міжнародних критеріїв CCITSE в 1996 р., що розроблялись шістьома провідними західними країнами, тільки через рік була опублікована відповідна методика оцінки захищеності інформації в комп'ютерних системах.

3. Використання базової моделі експертної системи штучного інтелекту забезпечує найбільші переваги щодо автоматизованої підтримки прийняття експертного рішення за багатьма критеріями стосовно поточного чи належного стану безпеки оцінюваної комп'ютерної системи. Досягається це її унікальним сервісом для користувачів щодо самонавчання, надання консалтингових послуг, прийняття найбільш раціонального рішення в режимі інтерактивного дружнього інтерфейсу шляхом використання системи меню і підменю на базі CASE-технології Delphi тощо.

4. Ядром базової моделі експертної системи є множина певних "правил", серед яких базовими визначаються СФПБ-, СПГБ-, СФПЗ-, ПРБК-правила, додатковими – НПЗІ-правила.

5. Ядром програмного забезпечення базової моделі експертної системи мають бути програмні модулі забезпечення функціонування визначеної вище множини правил, а також візуально-графічна система меню і підменю CASE-технології Delphi.

6. Базова модель експертної системи може бути інструментальною базою для реалізації методики оцінки захищеності інформації комп'ютерних систем від загроз НСД.

Література: 1. Д. Уотермен. Руководство по экспертным системам. Издательство "Мир", М. 1998. 2. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99 р. № 22. Чинний від 01. 07. 1999 р. 3. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28. 04. 99 р. № 22. Чинний від 01. 07. 1999 р. 4. В. В. Шорошев, А. Е. Ильницкий, И. Л. Близнюк. Защита информации компьютерных систем от угроз НСД и национальные критерии ее экспертной оценки. Бизнес и безопасность. № 6, 2000.

УДК 681.3

БЕЗПЕКА ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА ДЕЯКІ ПІДХОДИ ДО ЇЇ ЕКСПЕРТНОЇ ОЦІНКИ

Анатолій Ільніцький
НДІ НАВСУ

Анотація: **Розглядаються системно-концептуальні підходи щодо експертної оцінки безпеки інформації в комп'ютерних системах.**
Summary: **In the article the approaches of a rather expert evaluation of safety of the information in computer systems are considered system-conceptual.**
Ключові слова: **Безпека інформації, системно-концептуальна ієрархія, послуги безпеки, експертна оцінка, принципи оцінки.**

Забезпечення захисту інформації, яка оброблюється в комп'ютерних системах органів внутрішніх справ (ОВС), – актуальна проблема, для вирішення якої необхідні певні витрати як фінансових, так і інших ресурсів. В статті висловлюється ряд пропозицій і рекомендацій щодо реалізації захисту інформації.

Перше питання, що виникає перед керівником будь-якої структури чи підрозділу ОВС – як забезпечити захист інформації надійно і дешево. Адже витрати на захист складають тепер від 10% до 30% собівартості комп'ютерної системи. Проти цього заперечувати дуже важко. Краще надійніше і популярніше викласти свої пропозиції і, що дуже бажано, не просто у вигляді набору проблем, а науково-обґрунтовані і перспективні варіанти їх рішення. Це необхідно, насамперед, для розроблювачів, експертів кваліфікаційного аналізу, власників, а також і для масових користувачів захищених комп'ютерних систем.

Що потрібно мати на увазі в першу чергу, виконуючи неминучу процедуру оцінки поточного стану безпеки інформації, і не тільки оброблюваної, а і, що важливо підкреслити, розповсюджуваної у своїй комп'ютерній системі. Поняття обробки інформації, як правило, включає і передачу інформації, але іноді не зайво виділити її в самостійний компонент безпеки, з огляду на той факт, що на сьогодні проблема безпеки каналів зв'язку є поки самою слабкою ланкою в реалізації безпеки інформації комп'ютерних систем.

Перша проблема – від яких загроз потрібно перевіряти ефективність захисту своєї комп'ютерної системи. Ці загрози специфічні і вони відомі керівнику чи фахівцю ТЗІ певної структури або підрозділу ОВС. Але це, на жаль, ще не все. Необхідно, крім специфічних, визначити ще потенційні загрози, захист від

яких є обов'язковим згідно з вимогами чинних нормативно-правових засад, насамперед, нормативних документів НД ТЗІ (захист від несанкціонованого доступу) Департаменту СТСЗІ СБУ [1, 2]. Це захист від загроз конфіденційності, цілісності, доступності, спостереженості і гарантії безпеки інформації у своїх КС. Експертну оцінку захисту від цих потенційних і специфічних загроз рекомендується робити за національними критеріями захищеності інформації від несанкціонованого доступу НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99. Додатково, для аналітичного порівняння експертну оцінку також можна робити за міжнародними критеріями TCSEC, ITSEC, CCITSE [3].

Друга проблема – яку найбільш далекоглядну стратегію оцінки безпеки інформації у своїй відомчій комп'ютерній системі взяти за основу. Іншими словами – як і з якою періодичністю робити оцінку (вибірково, планово, контрольно-оглядово тощо), за якими критеріями, а саме – вітчизняні критерії (більш 110 часткових показників згідно з НД ТЗІ 2.5-004-99), або досить проста універсальна 6–10 бальна шкала безпеки критеріїв TCSEC, ITSEC, чи шкала більш 280 часткових показників найкращих міжнародних критеріїв CCITSE (стандарт ISO/IEC 15408), з використанням яких методик, наскільки доступно і просто, з якою гарантією для безпеки і т. д.

Відповіді на ці питання не прості і вимагають певних рекомендацій. Звичайно, найпростіше запропонувати набір конкретних засобів чи систем захисту (і це вкрай необхідно), але це не далекоглядніше рішення. Рекомендації з вибору засобів і систем захисту необхідні, але це окреме проблемне питання і тема окремої статті. Важливіше, на наш погляд, визначити базові варіанти рішення самої проблеми експертної оцінки безпеки інформації в комп'ютерних системах. Наскільки це дуже складна проблема і в науковому, і в інвестиційно-фінансовому плані, можна судити вже по тому, що кооперація шести провідних західних країн, починаючи з 1983 року понад 14 років послідовно розробляла, удосконалювала і впроваджувала всього п'ять міжнародних критеріїв безпеки комп'ютерних систем (TCSEC, ITSEC, FCITS, CTCPEC, CCITSE).

Які ж можливі шляхи рішення цієї проблеми. Безумовно, що кращий міжнародний досвід треба використовувати, але тільки в плані подальшого розвитку та удосконалення наших вітчизняних нормативно-правових засад з питань захисту інформації в комп'ютерних та автоматизованих системах. Основи стратегії, передусім, передбачають визначення системно-концептуальних положень, правил, вимог, першочергових напрямів державної та відомчої політики з питань забезпечення безпеки інформації, що обробляється, з використанням новітніх комп'ютерних технологій і згідно з вимогами вітчизняних нормативно-правових засад.

На рис. 1 представлено правило системно-концептуальної ієрархії основ стратегії експертної оцінки безпеки інформації в комп'ютерній системі (правило СкіосЕо-1). Ця багаторівнева системно-концептуальна ієрархія декомпозована п'ятьома базовими рівнями.

На **першому рівні** ієрархії основ стратегії експертної оцінки визначається, що вона, згідно з вимогами НД ТЗІ Департаменту СТСЗІ СБУ, повинна здійснюватися за трьома напрямками:

* оцінка функціональних послуг безпеки інформації в певній комп'ютерній системі (КС) органів внутрішніх справ;
* оцінка послуг безпеки стандартних функціональних профілів захищеності оброблюваної інформації в певній КС;
* оцінка послуг гарантії безпеки інформації в певній КС.

При цьому **першим понятійним компонентом,** важливим для експертної оцінки, визначаються так звані **"послуги безпеки".** На першому рівні ієрархії відповідно до правила СкіосЕо-1 визначаються три таких послуги безпеки – функціональні послуги безпеки, послуги безпеки стандартних функціональних профілів захищеності інформації і послуги гарантії безпеки КС. Надалі ці послуги безпеки, в свою чергу, розділяються на підпослуги безпеки другого, третього і т. д. рівнів ієрархії. Послуги і підпослуги безпеки за альтернативним правилом "так-ні" оцінюються:

* рейтинговою шкалою часткових **критеріїв-вимог** таблично-текстового формату відповідно до положень НД ТЗІ 2.5-004-99 "Критерії захищеності інформації від несанкціонованого доступу в комп'ютерних системах";
* рейтинговою шкалою часткових **критеріїв-профілів** теж таблично-текстового формату відповідно до положень НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу".

Другим понятійним компонентом, принципово важливим для реалізації стратегії експертної оцінки безпеки інформації в КС, визначаються так звані системно-концептуальні **"правила"**. Справа в тому, що правила є необхідною складовою частиною політики безпеки КС, під якою розуміють сукупність законів, норм і правил, що визначають порядок обробки, захисту і поширення інформації в будь-якій КС.

В подальшому на **інших рівнях** системно-концептуальної ієрархії правил СкіосЕо-1 визначаються базові компоненти, що забезпечують найбільш успішну реалізацію основ стратегії експертної оцінки безпеки

інформації в КС, а саме – концептуальність, системність, принципи і можливі варіанти практичної реалізації експертної оцінки.

На **другому рівні** ієрархії визначається, що реалізація **концептуальності** експертної оцінки безпеки інформації в КС забезпечує найбільш раціональне об'єднання і єдність різних варіантів рішень експертної оцінки. Концептуальність експертної оцінки досягається розробкою і використанням:

* нормативно-правових рішень експертної оцінки, у тому числі з обліком накопиченого світового досвіду рішення цієї проблеми;
* новітніх програмно-технічних рішень експертної оцінки безпеки інформації в комп'ютерних системах на рівні кращих вітчизняних і світових досягнень;
* організаційних рішень експертної оцінки;
* інших рішень експертної оцінки безпеки інформації в КС (ергономічних, управлінських, перспективних).

До таких рішень, насамперед, можна віднести облік і реалізацію вимог нормативно-правових документів з питань ТЗІ, використання програмно-апаратних модулів і засобів для моніторингу й експертної оцінки стану безпеки інформації в даній КС, визначення порядку організації і документування контрольно-наглядових, вибіркових, ремонтно-регламентних і інших робіт, контролів, перевірок і т. д.

На **третьому** рівні ієрархії визначається, що реалізація **системності** експертної оцінки безпеки інформації в КС забезпечує:

* упровадження, розробку і реалізацію експертної оцінки з єдиних методологічних позицій (методи моделювання, математичні методи оптимізації рішень, об'єктивність і суб'єктивність оцінки);
* системний облік всіх умов і факторів, що впливають на експертну оцінку (потенційні і перспективні загрози безпеки КС, їхня пріоритетність, внутрішнє і зовнішнє середовище ТЗІ, типовий стандартний чи специфічний склад програмно-апаратного і телекомунікаційного забезпечення і т. д.);
* розгляд у єдиному комплексі всіх питань експертної оцінки (оцінка функціональних послуг безпеки, оцінка стандартних функціональних профілів захищеності, оцінка послуг гарантії безпеки, ухвалення експертного рішення).

На **четвертому** рівні ієрархії зазначається, що успішність експертної оцінки безпеки інформації в КС досягається завжди, якщо базовими принципами експертної оцінки будуть її **конкретність, легітимність, комплексність, безперервність, суб'єктивність, достатність і вірогідність.**

Необхідність реалізації принципу **конкретності** експертної оцінки обумовлюється тим, що універсальних оцінок, як і засобів, систем ТЗІ, не існує, кожна з них здійснюється і реалізується:

* для конкретного класу КС: персональних ЕОМ, робітників станцій обчислювальної мережі (1 клас); локальних обчислювальних мереж LAN (2 клас); глобальних (територіально-розподілених) обчислювальних мереж WAN (3 клас);
* для визначеного внутрішнього і зовнішнього середовища КС;
* для визначених потенційних загроз безпеці інформації визначеної КС;
* під реалізацію конкретних функціональних вимог, вимог стандартних функціональних профілів захищеності і вимог гарантії безпеки інформації КС.

Реалізація принципу **легітимності** експертної оцінки означає (гарантує), що вона базується на положеннях і вимогах діючих нормативно-правових документів з питань ТЗІ.

інших рішень щодо забезпечення безпеки інформації в КС різних класів, рівнів і призначення.

Реалізація принципу **безперервності** експертної оцінки безпеки інформації в КС означає, що вона буде забезпечуватися:

* на всіх етапах життєвого циклу КС;
* в усіх режимах роботи захищеної КС;
* у тому числі при проведенні ремонтно-регламентних робіт.

Реалізація принципу суб'єктивності **експертної оцінки безпеки інформації в КС означає, що:**

* експертна оцінка може здійснюватися ручним, автоматизованим чи автоматичним способом, але остаточне рішення завжди приймається людиною-експертом (фахівець ТЗІ);
* при експертній оцінці завжди враховується фактор суб'єктивності прийняття рішень людиною-експертом, для чого використовуються методи теорії прийняття рішень [4];

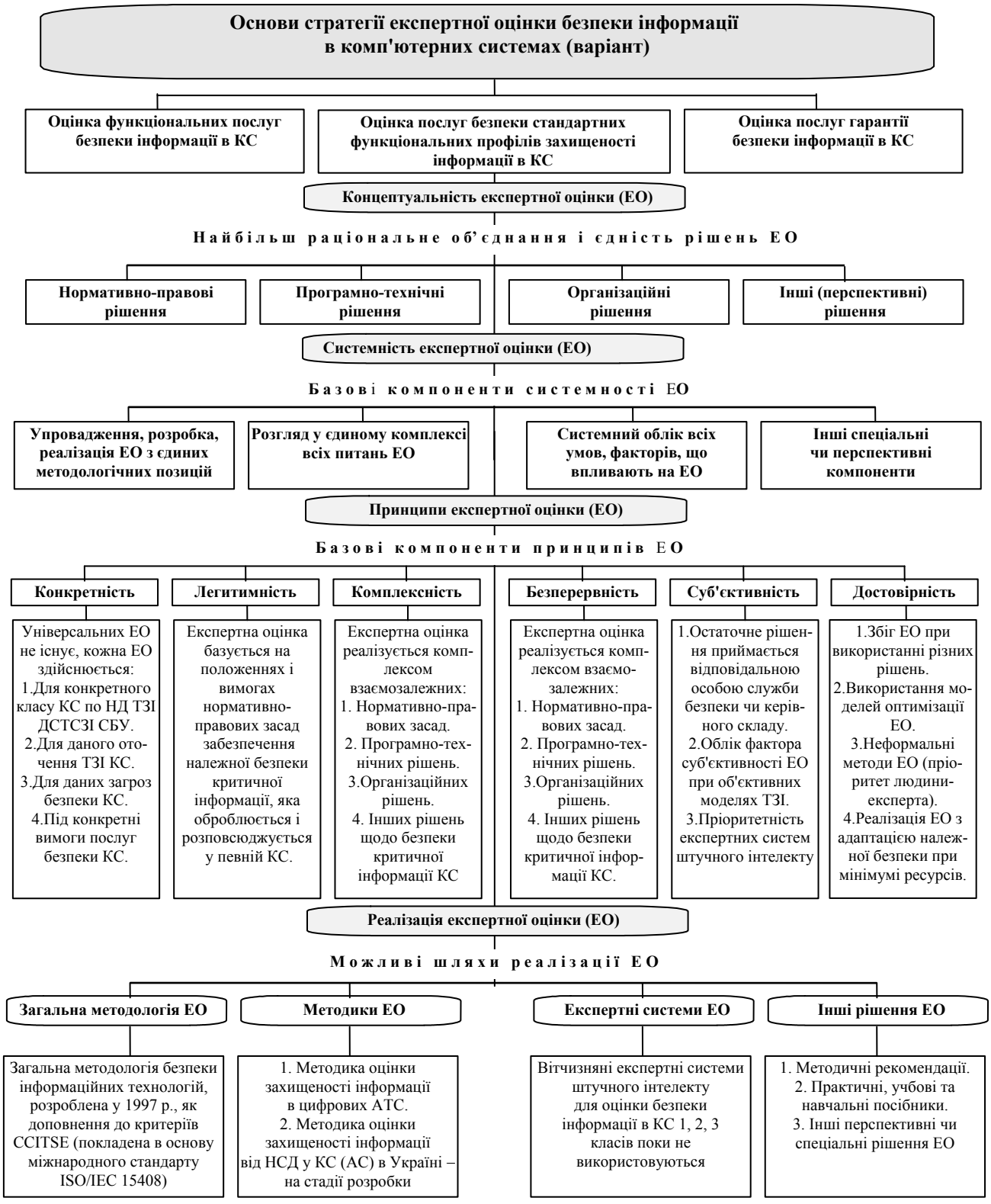

Рисунок 1 – Системно-концептуальна ієрархія основ стратегії експертної оцінки безпеки інформації в КС (правило СкіосЕо-1)

* для моделювання експертної оцінки найбільш доцільно використовувати експертні системи штучного інтелекту, їх іноді називають системами колективного розуму, що найбільше здатні враховувати

індивідуальні особливості ухвалення рішення людиною-експертом.

Реалізація принципу **вірогідності** експертної оцінки безпеки інформації в КС означає, що:

* для експертної оцінки повинні використовуватися різні методи прийняття рішень;
* забезпечується збіг результатів експертної оцінки при різних методах;
* використовуються неформальні методи оптимізації рішення для систем, де людина займає пріоритетне місце; при таких методах шукається не просто оптимальне рішення, а найбільш раціональне для визначених умов, факторів і параметрів системи для досягнення поставленої мети і придатне для широкого класу задач і умов експертної оцінки.

На **п'ятому рівні** ієрархії визначається, що можливими шляхами реалізації експертної оцінки безпеки інформації в КС можуть бути:

* розробка і використання для оцінки загальної методології безпеки інформаційних технологій; такий варіант реалізації експертної оцінки використовується в Єдиних міжнародних критеріях CCITSE, 1996–1997, що також покладені в основу міжнародного стандарту ISO/IEC 15408;
* методика експертної оцінки захищеності (безпеки) інформації від несанкціонованого доступу в комп'ютерних системах; така методика як нормативний документ Департаменту СТСЗІ СБУ поки на стадії розробки ;
* експертна оцінка безпеки інформації в КС із використанням експертних систем штучного інтелекту; досвід їхнього застосування показує, що вони найбільш перспективні для автоматизації і підвищення гарантії експертної оцінки;
* інші рішення експертної оцінки, до яких можна віднести перспективні і спеціальні методи, засоби автоматизованої підтримки прийняття рішень, наприклад, системи підтримки прийняття колективних рішень, конференції з прийняття рішень (decision conference), що, наприклад, уже використовуються Центром з прийняття рішень Лондонської школи економіки і політичних наук [5].

Таким чином, розглянуті шляхи рішення проблеми експертної оцінки безпеки інформації в комп'ютерних системах свідчать про те, що невирішених питань ще багато як у теоретичному, так і в практичному плані. Обговорення цієї проблеми в наступному доцільно продовжити.

Література: 1. Пакет з п'яти нормативних документів щодо захисту інформації від несанкціонованого доступу, Департамент СТСЗІ СБ України, Київ, 1999 р. 2. Шорошев В. В., Ильницкий А. Е., Близнюк И. Л. Защита информации компьютерных систем от угроз НСД и национальные критерии ее экспертной оценки. Бизнес и безопасность № 6, 2000 г., с. 5–6. 3. Ж-л ББ-4-1998, с. 28–32, ББ-1-1999, с. 10–12. 4. Тарасов Г. П., Шорошев В. В., Ильницкий А. Е. Технологическая карта испытаний компьютерных систем на соответствие требованиям оцениваемого класса безопасности по международным критериям ITSEC, TCSEC. Бизнес и безопасность № 4, 1998 г., с. 28–32. 5. Ларичев О. И. Объективные модели и субъективные решения. Издательство ВНИИ системных исследований АН СССР "Наука", М., 1987.

УДК 681.3.06:519.248.681

АНАЛИЗ МЕТОДОВ И СРЕДСТВ ЗАЩИТЫ ОТ НСД

Александр Замула, Виктор Руженцев

Харьковский национальный университет радиоэлектроники

Акционерное общество «ИИТ»

Анотація: **Сформульовано концепцію забезпечення безпеки інформації в автоматизованих системах її обробки. Розглядаються основні проблеми, пов'язані з забезпеченням інформаційної безпеки. Оскільки сьогодні майже всі нові розробки систем обробки даних ведуться на основі ПЕОМ, однією з основних складових підсистеми інформаційної безпеки є підсистема захисту локальних робочих місць. Тому особлива увага приділяється саме цій підсистемі.**

Summary: **The main task of this report is to propose the conception of information security in automatized systems. The main problems of information security are considered in this report. Most of all modern information systems consist of local personal computers. That is why subsystem of security of local computers considered in report especially thoroughly.**

Ключевые слова: **Информационно-телекоммуникационные системы, несанкционированный доступ, локальная рабочая станция, программно-аппаратный комплекс, система защиты информации.**