Генератор предназначен для управления антенным коммутатором. В его состав входят мультивибратор на частоту 600 Гц и триггер, а также схема, контролирующая работу генератора и вырабатывающая сигнал "авария" в случае его отказа.

Фильтр F_k с компаратором предназначен для выявления сигнала с частотой коммутации антенн и подачи команды на остановку перестройки радиоприемного устройства. При обнаружении сигнала с частотой коммутации обеспечивается звуковая и световая сигнализация. В состав блока обнаружителя входят фильтр, пороговое устройство и схема сигнализации. Выделенный сигнал коммутации выпрямляется, и, если его уровень превышает установленный порог, производятся при необходимости включение сигнализации и выработка напряжения "остановка" для прекращения перестройки приемника. Обнаруженное ПЭМИ замеряется и анализируется. В режиме "измерение" на вход приемника подается напряжение от дальней антенны ($A2$), находящейся вблизи границы охраняемой зоны. Зная коэффициенты передачи антенны, радиоприемника, коммутатора и предварительно откалибровав радиоприемное устройство на данной частоте, определяем напряженность поля побочного излучения

$$E = \frac{U_{\text{вых1}}}{K_{\text{пр}} K_{\text{А}} K_{\text{ком}} h_{\text{д}}}, \left[\frac{\text{мкВ}}{\text{м}}\right],$$

где $K_{\text{пр}}$ – коэффициент передачи радиоприемного устройства; $K_{\text{А}}$ – коэффициент передачи активной антенны; $K_{\text{ком}}$ – коэффициент передачи коммутатора; $h_{\text{д}}$ – действующая высота антенны.

Полученное значение напряженности электрического поля сравнивается с допустимым. Если уровень превышает допустимый, то производится информационный анализ излучения, в результате чего определяется тип аппарата, а затем и сам конкретный аппарат.

В случае автоматического постоянного поиска при обнаружении ПЭМИ ПЭВМ записывает частоту РПУ в таблицу, определяет степень опасности излучения по приведенному выше принципу, записывает полученные данные в таблицу, выделяя степень опасности цветом.

IV Выводы

Проведенные эксперименты подтвердили ожидаемые результаты:

- максимальная чувствительность системы определяется чувствительностью радиоприемного устройства и уровнем сигнала на выходе антенны $A1$;
- при малых значениях ПЭМИ, когда уровень сигнала на выходе антенны $A2$ $U_{\text{вых}A2}$ меньше чувствительности радиоприемного устройства, а на выходе антенны $A1$ $U_{\text{вых}A1}$ выше (что характерно для ближней зоны распространения радиоволн), глубина модуляции сигнала с F_k достигает 100%, что можно использовать как признак того, что уровень излучения ПЭМИ за пределами контролируемой зоны ниже чувствительности радиоприемного устройства, т. е. ниже опасного уровня.
- порог компарации зависит от области исследуемого диапазона радиочастот – на верхних частотах диапазона порог компарации следует снижать. Это объясняется зависимостью размеров ближней, промежуточной и дальней зоны распространения радиоволн от длины волны.

Литература: 1. Я. Л. Альперт, В. Л. Гинзбург, Е. Л. Фейнберг. Распространение радиоволн М., Гос. изд-во технико-теоретической литературы, 1953. 2. М. П. Долуханов. Распространение радиоволн М., "Сов. радио", 1972 – 118 с.

УДК.681.3

БАЗОВА МОДЕЛЬ ЕКСПЕРТНОЇ СИСТЕМИ ОЦІНКИ БЕЗПЕКИ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

Вячеслав Шорошев
НДІ НАВСУ

Анотація: **Розглядається базова модель експертної системи оцінки безпеки інформації в комп'ютерних системах згідно з вимогами національних стандартів ТЗІ України. Обраний Україною шлях наслідування кращого міжнародного досвіду та запобігання їх недолікам щодо комп'ютерної безпеки заслуговує уваги. Прикладом цієї реалізації є нормативні документи НД ТЗІ з**

питань захисту інформації від загроз НСД, які покладені в основу критеріїв оцінки при розробці правил базової моделі експертної системи.
Summary: **The base model of the consulting model for an evaluation of safety of the information in computer systems under the requirements of the national standards TPI of Ukraine is considered. It is necessary to notice, that selected the path of Ukraine concerning inheriting the best international experience and avoidance of their defects of rather computer safety deserves attention. An example of this realization are the normative documents on problems of protection of the information from threats UAA, which are fixed in the basis of criterions of an evaluation at development of rules of base model of the consulting model.**
Ключові слова: **Базова модель, експертна система, технічний захист інформації (ТЗІ), загрози несанкціонованого доступу (НСД), експертна оцінка, база знань, конфіденційність, цілісність, доступність, спостереженість.**

І Вступ

Ядром розроблюваної базової моделі експертної системи, як і будь-якої іншої [1], є база знань, механізм логічного висновку та інтерактивний дружній інтерфейс користувача. Їх функціонування в базовій моделі засновано на використанні певної множини так званих "правил" експертної оцінки послуг безпеки певної комп'ютерної системи (КС). Унікальною особливістю експертних систем, як систем штучного інтелекту, є їх здатність "модифікувати" накопичені знання, виконувати функції "колективного розуму" експертів та зростаюча ефективність результатів при поступовому зростанні загального терміну експертного оцінювання послуг безпеки певної КС.

Ті фахівці або особи керівного складу, хто мав будь-яку причетність до експертних систем штучного інтелекту, поступово починають розуміти, що їх сила полягає у спроможності надавати певним фахівцям всі умови для систематизації та максимально ефективної демонстрації своїх знань, які самі по собі мають велике значення. Експертні системи призначені вирішувати задачі, де неможливо обійтися без додаткової спеціальної експертизи, без експерта-людини.

Наприклад, фахівцям випадає вирішувати задачі щодо безпеки КС, які нечітко визначені, або коли визначені не всі частки "складу" комп'ютерного злочину, коли певні діяння порушників безпеки можуть не регулюватись чинними нормативно-правовими засадами або необхідна додаткова експертиза і т. д.

Таким чином, згідно з цільовим призначенням розроблюваної базової моделі експертної системи, можна визначити, що множина правил для бази знань, механізму логічного висновку та інтерактивного інтерфейсу користувача повинна забезпечувати, з одного боку, їх високу швидкодію, вірогідність і надійність в роботі, а з іншого боку, рішення як прямих, так і зворотних задач експертної оцінки.

Зворотні задачі експертної оцінки мають дуже важливе практичне значення для автоматизованої адаптації належного рівня безпеки КС. Наприклад, такі задачі завжди використовуються для консалтингових послуг щодо виявлення причин та наслідків незадовільного стану безпеки оцінюваної КС. Але при рішенні таких задач виникає проблема забезпечення однозначності і вірогідності експертних оцінок.

Найбільш коректно такі задачі вирішуються при **процедурній** формі подання знань за правилом: if (...), then (...), тобто "якщо ... (умова), то ... (твердження)". Але зі збільшенням множини процедурних правил швидкодія експертної системи значно знижується.

При **фреймовій** формі подання знань (правил) швидкодія експертної системи на декілька порядків більша, ніж при процедурній формі. Але при рішенні прикладних задач однозначність результатів забезпечується не завжди. Наприклад, при фреймовій формі подання знань для фрейму з ім'ям КД-1 (послуга безпеки "довірча конфіденційність") існує відповідна сукупність слотів (вимог до послуги безпеки), які можуть мати певне значення "так/ні" (falsh/true) або певний тип даних (текст, числа, графіка і т. д.). В свою чергу, слот також може бути певним фреймом і т. д. Таким чином, утворюється певне дерево подій складної ієрархічної структури. При рішенні прямих задач воно працює однозначно, але при зворотних задачах однозначність результатів експертної оцінки гарантується не завжди.

В базовій моделі експертної системи як розумний компроміс використовується **процедурно-фреймова** форма подання знань і правил з використанням програмного інструментарію кейс-технологій Delphi та, при необхідності, інші форми.

Розробка методологічних основ експертної оцінки безпеки інформації в КС здійснюється у такій послідовності.

Спочатку розроблюється **комплексна модель** експертної оцінки безпеки інформації в КС. Визначаються системно-концептуальні основи стратегії експертної оцінки безпеки КС, класи та підкласи КС як об'єктів експертної оцінки, види оцінюваної безпеки та базові критеріальні підходи щодо експертної оцінки послуг безпеки певних КС від загроз НСД, регламентованих згідно з вимогами чинних НД ТЗІ Департаменту СТСЗІ СБ України [2, 3, 4].

Далі здійснюється розробка базової моделі експертної системи оцінки безпеки інформації в КС, а саме:

* визначення і формалізація правил експертної оцінки стандартних функціональних послуг безпеки інформації в КС (визначення і формалізація множини СФПБ-правил);
* визначення і формалізація правил експертної оцінки комплексу стандартних послуг гарантії безпеки інформації в КС (визначення і формалізація множини СПГБ-правил);
* визначення і формалізація правил експертної оцінки стандартних профілів захищеності інформації в КС (визначення і формалізація множини СПЗІ-правил);
* визначення і формалізація правил експертної оцінки нормативно-правових засад захисту інформації в КС (визначення і формалізація множини НПЗІ-правил);
* визначення і формалізація правил прийняття рішень за багатьма критеріями щодо поточного або належного стану безпеки оцінюваної КС (визначення і формалізація множини ПРБК-правил).

Далі на базі CASE-технологій Delphi розроблюється прикладне програмне забезпечення для поданих вище правил щодо функціонування бази знань, механізму логічного висновку та інтерактивного дружнього інтерфейсу користувача для розроблюваної базової моделі експертної системи (БМЕС).

Множина СФПБ-правил використовується для алгоритмізації експертної оцінки функціональних послуг безпеки, які надаються в певній захищеній КС (рис. 1, ієрархічні послуги конфіденційності, цілісності, доступності, спостереженості інформації і ресурсів КС).

Множина КПГБ-правил використовується в базовій моделі експертної системи для експертної оцінки послуг гарантії безпеки, що надаються в певній КС з використанням рівнів безпеки Г-1...Г-7 згідно з вимогами НД ТЗІ 2.5-004-99 (рис. 1, ієрархічні послуги гарантії безпеки КС на всіх етапах її життєвого циклу від архітектури до випробувань).

Множина СПЗІ-правил використовується в базовій моделі експертної системи для експертної оцінки послуг безпеки, що надаються в певній КС з використанням стандартних функціональних профілів захищеності інформації від потенційних загроз НСД (рис. 1, класи 1, 2, 3 КС).

Множина НПЗІ-правил використовується в базовій моделі експертної системи для оцінки послуг безпеки, що надаються в певній КС щодо використання регулятивних, захисних та установчих функцій чинних нормативно-правових засад України з питань захисту інформації.

Множина ПРБК-правил використовується в базовій моделі експертної системи для прийняття рішення за багатьма критеріями (згідно з НД ТЗІ 2.5-004-99 їх понад 110) щодо поточного чи належного стану безпеки інформації в оцінюваній КС.

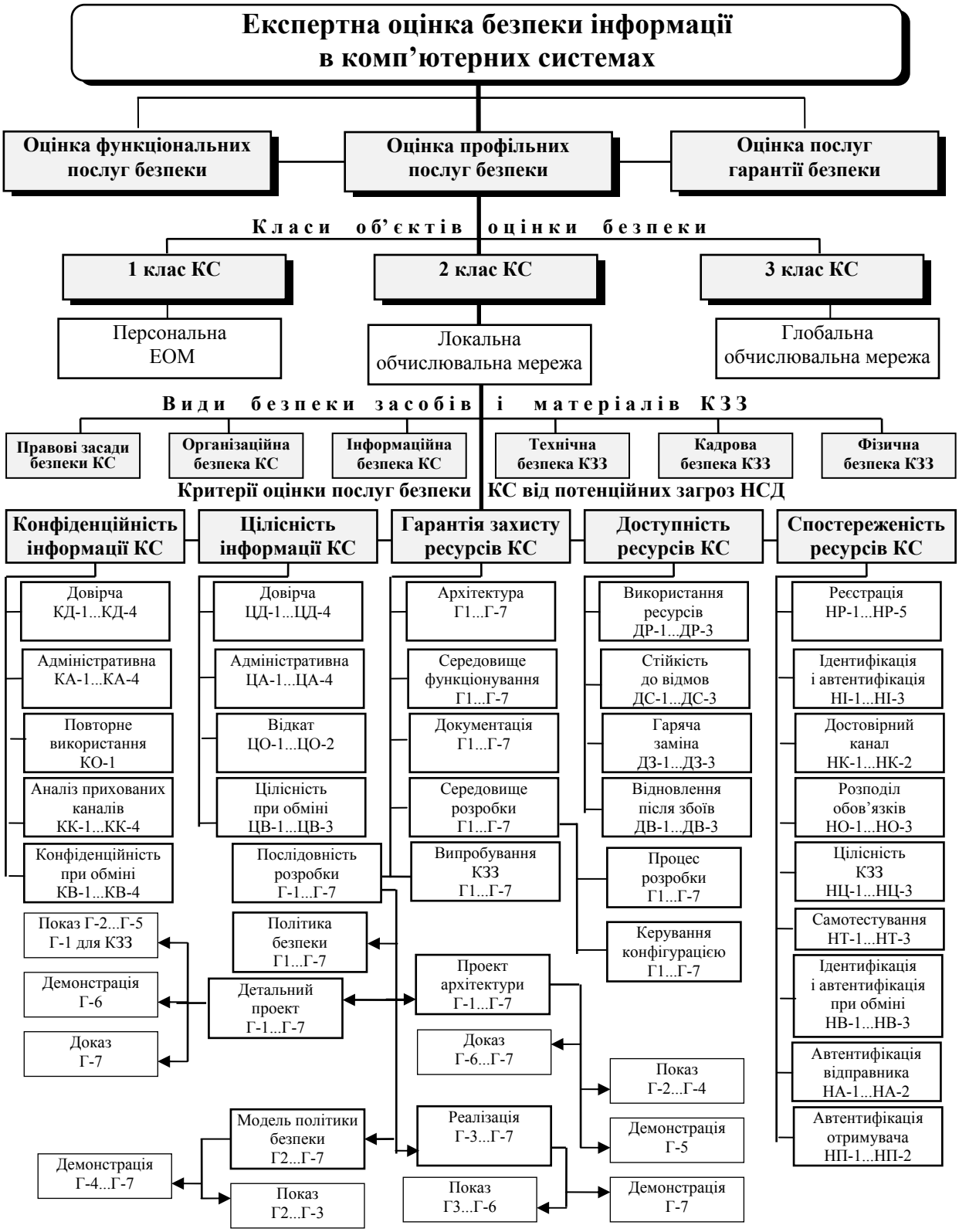
II Комплексна модель та методологічні основи експертної оцінки безпеки інформації в комп'ютерних системах

Розробку базової моделі експертної системи найбільш доцільно почати з розробки її комплексної (базової) моделі як варіанту реалізації таксономічних підходів до систематизації та класифікації суттєвих ознак проблеми. Модель, як абстрактний формалізований або неформалізований опис, передбачає, насамперед, найбільш доцільну форму представлення знань щодо реалізації мети та задач, які вирішуються експертною системою.

Ознака **"базової"** моделі понятійно регламентує, що в ній визначаються та декомпозуються тільки найбільш суттєві і мінімально необхідні принципи класифікації та найбільш суттєві ознаки досліджуваної системи.

Ознака **"комплексної"** моделі понятійно регламентує, що в ній визначаються та декомпозуються, передусім, її системно-концептуальні засади як сукупність вимог до всіх видів безпеки КС та на всіх етапах її життєвого циклу. Це досягається використанням певного комплексу послуг безпеки, а саме:

- стандартних **функціональних** послуг щодо захисту інформації і ресурсів КС шляхом визначення та дотримання регламентованих вимог ієрархічної множини часткових критеріїв конфіденційності, цілісності, доступності та спостереженості інформації і ресурсів КС;
- стандартних послуг **гарантії** безпеки КС на всіх етапах її життєвого циклу шляхом визначення та дотримання регламентованих вимог із їх ієрархічної множини щодо часткових критеріїв експертної оцінки відповідності стосовно архітектури, середовища розробки, послідовності розробки, середовища функціонування, документації і випробувань комплексу засобів захисту (КЗЗ) КС;
- **елементарних** послуг безпеки, в яких регламентуються первинні функціональні вимоги і вимоги гарантії безпеки згідно з [2];



Примітка: Часткові критерії послуг безпеки КД-1...КД-4 і т. д. вказані в скороченнях згідно з НД ТЗІ 2.5-004-99

Рисунок 1 – Комплексна базова модель системно-концептуальних основ експертної оцінки безпеки КС (правило СкоЕоБкс-1)

- **профільних** послуг захищеності інформації шляхом визначення та дотримання регламентованих вимог із їх ієрархічної множини (рис. 1, послуги КД-1…КД-4, КА-1….КА-4, ЦД-1…ЦД-4, ДР-1…ДР-3, ДС-1…ДС-3, НР-1…НР-5 тощо). Профільні послуги безпеки є структурною основою експертної оцінки відповідності обраних стандартних профілів захищеності, **по-перше**, для певного класу, **по-друге**, для певного підкласу КС, **по-третє**, проти певних потенційних загроз, а саме: "К" (конфіденційності), "Ц" (цілісності), "Д" (доступності), "С" (спостереженості), "КЦ" (конфіденційності і цілісності), "КД" (конфіденційності і доступності), "ЦД" (цілісності і доступності), "КЦД" (конфіденційності, цілісності і доступності);

- **необхідних** послуг безпеки, до яких належать певні профільні послуги, а також повний комплекс послуг гарантії безпеки рівня Г-3 тощо. Наприклад, послуги безпеки НІ-1, НЦ-1, КО-1, НО-1, НВ-1, ДС-1, НК-1, НР-1 тощо. Надання необхідних послуг безпеки є обов'язковою умовою для надання певної профільної послуги;

- послуг **нормативно-правових** засад щодо захисту інформації КС, передусім, обмеженого доступу, стосовно регулятивних та захисних функцій щодо злочинів з використанням електронно-обчислювальних машин, систем та комп'ютерних мереж згідно з вимогами розділу XVI, ст. 361, 362, 363 Кримінального кодексу України та інших засад.

Цілком зрозуміло, що при цьому передбачається, насамперед, визначення таких системно-концептуальних основ ієрархії послуг безпеки КС, які в подальшому забезпечують формулювання і алгоритмізацію "правил" бази знань, механізму логічного висновку та інтерактивного інтерфейсу користувача базової моделі експертної системи, тобто інструментальне забезпечення розробки "ядра" БМЕС на базі новітніх CASE-технологій, наприклад, Delphi 3-5 (до 80–85 % автоматизація розробки програмного забезпечення і тільки до 15–20 % – ручні технології програмування). Ядром безпеки КС визначається її КЗЗ.

Експертна оцінка безпеки розроблюваної КС певного класу є початковою та обов'язковою операцією і для розробки базової моделі експертної системи. В подальших дослідженнях передбачається, що окрім експертної оцінки доцільно в подальшому планувати надання експертній системі адаптивних функцій автоматизованого моніторингу та автоматизованого регулювання "належного" стану безпеки КС.

На основі аналізу комплексної моделі рис. 1 можна зробити наступні висновки та рекомендації щодо подальшої розробки відповідної структури і програмного забезпечення базової моделі експертної системи.

Подібні задачі вже вирішуються мережевими аналізаторами (екранами), серверами безпеки, проксі-серверами та іншими системами щодо захисту корпоративних мереж Intranet, Extranet від загроз НСД (на цей час вже здійснюється моніторинг понад 290 протоколів обміну). Але проблему безпеки вони вирішують тільки частково і саме тому, що це, насамперед, так звані "універсальні" програмно-апаратні або програмні пакети, коли для успішної реалізації їхніх послуг безпеки ще необхідно врахування не тільки "універсальних" (стандартних), а й "специфічних" для кожної КС певної множини послуг безпеки. Це велика проблема забезпечення безпеки не тільки для окремих КС, а й для КС інших класів і призначення, і не тільки в теоретичному, а й в практичному значенні.

На рис. 1 така системно-концептуальна ієрархія (основи таксономії) експертної оцінки безпеки певної КС визначається у вигляді комплексної моделі експертної оцінки безпеки захищеної КС.

1. **Експертна оцінка** безпеки КС повинна починатись і здійснюватись в об'ємах та в послідовності згідно з правилом СкоЕоБкс-1.
2. **Початковою** вирішальною та таксономічною ознакою є вибір користувачем експертної системи класу оцінюваної КС (класи 1, 2, 3 – кожний окремо, чи у визначеній сукупності).
3. **Другою** за важливістю таксономічною ознакою є визначення певних потенційних загроз, від впливу чи атак яких оцінюватиметься безпека КС (визначається через визначення підкласу КС).
4. **Третьою** за важливістю таксономічною ознакою є визначення пріоритетності стандартних функціональних послуг безпеки та правил їх експертної оцінки і реалізації в базовій моделі експертної системи.
5. Здійснюється визначення виду оцінюваної безпеки КС (кожної окремо чи у певній сукупності).
6. **Визначається** належний рівень гарантії безпеки КС та розроблюються правила експертної оцінки і реалізації цих послуг безпеки.
7. Розроблюється комплексна базова **модель політики безпеки.**
8. Розроблюються **правила** прийняття експертного рішення щодо забезпечення безпеки в певній КС, яка підлягає експертній оцінці.
9. Визначається **відповідність** оцінюваних в КС стандартних функціональних профілів захищеності (послуг СФПЗ) і рівнів (послуг) гарантії безпеки вимогам національних стандартів та, для порівняння, вимогам кращого із зарубіжних стандартів комп'ютерної безпеки, правил їх оцінки та прийняття експертного рішення.

10. **Надійність** роботи базової моделі експертної системи та вірогідність одержуваних результатів експертного рішення щодо безпеки оцінюваної КС повинна забезпечуватись використанням наступних форм випробувань (тестів): “показ”, “демонстрація”, “доказ”.

Основною **метою** випробувань (тестів) у вигляді “показ”, “демонстрація”, “доказ” має бути гарантоване забезпечення відповідності оцінюваних послуг безпеки певній політиці безпеки згідно з задокументованою певною моделлю політики безпеки. При цьому критерії гарантій включають вимоги до відповідності специфікацій певного рівня деталізації (декомпозиції). Рівень зусиль, необхідних для досягнення такої відповідності, зростає разом з рівнем гарантій. Для його характеристики використовують терміни *"показати", “продемонструвати" або "довести"*, а саме:

- якщо від Розробника вимагається **показати** повну відповідність між представленнями КС, то це означає, що є необхідністю наявність відповідності тільки між основними елементами кожної специфікації; прикладом може бути використання таблиці, елементи якої відображають відповідність, або використання належного представлення діаграми проекту;

- якщо від Розробника вимагається **продемонструвати** повну відповідність між представленнями КС, то це означає, що необхідним є наявність відповідності між більш дрібними елементами кожної специфікації; демонстрація відповідності виконується на основі аналізу з використанням структурованого наукового підходу, що дає переконливі аргументи на користь того, що існує повна відповідність між елементами двох специфікацій;

- якщо від Розробника вимагається **довести** повну відповідність між представленнями КС, то необхідним є наявність відповідності між ще більш дрібними елементами кожної специфікації; відповідність між елементами має бути виражена формально.

11. **Ядром** безпеки захищеної КС визначається її комплексна система захисту інформації **(КСЗІ)**, **ядром** безпеки обчислювальної системи (ОС), тобто програмно-апаратного забезпечення КС, визначається її комплекс засобів захисту**.**

КСЗІ КС реалізується наданням послуг безпеки певною сукупністю апаратно-програмних, телекомунікаційних, інженерно-технічних, організаційних та нормативно-правових рішень, заходів і засобів.

КЗЗ КС реалізується наданням апаратно-програмним забезпеченням певної сукупності стандартних функціональних послуг безпеки, стандартних послуг гарантії безпеки та стандартних функціональних профілів захищеності оброблюваної інформації в КС. В розроблюваній базовій моделі експертної системи ці послуги безпеки визначаються та формалізуються відповідною множиною СФПБ-, СПГБ- і СФПЗ-правил.

Найбільш пріоритетними визначаються стандартні функціональні профілі захищеності. Головною вимогою до них є надання послуг “К”, “Ц”, “Д”, “КЦ” (конфіденційності, цілісності, доступності, конфіденційності і цілісності), аналогічно “КД”, “ЦД”, “КЦД”. Послуги спостереженості “Н” (в залежності від класу КС надаються від 6 до 9 послуг із їх повної низки), послуги “ЦО-1” (цілісність КЗЗ) і послуги гарантії рівня безпеки “Г-3” – завжди є **необхідними** для надання послуг “К”, “Ц”, “Д” і їх сполучень (“КЦ”, “КД”, “ЦД”, “КЦД”).

12. Для більш чіткої формалізації і полегшення експертної оцінки (експертизи) поточного або належного стану безпеки певної КС у розроблювальній БМЕС визначаються **класи і підкласи** КС, які суттєво пов’язані з характеристиками стандартних функціональних профілів захищеності. Основною метою визначення при експертній оцінці класів і підкласів має бути полегшення співставлення вимог до КЗЗ КС з характеристиками самої КС.

13. Вимоги до **функціонального складу** КЗЗ при його експертній оцінці залежать від **характеристик** оброблювальної інформації, самої обчислювальної системи (ОС) як певного **апаратно-програмного** забезпечення КС, **фізичного** середовища, **персоналу** і **організаційної** підсистеми (як сукупності певних заходів забезпечення безпеки).

14. Вимоги до **гарантії безпеки** при оцінці КЗЗ залежать від ступеню дотримання розробником КС виконання регламентованих вимог до її **архітектури, середовища і послідовності розробки, середовища функціонування, документації, випробувань КЗЗ,** а також від дій Розробника, Власника і Експерта під час оцінки належного або поточного стану безпеки КС. Необхідною вимогою до середовища розробки є документування використовуваних методик забезпечення **фізичної, технічної, організаційної і кадрової безпеки** КС (НД ТЗІ 2.5-004-99, п. Б2).

15. За сукупністю характеристик КС (конфігурація апаратних засобів ОС і їх фізичне розміщення, кількість різноманітних категорій оброблюваної інформації, кількість користувачів і категорій користувачів) у СФПЗ-правилах визначаються **три ієрархічні класи** КС, вимоги до функціонального складу КЗЗ яких істотно відрізняються. Саме тому за цією ознакою реалізації КЗЗ (щодо надання певних базових послуг безпеки) в межах кожного класу при експертній оцінці здійснюється класифікація КС на підставі вимог до забезпечення певних властивостей інформації, яка підлягає захисту в КС.

16. З точки зору безпеки інформація в СФПЗ-правилах характеризується трьома базовими і функціонально-самостійними властивостями: **конфіденційністю, цілісністю і доступністю.** В зв'язку з цим в кожному класі КС в СФПЗ-правилах визначаються також певні **підкласи**. Для кожного з підкласів кожного класу в СФПЗ-правилах вводиться певна множина ієрархічних функціональних профілів, яка може бути різною для кожного класу і підкласу КС. Наприклад, семантика підкласу "х.КЦ" означає, що в оцінюваній КС головною метою захисту є забезпечення конфіденційності і цілісності оброблюваної інформації, тобто надання **базових** послуг "К" і "Ц". Таким чином, **базові послуги** "К", "Ц", "Д", "КЦ", "КД", "ЦД", "КЦД" і відповідні підкласи "х.К", "х.К", "х.Ц", "х.Д", "х.КЦ", "х.КД", "х.ЦД", "х.КЦД" в СФПЗ-правилах визначаються як аналогічні формалізовані компоненти безпеки КС.

17. Використання в СФПЗ-правилах стандартних функціональних **профілів** захищеності обумовлюються наступними перевагами їх використання при розробці БМЕС.

17.1. **Стандартний функціональний профіль** захищеності є переліком мінімально необхідних рівнів послуг, які має реалізувати КЗЗ ОС КС, щоб задовольнити вимоги щодо захищеності інформації, що обробляється у даній КС.

17.2. Стандартні функціональні профілі будуються на **підставі** існуючих **вимог** щодо **захисту** певної інформації від певних **загроз і відомих** на сьогодні **функціональних послуг,** що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які пред'являються користувачем КС.

17.3. Для стандартних функціональних профілів захищеності не вимагається ні зв'язаної з ними **політики безпеки**, ні **рівня гарантій**, хоч їх наявність і допускається при необхідності. Політика безпеки КС, що реалізує певний стандартний профіль, має бути "успадкована" з відповідних документів, що встановлюють вимоги до порядку обробки певної інформації в КС. Так, один і той же профіль захищеності може використовуватися для опису функціональних вимог з захисту оброблюваної інформації і для обчислювальних систем, і для СУБД, в той час як їх політика безпеки, зокрема визначення об'єктів захисту, може бути різною.

17.4. Стандартні функціональні **профілі** захищеності визначаються в СФПЗ-правилах системно **ієрархічними** в тому розумінні, що їх реалізація забезпечує наростаючу захищеність від загроз відповідного типу (конфіденційність, цілісність, достатність). При цьому **наростання** ступеня захищеності може досягатися як **підсиленням** певних послуг, так і включенням до профілю **нових** певних послуг, але на умовах їх обов'язкової кількісної оцінки щодо впливу на ступінь наростання.

17.5. Основними вимогами в СФПЗ-правилах до критеріїв кількісної оцінки наростання ступеня захищеності визначаються: **з** одного боку, **максимальна чутливість** до надання (ненадання) кожної **елементарної** (первинної) послуги безпеки, регламентованої в СФПБ-правилах; з другого боку, **мінімальна кількість рівнів** профільних послуг безпеки (наприклад, КД-1 ... КД-4, НР-1 ... НР-5 тощо) і базових послуг безпеки (наприклад, оптимальна кількість рівнів безпеки Г1 ... Г7).

17.6. Визначення в СФПЗ-правилах **класів і підкласів** КС корисне для полегшення вибору при експертній оцінці переліку функцій, які повинен реалізувати КЗЗ КС для забезпечення належного стану безпеки КС. Цей підхід дозволяє також мінімізувати витрати Розробника, Власника на початкових етапах створення КСЗІ КС. Проте слід визнати, що для створення КЗЗ, яка найповніше відповідає характеристикам і вимогам до конкретної КС, необхідне проведення в повному обсязі аналізу потенційних загроз і оцінки ризиків.

17.7. Єдина вимога, якої слід дотримуватися при **утворенні нових профілів** – це додержання описаних в НД ТЗІ 2.5-004-99 **необхідних** послуг безпеки для кожної із **профільних** послуг, що включаються до профілю.

17.8. Стандартні функціональні профілі захищеності можуть також використовуватися для порівняння оцінки функціональності КС за **критеріями інших держав** з оцінкою за національними критеріями (наприклад, з оцінками по критеріям CTCPEC, ITSEC, TCSEC, CCITSE тощо).

III Висновки

Визначені вище основні системно-концептуальні та методологічні підходи свідчать про те, що при розробці базової моделі експертної системи оцінки безпеки інформації в комп'ютерних системах можна зробити наступні висновки та рекомендації.

1. Актуальною задачею сьогодення слід вважати впровадження нових НД ТЗІ Департаменту СТСЗІ щодо захисту інформації і ресурсів комп'ютерних систем від загроз НСД на рівні кращих міжнародних стандартів комп'ютерної безпеки.

2. Крім наявності національних стандартів захисту комп'ютерних систем від загроз НСД необхідна також певна методика оцінки безпеки інформації і ресурсів комп'ютерних систем від загроз НСД. Слід додати, що це проблема не тільки практичного, а і теоретичного значення. Після публікації Єдиних

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