що за все потрібно платити (і не лише грошима) і, що вимоги безпеки обов'язково суперечать функціональним вимогам (зручності роботи, швидкодії і т. п.), накладають обмеження на сумісність і, як правило, змушують відмовитися від дуже широко поширених незахищених прикладних програмних засобів.

Виробники, у свою чергу, потребують стандартів для порівняння можливостей своїх продуктів у застосуванні процедури сертифікації для об'єктивної оцінки їх властивостей, а також в стандартизації певного набору вимог безпеки, який міг би обмежити фантазію замовника конкретного продукту і змусити його обирати вимоги з цього набору. З точки зору виробника, вимоги мають бути максимально конкретними та регламентувати необхідність застосування тих або інших засобів, механізмів, алгоритмів і т. д.

Експерти з кваліфікації та фахівці з сертифікації розглядають стандарти як інструмент, що дозволяє їм оцінити рівень безпеки, який забезпечується продуктами інформаційних технологій, і надати споживачам можливість зробити обґрунтований вибір. Виробники в результаті кваліфікації рівня безпеки отримують об'єктивну оцінку можливостей свого продукту.

Таким чином, перед стандартами інформаційної безпеки стоїть непросте завдання — примирити ці три точки зору та створити ефективний механізм взаємодії усіх сторін. Причому обмеження потреб хоч би однієї з них приведе до неможливості взаєморозуміння та взаємодії і, отже, не дозволить вирішити загальне завдання — створення захищеної системи обробки інформації.

Найбільш значними стандартами інформаційної безпеки являються (у хронологічному порядку): "Критерії безпеки комп'ютерних систем міністерства оборони США"[1], Керівні документи Держтехкомісії Росії ("Концепция защиты средств вычислительной техники от несанкционированного доступа к информации", "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации", "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации", "Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники", "Защита от несанкционированного доступа к информации. Термины и определения"); Європейські критерії безпеки інформаційних технологій ("Information Technology Security Evaluation Criteria. Harmonized Criteria of France-Germany-Netherlands-United Kingdom"); Федеральні критерії безпеки інформаційних технологій США (Federal Criteria for Information Technology Security); Канадські критерії безпеки комп'ютерних систем (Canadian Trusted Computer Product Evaluation Criteria); "Єдині критерії безпеки інформаційних технологій" (Common Criteria for Information Technology Security Evaluation, rational).

Розглянемо "Критерії безпеки комп'ютерних систем міністерства оборони США", Які розроблені Міністерством оборони США в 1983 році з метою визначення вимог безпеки, що пред'являються до апаратного, програмного та спеціального забезпечення комп'ютерних систем і вироблення відповідної методології аналізу політики безпеки, що реалізовується в комп'ютерних системах військового призначення.

У "Помаранчевій книзі" запропоновано три категорії вимог безпеки - політика безпеки, аудит і коректність, у рамках яких сформульовані шість базових вимог безпеки. Перші чотири вимоги спрямовані безпосередньо на забезпечення безпеки інформації, а дві останніх — на якість самих засобів захисту.

Вимога 1. *Політика безпеки.*

Можливість здійснення суб'єктами доступу до об'єктів повинна визначатися на підставі їх ідентифікації та набору правил управління доступом.

Вимога 2. *Мітки.*

Для реалізації нормативного управління доступом система повинна забезпечувати можливість присвоювати кожному об'єкту мітку або набір атрибутів, що визначають міру конфіденційності (гриф секретності) об'єкту і/або режими доступу до цього об'єкту.

Вимога 3. *Ідентифікація та аутентифікація.*

Усі суб'єкти повинні мати унікальні ідентифікатори. Контроль доступу повинен здійснюватися на підставі результатів ідентифікації суб'єкта і об'єкта доступу, підтвердження достовірності їх ідентифікаторів (аутентифікації) і правил розмежування доступу.

Вимога 4. *Реєстрація та облік.*

Для визначення ступеня відповідальності користувачів за дії в системі усі події, що відбуваються в ній події, які мають значення з точки зору безпеки, повинні відстежуватися і реєструватися в захищеному протоколі.

Вимога 5. *Контроль коректності функціонування засобів захисту.*

Засоби захисту повинні містити незалежні апаратні і/або програмні компоненти, що забезпечують працездатність функцій захисту. Це означає, що усі засоби захисту, які забезпечують політику безпеки, управління атрибутами і мітками безпеки, ідентифікацію та аутентифікацію, реєстрацію і облік, повинні знаходиться під контролем засобів, що перевіряють коректність їх функціонування.

Вимога 6. *Безперервність захисту.*

Усі засоби захисту (в т.ч. і ті, що реалізовують цю вимогу) мають бути захищені від несанкціонованого втручання і/або відключення, причому цей захист має бути постійним і безперервним у будь-якому режимі функціонування системи захисту і комп'ютерної системи в цілому.

Критерії безпеки комп'ютерних систем, що розглядаються далі, представляють собою конкретизацію цих узагальнених вимог.

Приведені вище базові вимоги до безпеки служать основою для критеріїв, що утворюють єдину шкалу оцінки безпеки комп'ютерних систем, яка визначає сім класів безпеки.

Зважаючи на широку доступність самої "Помаранчевої книги" та її численних оглядів й інтерпретацій, наведено тільки схему, що відображає таксономію запропонованих в ній функціональних вимог безпеки (рис. 1).

Оскільки "Помаранчева книга" досить детально освітлювалася у вітчизняних дослідженнях [1], обмежимося тільки коротким оглядом класів безпеки. "Помаранчева книга" передбачає чотири групи критеріїв, які відповідають різній мірі захищеності: від мінімальної (група D) до формально доведеної (група A). Кожна група включає один або декілька класів. Групи D і A містять по одному класу (класи D1 і A1 відповідно), група C — класи C1, C2, а група B — B1, B2, B3, що характеризуються різними наборами вимог безпеки.

Рівень безпеки зростає при переміщенні від групи D до групи A, а всередині групи — із зростанням номера класу.

• Група D. Мінімальний захист.

Клас D1. Мінімальний захист. До цього класу відносяться усі системи, які не задовольняють вимогам інших класів.

• Група С. Дискреційний захист.

Група С характеризується наявністю довільного управління доступом і реєстрацією дій суб'єктів.

Клас С1. Дискреційний захист. Системи цього класу задовольняють вимогам забезпечення розділення користувачів та інформації та включають засоби контролю й управління доступом, що дозволяють задавати обмеження для індивідуальних користувачів, що, в свою чергу, дає їм можливість захищати свою приватну інформацію від інших користувачів. Клас С1 розрахований на багато користувачів системи, в якій здійснюється спільна обробка даних одного рівня секретності.

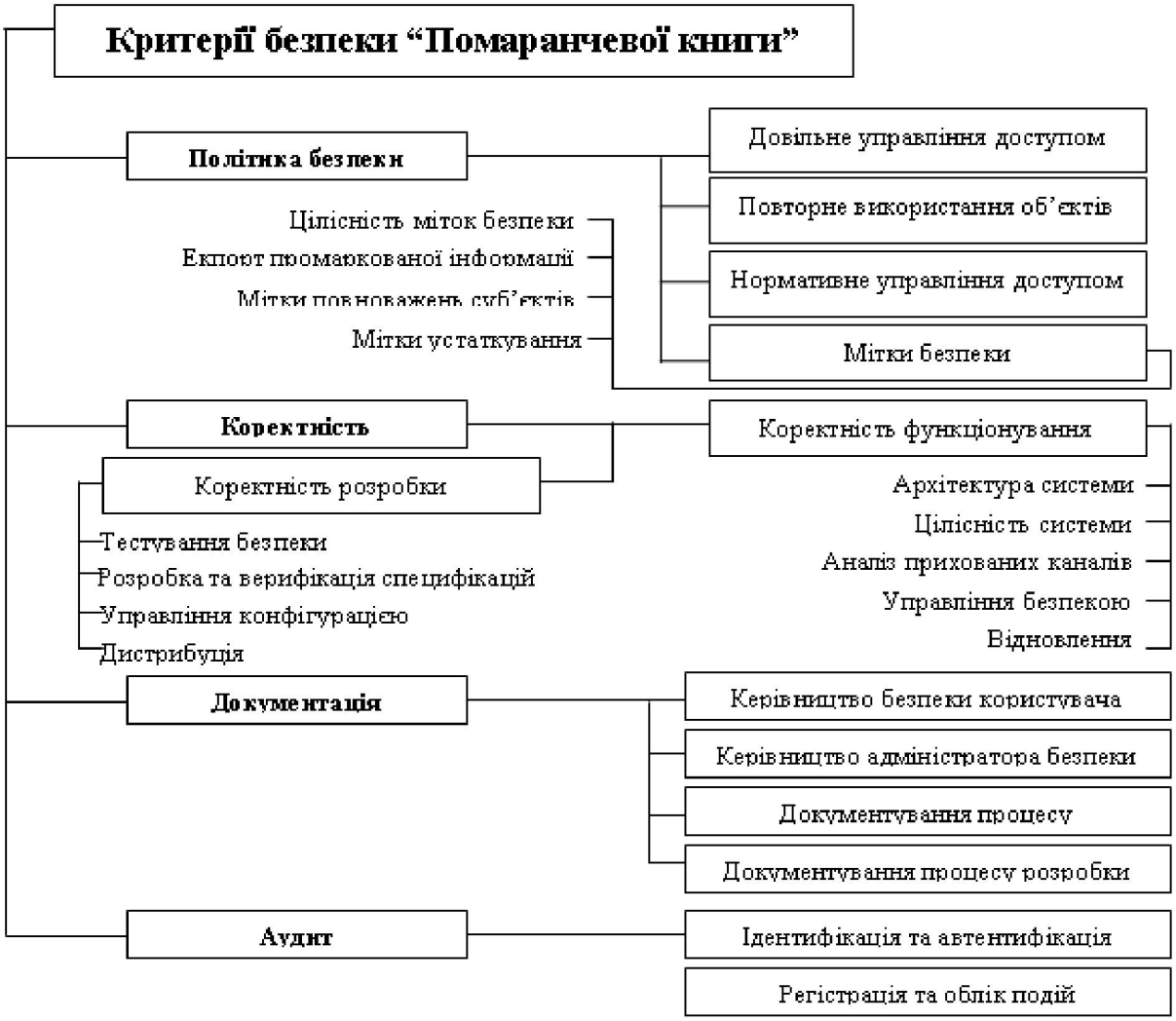


**Рис. 1. Таксономія вимог "Помаранчевої книги"**

Клас С2. Управління доступом. Системи цього класу здійснюють більш виборче управління доступом, ніж системи класу С1, за допомогою застосування засобів індивідуального контролю за діями користувачів, реєстрацією, обліком подій і виділенням ресурсів.

• Група В. Мандатний захист.

Основні вимоги цієї групи — нормативне управління доступом з використанням міток безпеки, підтримка моделі та політики безпеки, а також наявність специфікацій на функції ядра безпеки (Trusted Computing Base – TCB). Для систем цієї групи монітор взаємодій повинен контролювати усі події в системі.

Клас В1. Захист із застосуванням міток безпеки.

Системи класу В1 повинні відповідати усім вимогам, що пред'являються до систем класу С2, та, крім того, повинні підтримувати визначену неформально модель безпеки, маркування даних та нормативне управління доступом. При експорті з системи інформація повинна піддаватися маркуванню. Виявлені в процесі тестування недоліки мають бути усунені.

Клас В2. Структурований захист. Для відповідності класу В2 ядро безпеки системи повинно підтримувати формально визначену та чітко документовану модель безпеки, що передбачає довільне й нормативне управління доступом, яке поширюється, в порівнянні з системами класу В1, на всі суб'єкти. Крім того, повинен здійснюватися контроль прихованих

каналів проникнення інформації. У структурі ТСВ мають бути виділені елементи, що критичні з точки зору безпеки. Інтерфейс ТСВ повинен бути чітко визначений, а його архітектура і реалізація мають бути виконані з урахуванням можливості проведення тестових випробувань. В порівнянні з класом B1 мають бути посилені засоби аутентифікації. Управління безпекою здійснюється адміністраторами системи. Мають бути передбачені засоби управління конфігурацією.

Клас B3. Домени безпеки. Для відповідності цьому класу ТСВ системи повинне підтримувати монітор взаємодій, який контролює усі типи доступу суб'єктів до об'єктів і який неможливо обійти. Крім того, ТСВ повинно бути структуроване з метою виключення з нього підсистем, що не відповідають за реалізацію функції захисту, і бути досить компактними для ефективного тестування та аналізу. В ході розробки і реалізації ТСВ повинні застосовуватися методи і засоби, спрямовані на мінімізацію його складності. Засоби аудиту повинні включати механізми оповіщення адміністратора при виникненні подій, що мають значення для безпеки системи. Необхідна наявність засобів відновлення працездатності системи.

• Група А. Верифікаційний захист.

Ця група характеризується застосуванням формальних методів верифікації коректності роботи механізмів управління доступом (довільного та нормативного). Необхідна додаткова документація, що демонструє, що архітектура і реалізація ТСВ відповідають вимогам безпеки.

Клас A1. Формальна верифікація. Системи класу A1 функціонально еквівалентні системам класу B3 і до них не пред'являється ніяких додаткових функціональних вимог. На відміну від систем класу B3 в ході розробки повинні застосовуватися формальні методи верифікації, що дозволяє з високою впевненістю отримати коректну реалізацію функцій захисту. Процес доведення адекватності реалізації починається на ранній стадії розробки з побудови формальної моделі політики безпеки і специфікацій високого рівня. Для забезпечення методів верифікації системи класу A1 повинні містити потужніші засоби управління конфігурацією та захищену процедуру дистрибуції.

Приведені класи безпеки надовго визначили основні концепції безпеки та хід розвитку засобів захисту.

В ході застосування положень "Помаранчевої книги" з'ясувалося, що частина практично важливих питань залишилася за рамками цього стандарту і, крім того, з плином часу (з моменту публікації пройшло п'ятнадцять років) ряд положень застарів і вимагав перегляду.

Коло специфічних питань по забезпеченню безпеки комп'ютерних мереж і систем управління базами даних знайшло відображення в окремих документах, виданих Національним центром комп'ютерної безпеки США у вигляді доповнень до "Помаранчевої книги" — "Інтерпретація "Помаранчевої книги" для комп'ютерних мереж (Trusted Network Interpretation) та "Інтерпретація "Помаранчевої книги" для систем управління базами даних" (Trusted Database Management System Interpretation). Ці документи містять трактування основних положень "Помаранчевої книги" стосовно тих, що відповідають класам систем, обробки інформації.

Втрата актуальності ряду положень "Помаранчевої книги" викликана, передусім, інтенсивним розвитком комп'ютерних технологій та переходів з мейнфреймів (типу обчислювальних комплексів IBM — 360, 370; радянський аналог — машини серії ЄС) до робочих станцій, високопродуктивних персональних комп'ютерів і мережевої моделі обчислень. Саме для того, щоб виключити некоректність деяких положень "Помаранчевої книги", що виникла в зв'язку зі зміною апаратної платформи, та адаптувати їх до сучасних умов й зробити адекватними потребам розробників і користувачів програмного забезпечення, була виконана величезна робота з інтерпретації та розвитку положень цього стандарту. В результаті виник цілий ряд супутніх "Помаранчевій книзі" документів, багато з яких стали її невід'ємною частиною. До найчастіше згадуваним відносяться:

Керівництво по довільному управлінню доступом у безпечних системах (A guide to understanding discretionary access control in trusted systems);

Керівництво по управлінню паролями (Password management guideline);

Посібник по застосуванню критеріїв безпеки комп'ютерних систем в специфічних середовищах (Guidance for applying the Department of Defence Trusted Computer System Evaluation Criteria in specific environment);

Керівництво по аудиту у безпечних системах (A Guide to Understanding Audit in Trusted Systems);

Керівництво по управлінню конфігурацією у безпечних системах (Guide to understanding configuration management in trusted systems).

Кількість подібних допоміжних документів, коментарів і інтерпретацій значно перевищила об'єм первинного документу, і в 1995 році Національним центром комп'ютерної безпеки США був опублікований документ під назвою "Пояснення до критеріїв безпеки комп'ютерних систем" (The Interpreted Trusted Computer System Evaluation Criteria Requirements), що об'єднує усі доповнення і роз'яснення. При його підготовці перелік питань, що підлягають розгляду та тлумаченню обговорювався на спеціальних конференціях розробників і користувачів захищених систем обробки інформації. В результаті відкритого обговорення була створена база даних, яка включає усі спірні питання, які

потім в повному обсязі були опрацьовані спеціально створеною робочою групою. У результаті з'явився документ, який об'єднав усі зміни та доповнення до "Помаранчевої книги", зроблені з моменту її публікації, що призвело до оновлення стандарту та дозволило застосовувати його в сучасних умовах.

## Висновки

"Критерії безпеки комп'ютерних систем" міністерства оборони США були першою спробою створити єдиний стандарт безпеки, розрахований на розробників, споживачів і фахівців по сертифікації комп'ютерних систем. Основною відмінною рисою цього документу являється його орієнтація на системи військового застосування, в основному на операційні системи. Це зумовило домінування вимог, спрямованих на забезпечення секретності оброблюваної інформації та унеможливлення її розголошування. Велика увага приділена міткам (грифам секретності) та правилам експорту секретної інформації. При цьому критерії адекватності реалізації засобів захисту і політики безпеки відображені слабо, відповідний розділ обмежений вимогами контролю цілісності засобів захисту та підтримки їх працездатності, чого явно недостатньо. Вищий клас безпеки, що вимагає здійснення верифікації засобів захисту, побудований на доведенні відповідності програмного забезпечення його специфікаціям за допомогою спеціальних методик, проте це доведення (дуже дороге, трудомістке і практично нездійсненне для реальних операційних систем) не підтверджує коректність й адекватність реалізації політики безпеки.

"Помаранчева книга" послужила основою для розробників усіх інших стандартів інформаційної безпеки і досі використовується в США у якості керівного документу при сертифікації комп'ютерных систем обробки інформації.

## *Література*

**Галатенко В. А.** Информационная безопасность. "Открытые системы", NN4-6 1995г.

Рассматривается принцип создания стандарта информационной безопасности інформационно-управляющих систем на примере "Помаранчевой книги" США.

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

The article highlights the principles of creation for information security standart for control information systems with the example of the "Trusted Computer System Evaluation Criteria Requirements. National Computer Security Center" of the USA.

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