$$\sum_{j=1}^{n} a_j = \sum_{i=1}^{m} z_i .$$

З цією метою досить ввести імітацію (n+1)-го нападу з ресурсом $a_{n+1} = \sum_{i=1}^{m} z_i$ і помилкове (m+1)-ше спрацьовування, рівне $z_{m+1} = \sum_{j=1}^{n} a_j$, і прийняти вартість $c_{m+1,j} = 0$ для j=1,2,…,n+1, а вартість $c_{i,n+1}$, i=1,2,…,m рівною як завгодно великій величині $b > \max_{\substack{1 \le i \le m \\ 1 \le j \le n}} (c_{ij})$.

Отже сумарна потужність нападу, що імітується, дорівнює сумарному помилковому спрацьовуванню. Звідси модель транспортної задачі приймає вид:

мінімізувати $F = \sum_{i=1}^{m+1} \sum_{j=1}^{n+1} c_{ij} q_{ij}$ при обмеженнях,

$$\sum_{i=1}^{m+1} q_{ij} \le a_j, j = 1,2,...,n+1 \quad \text{(пропозиція)},$$

$$\sum_{j=1}^{n+1} q_{ij} \le z_i, i = 1,2,...,m+1 \quad \text{(попит)},$$

де a_j, z_j – позитивні цілі числа, що задовольняють умову:

$$\sum_{j=1}^{n+1} a_j = \sum_{i=1}^{m+1} z_i .$$

Дана модель транспортної задачі має n+m+1 змінних. Для її рішення може бути використана одна з модифікацій симплекса-методу (метод потенціалів) [8].

III Висновки

Проведені дослідження дозволяють оцінити стійкість багато рубіжної комплексної системи технічного захисту. Отримані результати дають можливість з досить високою точністю оцінити ефективність розподілу ресурсів ТСЗІ між рубежами захисту при спрямованому і сконцентрованому подоланні визначеного рубежу.

Література: ***1****. Аналіз структури автоматизованої інформаційної системи ДПС України як об'єкту дослідження. Звіт про НДР частина 1, 2002р.* ***2****. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.* ***3****. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.* ***4****. Шорошев В. В., Ильницкий А. Е. Основы стратегии защиты информации в компьютерных системах / Бизнес и безопасность, 2000, №2.-с. 6-7.* ***5****. Хорошко В. А. Модель системы защиты информации./ Захист інформації,1999, №1.-с. 5–11.* ***6****. Арфкен Г. Математические методы в физике. - М.: Атомиздат, 1970.-712 с.* ***7****. Мину М. Математическое программирование. – М.: Наука, 1990.– 488 с.* ***8****. Сигорский В. П. Математический аппарат инженера. – К.: Техніка, 1975.-768 с.*

УДК 681.3

ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В ІНТЕРНЕТ

Михайло Гуцалюк
Міжвідомчий НДЦ при Координаційному комітеті по боротьбі з корупцією і організованою злочинністю при Президентові України

Анотація: **Розглянуто деякі аспекти захисту інформації в мережі Інтернет.**
Summary: **Some aspects of information safety in a network the Internet are considered.**
Ключові слова: **Інформаційна безпека, Інтернет, провайдер, браузер.**

I Вступ

Геополітична спрямованість сучасного цивілізаційного процесу визначається його глобалізацією, прогресуючим зростанням значущості гуманітарної сфери, високих інформаційних технологій,

постіндустріальних принципів суспільного розвитку [1]. За визначенням, поданим 1993 року Комісією Європейського Союзу, постіндустріальне, або "інформаційне суспільство" – це суспільство, в якому діяльність людей здійснюється на основі використання послуг, що надаються за допомогою інформаційних технологій та технологій зв'язку [2]. Пріоритетними завданнями державної політики у сфері інформаційної та телекомунікаційної інфраструктури є забезпечення випереджаючих темпів розвитку інфраструктури зв'язку, істотне вдосконалення національної мережі телекомунікацій, насамперед на базі новітніх вітчизняних технологій, їх інтегрування в глобальні інформаційні структури, у т. ч. в мережу Інтернет. Нагадаємо основні етапи розвитку цього соціально-технічного феномену [3].

При Міністерстві оборони США у 1958 році було створено Агентство Передових Дослідницьких Проектів (Advanced Research Projects Agency – ARPA), яке, зокрема, займалося дослідженнями в галузі забезпечення безпеки зв'язку і комунікацій у ході обміну ядерними ударами.

У 1961 році студентом Масачусетського Технологічного Інституту (Massachusetts Institute of Technology) Леонардом Клейнроком (Leonard Kleinrock) описано технологію, здатну розбивати файли на частини і передавати їх різними шляхами через мережу. Defence Advanced Research Agensy (DARPA – перейменована APRA, D (Defense) – оборона) за завданням міністерства оборони США приступило до проекту "Interneting Project" з створення експериментальної мережі передачі пакетів. Ця мережа, була названа ARPANET і призначалася спочатку для вивчення методів забезпечення надійного зв'язку між комп'ютерами різних типів для підтримки наукових досліджень у військово-промисловій сфері.

У 1963 році керівник комп'ютерної лабораторії ARPA Джон Ліклідер (J. C. R. Licklider) пропонує першу детально розроблену концепцію комп'ютерної мережі. 1967 року Ларі Робертс (Larry Roberts), практик, що втілює в життя теоретичні ідеї Ліклідера, пропонує зв'язати між собою комп'ютери ARPA. Починається робота над створення ARPANET.

У вересні 1969 року ARPANET запрацювала. До неї підключаються комп'ютери провідних, у тому числі і невоєнних, лабораторій і дослідницьких центрів США. 1974 року відкрито першу комерційну версію ARPANET – мережу Telenet. Основне, що відрізняє Internet від інших комп'ютерних мереж, це її протоколи – TCP/IP (транспортний та Інтернет-протоколи).

1982 року вийшов перший стандарт для протоколів TCP/IP, що ввійшов у військові стандарти, і всі, хто працював в мережі, зобов'язані були перейти до цих нових протоколів. Через деякий час TCP/IP був адаптований в загальнодоступний стандарт, і термін Internet увійшов у загальне вживання.

II Основна частина

Процес удосконалення глобальної мережі йде безперервно. Однак більшість цих перебудов відбувається непомітно для користувачів. Увімкнувши комп'ютер, ви не побачите оголошення про те, що найближчі півроку Internet не буде доступний через модернізацію. Кількість користувачів мережі почала зростати в геометричної прогресії після появи так званої "світової павутини".

1991 року Європейською фізичною лабораторією CERN створено відомий усім протокол – www – World Wide Web. Ця розробка була зроблена, насамперед, для обміну інформацією серед фізиків.

1993 рік. Марком Андресеном (Marc Andreesen) в Університеті штату Іллінойс (University of Illinois) створено перший Internet-браузер Mosaic. 1996 року почалося змагання між браузерами Netscape, створеним під керівництвом Марка Андресена, і Internet Explorer, розробленим компанією Microsoft.

1999 рік. У низці країн (Китай, Саудівська Аравія, Іран, Єгипет, країни колишнього СРСР) державними органами розпочато серйозні зусилля, щоб технічно блокувати доступ користувачів до визначених серверів і сайтів політичного, релігійного або порнографічного характеру.

2000–2003 роки. Значне зростання кількості користувачів мережі (понад 500 млн.) призвело водночас до поширення кіберзлочинності. В багатьох країнах розпочалося формування спеціальних правоохоронних підрозділів з боротьби з ними. Збитки від кіберзлочинності перевищують $ 100 млрд.

Розвиток мережі Internet в Україні.

У 1993 р. у Києві існувало 6 Internet-сайтів.

1995 р. користувачі масово почали міняти свої застарілі системи роботи з електронною поштою, відомою як UUPC, на сучасне програмне забезпечення (однак UUPC функціонує і досі: в країнах СНД цією доінтернетівською системою передачі користується не менше чверті абонентів). «Справжній Internet» почався з появою першого комерційного цифрового супутникового каналу з пропускною спроможністю 64 Кбіт/с. Він зв'язав вузол UA.NET із провайдером Demon у Лондоні.

Продовжує зростати інформаційне наповнення мережі. Web-сайт перестає бути «вотчиною» тільки Internet-провайдера. Крім чисто презентаційних сайтів різних фірм, з'являються і сайти з широким інформаційним наповненням: новини засобів масової інформації, законодавчі акти, огляди ринків різних товарів і послуг.

Жовтень 1996 року. Компанією «Глобал Юкрейн» запущено перший в Україні зовнішній супутниковий канал у 256 кілобіт на Америку (США).

На початку 1997 р. в Україні почали функціонувати справжні магістральні міжнародні канали. Одночасно розвивається мережа швидкісних цифрових каналів. Введення цифрових каналів Internet зв'язує Київ із регіонами.

Квітень 1999 року. В українському Internet'і з'явилася перша онлайн-газета – UAToday.Net. У вересні 1999 року з метою концентрації зусиль у сфері захисту інформації Указом Президента України створено Департамент спеціальних телекомунікаційних систем і захисту інформації СБ України (ДСТСЗІ СБУ).

21 листопада 2000 року. Пройшла державну реєстрацію Інтернет-асоціація України (ІнАУ). Асоціація була створена відповідно до загальних тенденцій розвитку Internet у світі і з метою консолідації зусиль задля розвитку Internet-ринку. Асоціація сприяє розвиткові українського сегмента глобальної мережі Internet, координує взаємодії учасників, пропагує, розробляє і впроваджує проекти, спрямовані на поліпшення умов функціонування ринку Internet-послуг.

Ефективному використанню в нашій державі можливостей глобальної мережі для розвитку науки, освіти, культури, підприємницької діяльності сприяє підписаний 31 липня 2000 року Президентом України Указ **«Про заходи щодо розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі в Україні»**. Указ, зокрема, передбачає встановлення та наповнення інформацією Веб-сторінок центральними органами виконавчої влади, створення належних економічних, правових, технічних умов для забезпечення широкого доступу до мережі громадян та юридичних осіб усіх форм власності.

Доступ до глобальної мережі Інтернет починає відігравати помітну роль у житті все більшої частини населення. Якщо у 1998 році кількість користувачів мережі Інтернет оцінювалась у 0,2 відсотка населення України, то сьогодні – близько 7 відсотків.

У 2003 році кількість хост-серверів у національному сегменті мережі Інтернет досягла 80 тис. Кількість веб-серверів в Україні становить на сьогодні близько 20 тисяч, кількість активних користувачів мережі Інтернет – 900 тис., а в цілому послугами мережі Інтернет з різною періодичністю користується близько 3,5 млн. жителів України. Зростає кількість українських інформаційних ресурсів, доступних через мережу Інтернет. Створено Урядовий веб-портал (Єдиний веб-портал органів виконавчої влади), який у 2003 році щодня відвідували понад 10 тис. користувачів. Активно відбувається процес розвитку веб-сайтів органів виконавчої влади, їх приведення у відповідність до встановлених вимог та інтеграція до Урядового веб-порталу [4].

Разом із позитивними досягненнями широке використання нових інформаційних технологій призвело до появи низки проблем.

- Комп'ютерні технології та міжнародні комп'ютерні мережі, які є необхідними складовими міжнародної фінансової та банківської діяльності, надали можливість вчинення злочинів економічного спрямування на національному та міжнародному рівнях.
- Організовані злочинні угрупування, представники "білокомірцевої" злочинності, інші кримінальні елементи використовують новітні технології для відмивання брудних коштів, фінансових махінацій, несанкціонованого доступу до інформаційних систем, поширення неправдивої інформації та інших правопорушень.

24 – 25 лютого 2004 року у м. Лондон проходив Другий міжнародний конгрес з проблем боротьби з кіберзлочинністю. Організатор конгресу – Національний центр з боротьби зі злочинами у сфері високих технологій (NHTCU – Великобританія). За оцінкою NHTCU у Великобританії 2003 року з 201 опитаних компаній 83% (167) стали жертвами комп'ютерних злочинців, що коштувало їм 195 мільйона фунтів стерлінгів; 62% опитаних зазнали збитків від Інтернет-шахрайства на суму 121 мільйон фунтів. З 44 опитаних фінансових компаній тільки три понесли збитки в розмірі 60 мільйонів фунтів від Інтернет-шахрайства; вірусні атаки стосувалися 77% опитаних і принесли збитки на суму 27,8 мільйона фунтів.

Серйозною проблемою для фінансово-кредитних установ є правопорушення у сфері обігу безготівкових електронних коштів. Так у листопаді 2002 року американські правоохоронці заарештували трьох осіб, які здійснювали електронні крадіжки грошей. Було доведено, що трійця пограбувала близько 30 тисяч американців на суму 2 мільйони 700 тисяч доларів. Хакери вираховували коди фінансових установ та банків, підробляли кредитні картки, виписували чеки та брали кредити. Слідчі вважають, що в історії США це найбільша афера з кредитними картками [5].

За даними американського Інституту комп'ютерної безпеки (Computer Security Institute), найбільш широко хакери використовують такі методи: підбір ключів, паролів (brute-force) – 13,9 % від загальної кількості; заміна IP-адрес (IP-spoofing) – 12,4 % (цей метод атаки передбачає заміну IP-адрес пакетів, що передаються в Internet, так, що вони виглядають як передані внутрішні повідомлення, де кожний вузол

довіряє адресній інформації іншого); ініціювання відмови в обслуговуванні (denial of service) – 16,3 % (вплив на мережу або її окремі частини з метою порушення порядку її штатного функціонування); аналіз трафіку (sniffer) – 11,2 % (прослуховування та дешифрування з метою збору інформації щодо ключів, паролів тощо); сканування (scanner) – 15,9 % (передбачає використання програми, яка перебирає можливі точки входження до системи); підміна, нав'язування, переупорядкування або заміна даних, що передаються мережею (data didling) – 15,6 %; інші методи – 14,7 %.

Для захисту інформації традиційно використовуються наступні методи: обмеження доступу, розмежування доступу, контроль і облік доступу, криптографічне перетворення інформації. Ці методи реалізуються завдяки апаратним та програмним рішенням.

Одним з напрямків забезпечення інформаційної безпеки можна вважати міжмережеві екрани (firewalls). Екран виконує свої функції, контролюючи всі інформаційні потоки між внутрішньою інформаційною системою та зовнішнім інформаційним простором як "інформаційна мембрана". Тобто, екран можна уявити собі як набір фільтрів, що аналізує інформацію, яка через нього проходить на основі певних алгоритмів, які приймають рішення про блокування інформації або її пересилання. Крім цього, така система може виконувати реєстрацію подій, зв'язаних з процесом розмежування доступу, зокрема фіксувати всі "незаконні" спроби доступу до інформації та сигналізувати про ситуації, які вимагають негайної реакції.

Відзначимо основні вимоги до таких систем:

забезпечення безпеки мережі і повний контроль над зовнішніми підключеннями і сеансами зв'язку;

система повинна мати гнучкі засоби керування для простого і повного втілення в життя політики безпеки організації і, крім того, для забезпечення простої реконфігурації системи при зміні структури мережі;

система має працювати непомітно для користувачів локальної мережі і не ускладнювати виконання ними легальних дій;

система має працювати досить ефективно і встигати обробляти весь вхідний і вихідний трафік у "пікових" режимах; це необхідно для того, щоб Firewall не можна було перевантажити великою кількістю викликів, що привели б до порушення її роботи;

система забезпечення безпеки має бути сама надійно захищена від будь-яких несанкціонованих впливів, оскільки вона є ключем до конфіденційної інформації в організації;

якщо в організації кілька зовнішніх підключень, у тому числі й у вилучених філіях, система керування екранами повинна мати можливість централізовано забезпечувати для них проведення єдиної політики безпеки.

Система Firewall повинна мати засоби авторизації доступу користувачів через зовнішні підключення. Система повинна вміти надійно розпізнавати легальних користувачів і надавати їм необхідний доступ до інформації.

У багатьох організаціях обмін даними з Internet централізовано контролюється брандмауером, які суміщені з маршрутизаторами, наприклад Solstice FireWall-1. Не зважаючи на це, через непрофесіоналізм адміністраторів приблизно 30 % зламів систем відбувається після встановлення захисних систем. При цьому складається помилкове враження захищеності. Останнім часом використовуються персональні брандмауери, які дозволяють здійснювати контроль за даними, які передаються в мережу (Norton Personal Firewall 2001, PGP Desktop Security 7.0, Sandbox Secure 4U Professional). При роботі з брандмауерами необхідно перш за все заблокувати всі порти комп'ютера і після цього відкрити тільки ті, які дійсно необхідні для роботи. Потрібно також активізувати протоколювання сигналів тривоги. При цьому прочитавши Log-файл можна взнати про всі спроби встановлення з'єднань.

Для блокування інформації, забороненої законодавчо (порнографія, насильство, расистські та військові заклики) використовують фільтруючі програми, такі як Arlington Custom Browser, Cyberpatrol, Web-broker та ін. Проте вони не завжди адекватно блокують певні сайти через недосконалі механізми визначення забороненої інформації.

Надзвичайно важливе значення в Інтернет мають засоби ідентифікації, адже отримавши їх правопорушник має можливість прочитати вашу електронну пошту, відправити листа від вашого імені, здійснити фінансові операції у віртуальному просторі.

Тому особисті паролі ні в якому разі не можна повідомляти ні усно ні електронною поштою. Забороняється запуск програм, вкладених в електронну пошту, якщо ви їх спеціально не замовляли. В них можуть бути вкладені троянські програми для отримання ідентифікаторів користувачів.

Якщо пароль скомпрометовано, необхідно негайно його змінити. Якщо самостійно це зробити неможливо, зверніться за допомогою до вашого провайдера.

Крім захисту паролю при роботі в Інтернет необхідно якнайменше надавати особистої інформації (номери телефонів, домашню адресу тощо), адже цією інформацією можуть скористатися зовсім незнайомі вам люди. Відомі випадки реальних кримінальних подій після віртуального знайомства.

Декілька слів слід сказати про конфіденційність роботи в Інтернет. Адже програми, пристосовані для полегшення роботи, можуть надавати інформацію про те, що ви робили в глобальній мережі. Перш за все це стосується журналу браузеру, який зберігає список інтернет-адрес, які ви відвідували. Тому необхідно час від часу "очищати" цей перелік (General, History, Clear). Для того, щоб записи взагалі не фіксувалися, необхідно використовувати опцію браузера "Відкрити сторінку" ("Open page") у вікні якого і вказати потрібну адресу.

Для прискорення завантаження інтернет-сторінок браузери зберігають на магнітному диску. Для того, щоб видалити зазначені файли, необхідно в меню "Сервіс" ("Tools") браузера на вкладці "General" натиснути клавішу "Delete Files".

Окремого розгляду заслуговують файли "cookie". Ці файли створюються Web-серверами для запису інформації про дату та час перегляду сторінок, які саме сторінки переглядалися, паролів користувача та ін. Ця інформація використовується для аналізу статистичних даних та створення так званих профілів користувачів (які сторінки переважно переглядає користувач, які товари замовляв тощо). Тому для припинення такої діяльності використовують або знищення файлів "cookie" на вашому вінчестері, або блокування цих файлів завдяки опціям браузерів (Edit>Preferences>Advanced>Disable Cookies).

При роботі з Інтернет слід бути також досить обережним зі сторінками, які використовують елементи ActiveX, Java та JavaScript. Для підвищення безпеки необхідно відключити їх в меню браузера (Tools > Internet Options > Security > Setting).

Сьогодні вкрай важливими стають наукові дослідження з зазначеної проблематики. Після подій 11 вересня, як заявив Шервуд Белерт, голова Наукового комітету адміністрації Білого дому на перший план стають питання безпеки, у тому числі комп'ютерної. Тому Конгрес США схвалив триразове збільшення фінансування досліджень в галузі запобігання комп'ютерним злочинам. Протягом наступних п'яти років Національному дослідницькому фондові і Національному інститутові стандартизації і технологій будуть виділені 900 мільйонів доларів, у першу чергу, на підготовку наукових кадрів. "Стабільні довгострокові асигнування дозволять залучити більше вчених для розробок в галузі комп'ютерної безпеки" - повідомив Білл Вульф, ректор Національної інженерної академії [6].

Документ "Національна стратегія в сфері безпеки кіберпростору" був представлений радником президента Буша з кібербезпеки Річардом Кларком. Програма підкреслює роль індивідуальних і корпоративних користувачів у забезпеченні безпеки Інтернету і "життєво важливої для країни інфраструктури". Програма закликає інтернет-провайдерів, виробників програмного й апаратного забезпечення, постачальників послуг і т. д. до створення Центра мережних операцій у кіберпросторі (Cyberspace Network Operations Center). Його задачею, крім іншого, стане забезпечення безпеки Всесвітньої мережі. Серед інших заходів, включених у програму – створення підрозділами національної безпеки і силових відомств США системи попередження широкомасштабних кібератак [7].

В Україні Указом Президента «Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 р. "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України"» № 193/2001 від 6 грудня 2001 р. передбачено створення Міжвідомчого центру з питань боротьби з комп'ютерною злочинністю (МЦПБКЗ).

Кабінетом Міністрів України за пропозицією МВС, СБУ, Міністерства фінансів, Держкомзв'язку та інформатизації України пропонується створити відповідний Центр при Координаційному комітеті по боротьбі з корупцією і організованою злочинністю при Президентові України.

III Висновки

У Міжвідомчому НДЦ з проблем боротьби з організованою злочинністю при Координаційному комітеті наявний відповідний досвід дослідження зазначених проблем. В рамках теми “Координація діяльності органів влади у боротьбі з кіберзлочинністю” науковцями МНДЦ підготовлено проект Концепції стратегії реалізації державної політики щодо боротьби з кіберзлочинністю [8]. Рішенням Урядової комісії з питань аналітичного забезпечення органів виконавчої влади 6 жовтня 2000 р. прийнято за основу проект Концепції реформування законодавства України у сфері суспільних інформаційних відносин. Разом з тим, необхідно підкреслити, що створення підрозділу з питань боротьби з комп’ютерною злочинністю на базі Міжвідомчого НДЦ виявиться значно дешевшим за створення ще одного самостійного Міжвідомчого центру.

*Література: **1**. Послання Президента України до Верховної Ради України „Європейський вибір. Концептуальні засади стратегії економічного та соціального розвитку України на 2002 –- 2011 роки” // Урядовий кур'єр, 2002, –- № 100 4 червня .**2**. Європа на шляху до інформаційного суспільства. Збірник документів Європейської комісії 1994 – 1995 рр. – К. 2000. – С. 5. **3**. Комп’ютерна злочинність. Навчальний посібник / Біленчук П. Д., Бут В. В., Гавловський В. Д., Гуцалюк М. В., Романюк Б. В., Цимбалюк В. С. – Київ:*

*Атіка, 2002. – 240 с. **4**. Доповідь Кабінету Міністрів України Верховній Раді України про стан та розвиток інформатизації в Україні за 2003 рік. **5**. http:// www.1plus1.net. **6**. http://www.crime-research.org.**7**. http://itware.com.ua. **8**. В. Бутузов, М. Гуцалюк, В. Цимбалюк Протидія злочинності у сфері високих технологій // Міліція України. – 2002, –- № 9. – С. 20 – 21.*

УДК 681.3

ОЦІНКА СТАНУ БЕЗПЕКИ ІНФОРМАЦІЇ ЗА СТАНДАРТНИМИ ПРОФІЛЯМИ ЇЇ ЗАХИЩЕНОСТІ В КОМП'ЮТЕРНИХ (АВТОМАТИЗОВАНИХ) СИСТЕМАХ

В'ячеслав Шорошев
НДІ Національної академії внутрішніх справ України

Анотація: **Висвітлюються необхідність, правила та проблеми створення каталогу стандартних профілів захищеності інформації в комп'ютерних системах усіх класів і підкласів.**
Summary: **The rules and problems of creation of standard structures of security of the information in computer systems of all classes and subclasses are shined (covered) necessity.**
Ключові слова: **Послуги безпеки, підклас АС (КС), профіль захищеності інформації, конфіденційність, цілісність, доступність, спостереженість інформації.**

Проблема оцінки стану безпеки інформації в комп'ютерних (автоматизованих) системах дуже актуальна як в нормативно-правовому і системно-концептуальному, так і в суто практичному плані.

Справа в тому, що багатий міжнародний досвід інвестиційних програм США, Канади, Англії, Німеччини, Франції, Нідерландів щодо розробки, удосконалення, уніфікації та стандартизації критеріїв комп'ютерної безпеки свідчить про те, що безпека інформації, оброблюваної в комп'ютерних системах, і надалі була, є і буде вічною проблемою для трьох основних категорій: розробників, користувачів й експертів кваліфікаційного аналізу захищених комп'ютерних систем.

За вказаний проміжок часу проблема визначення та уніфікації критеріїв для експертної оцінки стану безпеки інформації в комп'ютерних системах витримила ряд кардинальних концептуальних змін, але ми зосередимося тільки на двох із них, які були використані у вітчизняних нормативних документах з питань технічного захисту інформації та одержали подальший розвиток.

Перша полягала в переході від простої універсальної шкали критеріїв комп'ютерної безпеки (шість критеріїв С1, С2, В1, В2, В3, А1 для стандарту TCSEC, США, 1983 р. та десять критеріїв F-C1, F-C2, F-B1, F-B2, F-B3, F-1N, F-AV, F-DI, F-DC, F-DX для європейських критеріїв ITSEC, 1991 р.) до великої сукупності часткових критеріїв (160 - для Федеральних критеріїв FCITS, США, 1992 р., 70 – для Канадських критеріїв CTCPEC, 1993 р., 280 – для Єдиних міжнародних критеріїв CCITSE, 1996 р.). Цей кращий досвід розвитку міжнародних критеріїв (європейських ITSEC та канадських CTCPEC) було враховано при розробці вітчизняних критеріїв. Так, в нормативних документах з питань технічного захисту інформації від несанкціонованого доступу Департаменту СТСЗІ Служби безпеки України, презентація яких відбулась в 1999 р., таких часткових критеріїв було визначено 110 [1, 2, 4 – 7].

Друга зміна була реалізована в канадських критеріях і полягала в концептуальному визначенні основної універсальної компоненти безпеки – "тег" (tag). Поняття "тег" визначає сукупність атрибутів безпеки, асоційованих з користувачем, процесом або об'єктом. У вітчизняних НД ТЗІ 2.5-004-99 це більш вдало й інформативно реалізовано шляхом регламентування та визначення в простому таблично-текстовому форматі низки так званих "профільних" послуг безпеки різних видів та рівнів (наприклад, послуг конфіденційності довірчої КД рівнів 1...4 та конфіденційності адміністративної КА рівнів 1…4, послуг цілісності довірчої ЦД рівнів 1…3 та цілісності адміністративної ЦА рівнів 1…3, послуг доступності інформації щодо використання ресурсів виду ДР рівнів 1…3, послуг спостереженості інформації та ресурсів щодо цілісності комплексу засобів захисту НЦ рівнів 1…3, щодо реєстрації НР рівнів 1…5, тощо). Кількість, види та рівні профільних послуг безпеки визначають собою так званий стандартний функціональний профіль захищеності інформації (СПЗІ) в автоматизованих (комп'ютерних) системах (АС, КС) різних класів та підкласів. А певний склад СПЗІ вже функціонально регулює стан безпеки інформації в певній захищеній АС, КС [1 – 2].

У провідних західних країнах вже створені каталоги профілів захисту та проектів захисту (профілі захисту плюс специфікації функцій захисту) як обов'язкових нормативних документів щодо стандартизації усіх компонентів ІТ-продуктів (продуктів інформаційних технологій), тобто стандартизації апаратних, програмних та спеціальних засобів, що реалізують функції захисту інформації в комп'ютерних системах. В