Аналогичные результаты могут быть получены и для ЗСПИ без резервирования.

Выводы

Основное назначение изложенного материала по подходу к получению поверхности оптимальных по качеству ЗСПИ и самих УОП – оптимизация ЗСПИ на разных этапах проектирования по совокупности технико-экономических показателей с учетом их взаимности. Если ЗСПИ является частью системы более высокого уровня, то УОП могут быть использованы как составляющие технико-экономической модели оптимизации такой системы. При этом оптимизация существенно облегчается за счет сокращения числа независимых переменных (в модуле могут выражаться показатели качества K_i вместо вариации технических параметров ЗСПИ x_i).

Следует также иметь в виду, что полученные в настоящей работе УОП носят универсальный характер в том смысле, что зависит лишь от принятых допущений в виде технико-экономических зависимостей подсистем ЗСПИ и справедливы для произвольных значений параметров этих зависимостей (т.е. $\beta_i, \gamma, \gamma_j \left| i = \overline{1,6}; j = \overline{7,10} \right.$) и показателей качества. Это позволяет использовать УОП для сравнения по совокупности показателей качества не только отдельные системы, но и классы систем, различающиеся своими технико-экономическими параметрами.

Список литературы

1. Сервинский Е.Г.–Оптимизация систем передачи дискретной информации / Сервинский Е.Г. – М. : Связь, 1974.–324 с.

2. Гуткин Л.С. – Оптимизация радиоэлектронных устройств по совокупности показателей качества / Гуткин Л.С. – М. : Сов. Радио, 1975.–366с.

3. Тискина Е.О.–Критерии оптимизации и синтез модели самообучающихся систем защиты информации/Тискина Е.О., Хорошко В.А. // Радиотехника, Вып.155, 2008.–с 116-122.

4. Орленбко В.С.–Методика оцінювання ефективності обміну інформацією в захищених телекомунікаційних системах / Орленко В.С., Хорошко В.А. // Зв'язок, №2, 2008.–с.33-36.

5. Диффин Р. – Геометрическое программирование / Диффин Р., Питерсон Э., Зенер К. – М. : Мир, 1992.–412с.

Рецензент: Петров А.С.
Надійшла 24.02.2011

УДК 004.056

Дудикевич В.Б., Микитин Г.В., Гарасим Ю.Р.
(НУ «Львівська політехніка»)

ІНТЕГРАЛЬНА БЕЗПЕКА ІНФОРМАЦІЇ: КОНЦЕПТУАЛЬНА МОДЕЛЬ, АВТОМАТИЗОВАНА СИСТЕМА ОБРОБЛЕННЯ ДАНИХ З ОБМЕЖЕНИМ ДОСТУПОМ

1. Актуальність застосування систем інтегральної безпеки інформації

У сфері технічного захисту інформації, інформаційної безпеки об'єктів сьогодні запитувані: нові підходи і методологічні засади; системи, засоби і методи захисту; інформаційні, інформаційно-комунікаційні технології та алгоритми захисту. Суттєве підвищення ефективності систем захисту об'єктів уможливлюється з використанням підходів інтегральної безпеки інформації [1-3]. Методологія інтегральної безпеки полягає у створенні умов функціонування суб'єктів, об'єктів, інформації, за яких вони будуть надійно захищені від усіх реальних видів загроз, при яких стає неможливим перехоплення,

видозмінення і знищення інформації за рахунок виявлення, блокування та нейтралізації моделей поведінки порушника.

Класифікація засобів інтегральної безпеки інформації (ІБІ) в рамках організаційного, технічного, програмного, криптографічного рівнів та функціональних принципів захисту показана на рис. 1. Виділимо п'ять груп технічних засобів ІБІ, причому. Перші чотири групи (основні) – засоби контролю і управління доступом до інформації, засоби закритого зв'язку, засоби виявлення загроз, засоби блокування загроз є основними групами, а п'ята (допоміжна) – засоби захисту інформації.

До групи засобів контролю і управління доступом до інформації відносяться засоби розмежування доступу до інформації в автоматизованій системі (АС) і у приміщеннях, де знаходиться інформація з обмеженим доступом. При цьому використовуються засоби ідентифікації (паролі, біометричні засоби) та інженерно-технічні засоби, які допомагають забезпечити режим перепусток (замки, пломби т. і.). За допомогою засобів контролю дій користувача здійснюється спостереження за відвідуванням охоронних об'єктів та використанням інформації користувачів. Це дає можливість відслідковувати неправомірні спроби доступу до інформації. До цієї групи відносяться засоби ідентифікації цінних паперів і документів, використання яких уможливлює виявлення шахрайських підробок.

До засобів закритого зв'язку відносяться: засоби криптозахисту (шифратори), скремблери, маскувальники, засоби стенографії, засоби захисту мереж і систем зв'язку та спецзасоби захисту перемовин. Всі вони призначені для захисту телефонних перемовин та даних, які передаються у комп'ютерних мережах. Захист даних здійснюється на рівні: шифрування інформації (шифратори), зашумлення сигналу (маскувальники, скремблери), приховування інформації у зображеннях, відеопотоці (стеганографічні програми), виявлення сигналів, які випромінюються нелегальними радіоприймачами т. і.

Третьою групою засобів ІБІ є засоби виявлення загроз. Засоби даної групи: виявляють можливі канали витоку інформації і закладні пристрої; здійснюють контроль приміщення на предмет дії пристрою зняття інформації. Дія засобів блокування загроз спрямована на блокування загроз витоку інформації, тобто закриття каналів витоку інформації та блокування закладних пристроїв. До допоміжних засобів захисту інформації відносяться засоби: відео-, аудіонагляду, тривожного оповіщення, антивірусного захисту. Важливими у цій групі є засоби, які дозволяють відновити втрачену інформацію.

З метою оптимального вибору, за відповідними критеріями захисту інформації, систем інтегральної безпеки необхідно: створити концептуальну модель предметної сфери «Системи інтегральної безпеки»; розробити автоматизовану систему оброблення даних з обмеженим доступом на основі інформаційної моделі бази даних.

2. Створення концептуальної моделі предметної сфери «Системи інтегральної безпеки»

Інформація, отримана в результаті спостереження, реєстрації, вимірювання, контролю, діагностування, розпізнавання даних (сигналів) повинна відображати адекватну модель об'єкта дослідження відповідної предметної сфери. З метою ефективного застосування систем інтегральної безпеки інформації відповідно до поставлених задач захисту об'єктів запропонована концептуальна модель предметної сфери на основні принципів системного аналізу: цілісності, ієрархічності, багатоаспектності [4,5].

Цілісність передбачає інтеграцію (об'єднання) частин цілого і проявляється в появі нових властивостей (ознак, параметрів, характеристик, фізичних величин) цілого, які відсутні у його частинах. Ієрархічність дає можливість точно виділити істотні властивості та взаємозв'язки складного об'єкта, що забезпечує докладний опис його властивостей за рахунок використання апріорних знань про внутрішню будову об'єкта (рис. 2.)

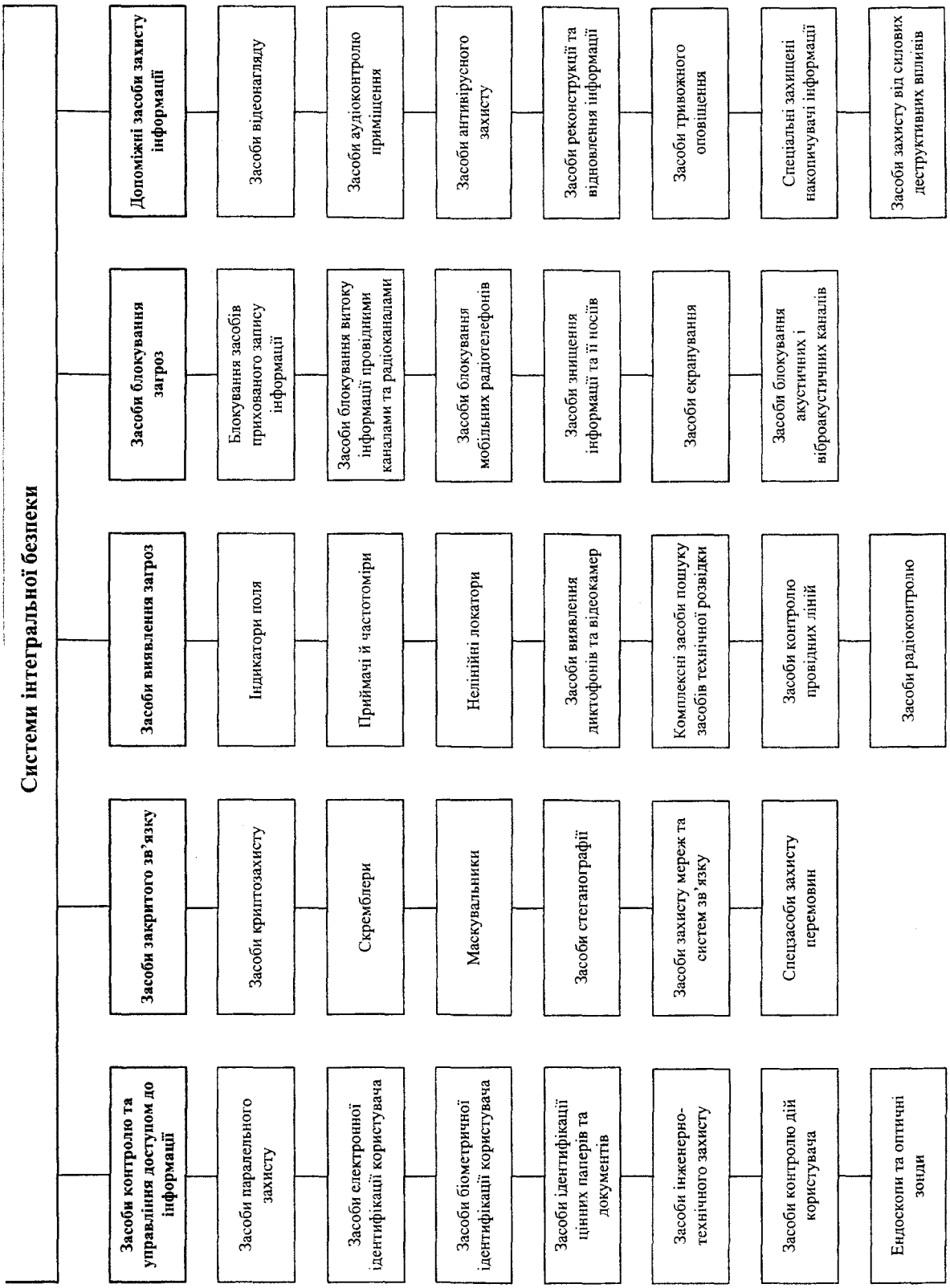

Рис. 1. Класифікація систем інтегральної безпеки

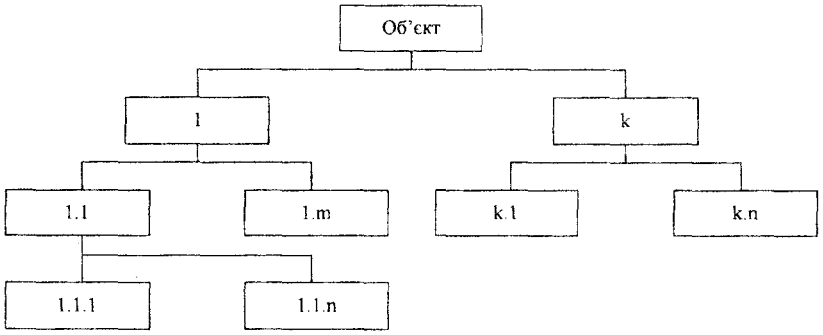

Рис. 2. Ієрархічність природної декомпозиції об'єкта дослідження

Багатоаспектність дозволяє розглядати об'єкт з різних точок зору з урахуванням взаємозв'язків виявлених елементів, зокрема при розділенні об'єкта на підсистеми, які дозволяють застосувати підхід до спрощеного опису об'єкта, з точністю припустимою для побудови концептуальної моделі (рис. 3).

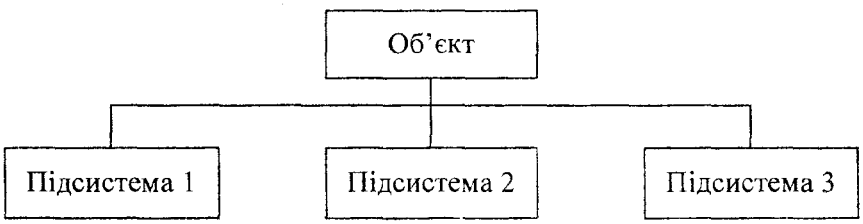

Рис. 3. Багатоаспектність об'єкта

На основі застосування принципів ієрархічності та багатоаспектності пропонується концептуальна модель, яка відображає принцип цілісності предметної сфери (рис.4). В моделі виділені аспекти взаємозв'язку частин складного об'єкта.

Для створення концептуальної моделі доцільно розглянути системи ІБІ на: апаратному, програмному, апаратно-програмному рівнях з відповідними функціональні засобами – апаратними пристроями, програмними продуктами, апаратно-програмним забезпеченням адекватно до класів систем (рис.1).

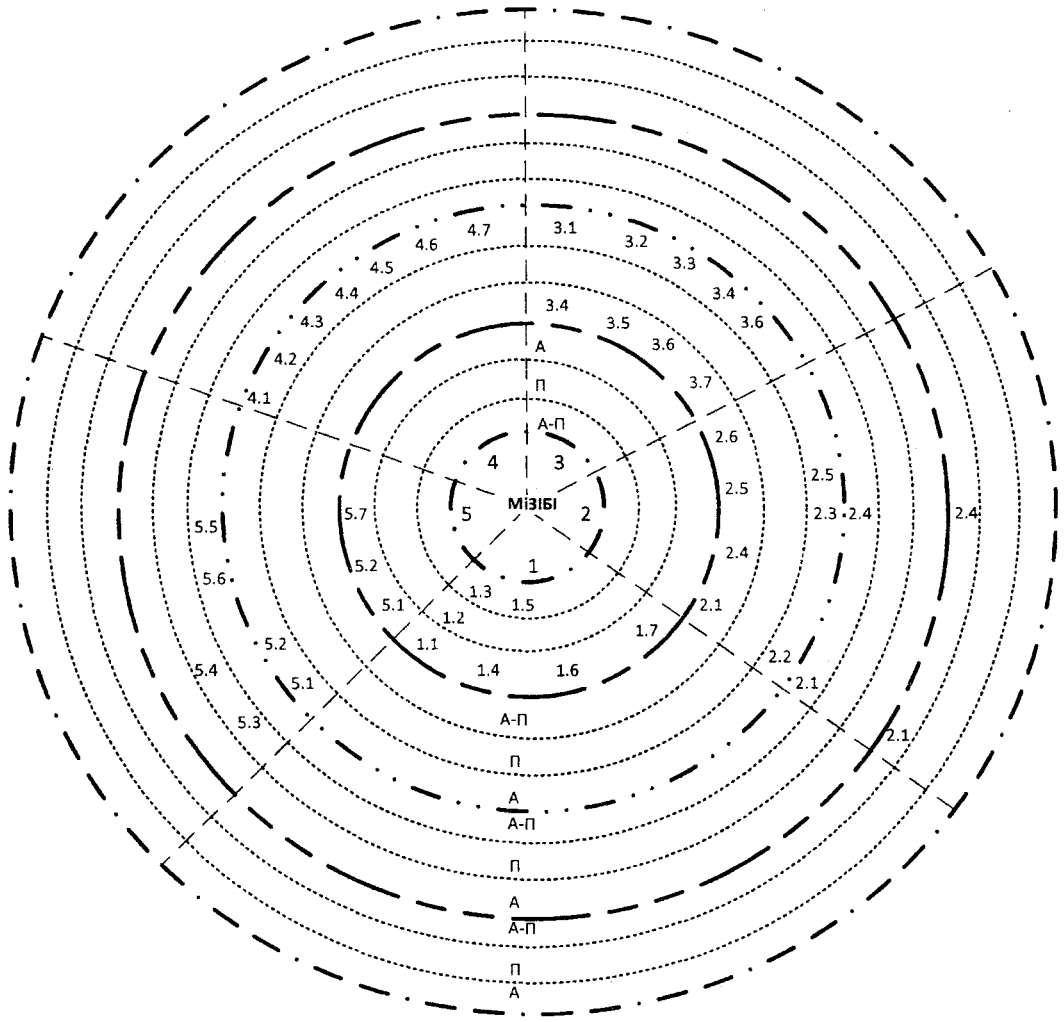

Рис. 4. Концептуальна модель «Системи інтегральної безпеки»

Пояснення ліній та скорочень до рис. 4:
1) класи систем інтегральної безпеки (— · — · — · —);
2) організаційний (——— — ———);
3) технічний (— · · — · · — · ·);
4) програмний (——— — — ———);
5) криптографічний (— — · — — · —) (методи захисту);
А – апаратні засоби, **П** – програмні засоби, **А-П** – апаратно-програмні засоби.

1 – Засоби контролю і управління доступом до інформації:
1.1 засоби паралельного захисту;
1.2 засоби електронної ідентифікації користувача;
1.3 засоби біометричної ідентифікації користувача;
1.4 засоби ідентифікації цінних паперів і документів;
1.5 засоби інженерно-технічного захисту;
1.6 засоби контролю дій користувача;
1.7 ендоскопи і оптичні зонди.
2 – Засоби закритого зв'язку:
2.1 засоби криптозахисту;
2.2 скремблери;

2.3 маскувальники;
2.4 засоби стенографії;
2.5 засоби захисту мереж і систем зв'язку;
2.6 спецзасоби захисту перемовин.

3 – Засоби виявлення загроз:

3.1 індикатори поля;
3.2 приймачі і частотоміри;
3.3 нелінійні локатори;
3.4 засоби виявлення диктофонів і відеокамер;
3.5 комплексні засоби пошуку;
3.6 засоби контролю провідних ліній;
3.7 засоби радіоконтролю.

4 – Засоби блокування загроз:

4.1 блокування засобів прихованого запису інформації;
4.2 засоби блокування витоку інформації провідними каналами і радіоканалами;
4.3 засоби блокування мобільних радіотелефонів;
4.5 засоби знищення інформації та її носіїв;
4.6 засоби екранування;
4.7 засоби блокування акустичних і віброакустичних каналів.

5 – Допоміжні засоби захисту інформації:

5.1 засоби відеонагляду (відеоконтролю);
5.2 засоби аудіоконтролю приміщення;
5.3 засоби антивірусного захисту;
5.4 засоби реконструкції і відновлення інформації;
5.5 засоби тривожного оповіщення;
5.6 спеціальні захищені накопичувачі інформації;
5.7 засоби захисту від силових деструктивних впливів.

3. Аспекти розроблення автоматизованої системи оброблення даних з обмеженим доступом

Характеристика підсистеми «Засоби виявлення загроз». Технічні засоби, які здійснюють виявлення загроз поділяються на [6-8]: індикатори поля; приймачі і частотоміри; нелінійні локатори; засоби виявлення диктофонів і камер; комплексні засоби пошуку; засоби контролю провідних ліній; засоби радіоконтролю.

Індикатори поля застосовуються для виявлення закладних пристроїв. Такими пристроями можуть бути радіомікрофони, телефонні радіоретранслятори, радіостетоскопи, приховані відеокамери з передаванням через радіоканал, радіомаяки систем відслідковування за переміщенням. Існує два основних методи пошуку і локалізації джерел небезпечних радіосигналів – «амплітудний метод» і метод «акустичної зав'язки». Деякі індикатори поля виконані в мініатюрному вигляді для непомітного встановлення факту наявності закладних пристроїв несанкціонованого зняття інформації в приміщенні. Індикатори поля оснащені світловою, звуковою або віброіндикацією, яка спрацьовує у випадку перевищення рівня прийнятого сигналу. Іноді індикатори поля використовують для постійного контролю приміщення. Ефективності виявлення радіозакладок сприяють частотоміри, пошукові і скануючи приймачі.

Нелінійні локатори призначені для виявлення радіоелектронних пристроїв несанкціонованого зняття інформації, незалежно від свого активного чи пасивного стану дії. Принцип дії: при опроміненні радіоелектронних пристроїв, які містять нелінійні елементи, такі як діоди, транзистори т. і., відбувається відбиття сигналу на вищих гармоніках. Більшість засобів нелінійної локації дозволяють виявляти приховані засоби зняття інформації незалежно від їх місцезнаходження – в цегляних або залізобетонних стінах, в меблях або металевих шафах, елементах інтер'єру, на тілі людини. Нелінійні

локатори функціонують в умовах впливу сильних зовнішніх радіозавад. Виявлення здійснюється шляхом опромінення контрольованої зони неперервним або модулюючим зондуючим сигналом з подальшим прийманням і аналізом сигналу відбиття одночасно на другій і третій гармоніках опромінюючого сигналу. Одночасне приймання другої і третьої гармонік дозволяє виявляти об'єкти, що містять напівпровідникові радіоелементи. У більшості пристроїв нелінійної локації інформація на предмет виявлення подається у вигляді звукового сигналу в головних телефонах, а також на пульті управління у вигляді світлового сигналу.

До засобів виявлення прихованих відеокамер та диктофонів відносяться: пристрій ТЛ-1, «Оптик»; «Айрис» т. і. Засоби радіоконтролю вирішують задачі радіомоніторингу. Вони призначені для контролю за радіовипромінюваннями у приміщеннях. Засоби контролю провідних ліній призначені для перевірки різних провідних ліній, зокрема електричної мережі 220В, телефонних ліній, т. і. Така перевірка проводиться для предмет визначення можливого витоку інформації через ці лінії та на предмет під'єднання до них з метою зняття інформації.

3.1 Критерії обґрунтування вибору структури бази даних, мови програмування і СКБД

Обґрунтування критеріїв вибору структури бази даних. Реляційна база даних (БД) – це сукупність відношень, які містять всю інформацію. Реляційна структура характеризується простотою структури даних, всі сучасні засоби системи керування базами даних (СКБД) підтримують реляційну модель даних, тому обираємо саме її. Реляційна база даних – це тіло взаємопов'язаної інформації, що зберігається в двомірних таблицях. Створивши декілька таблиць взаємопов'язаної інформації, можна виконувати більш складні операції з цими даними. Потужність бази даних залежить від зв'язку, який можна створити між фрагментами інформації. Реляційна база даних дозволяє виконати багатофункціональні задачі при отриманні інформації з таблиць згідно вказаних параметрів, особливо коли ці параметри включають в себе фрагменти інформації, пов'язані в різних таблицях один з одним.

Обґрунтування критеріїв вибору СКБД. СКБД – це програмний пакет, що забезпечує користувачу простий доступ до бази даних. Програмна частина СКБД (менеджер БД) виступає в якості інтерфейсу між користувачем і БД. Менеджер БД забезпечує програмні засоби, що необхідні для створення, загрузки, запитів і оновлення даних. Менеджер також контролює усі дії пов'язаних з управлінням вводу-виводу і пам'яттю БД. Тобто добре спроектована СКБД забезпечує програмне забезпечення, що спрощує для користувача роботу з БД. Існує велика кількість різних СКБД, наприклад, MS ACCESS, Oracle, Interbase, MySQL, mSQL, ORD, Firebird. Для побудови реляційної бази даних вибрана СКБД MySQL. MySQL – це реляційна система керування базами даних з відкритим кодом програми; надійна, стійка і проста в адмініструванні. Використовується для створення/видалення баз даних, таблиць, для доповнення таблиць даними, для здійснення вибірки даних. MYSQL має переваги: високу продуктивність, низьку вартість, просту конфігурацію і вивчення, доступність початкового коду, підтримку декількох одночасних запитів, оптимізацію зв'язків з приєднанням багатьох даних за одне звернення, запис фіксованої і змінної довжини, гнучку систему привілеїв і паролів, до 16 ключів в таблиці, зокрема кожен ключ може мати до 15 інформаційних полів. Також є: підтримка ключових полів і спеціальних полів в операторі *create,* підтримка стрічок змінної довжини і міток часу, інтерфейс з мовами C та Perl. Ґрунтується на інформаційному потоці, швидка система пам'яті, утиліта перевірки і ремонту таблиці, всі дані зберігаються в форматі стандарту ISO 8859-1. Простота в керуванні таблицями, зокрема у додаванні і видаленні ключів та полів. Крім того, MySQL працює як з *Unix,* так на платформі *Windows.*

Обґрунтування критеріїв вибору мови програмування. Щоб надати базі даних зручного для користувача інтерфейсу, подамо її у вигляді Web- сторінок, використовуючи

мову програмування PHP, яку обрали з міркувань організаційно-технічної сумісності з реляційною базою даних і СКБД. PHP – це відкритий інформаційний ресурс, що широко використовується, мова сценаріїв загального призначення, яка особливо підходить для Web і може бути упроваджений в HTML. Його синтаксис легкий для розуміння і вивчення. Головною метою створення цієї мови є: дати web-розробникам можливість швидко створювати сторінки, що динамічно генеруються. Мова PHP володіє безліччю переваг, в числі яких: висока продуктивність; наявність інтерфейсів до багатьом різним системам баз даних; вбудовані бібліотеки для виконання багатьох загальних завдань,пов'язаних з Web; низька вартість; простота вивчення і використання; перемістимість; доступність початкового коду.

3.2 Побудова реляційної бази даних

Інформаційна модель. Реляційна база даних підсистеми «Засоби виявлення загроз» представлена на рис. 5.

Структура бази даних. На основі інформаційної моделі підсистеми «Засоби виявлення загроз» визначаються атрибути відношення. Блок-схема функціональних залежностей між цими атрибутами показана на рис. 6.

Проаналізувавши функціональні залежності між атрибутами відношення, визначаємо, що пропонована база даних складається з трьох таблиць. В першій таблиці (zasoby) будуть зберігатися дані, які характеризують засоби виявлення загроз. Полями цієї таблиці є:

- Id засобу (Id) – індивідуальний номер конкретного засобу;
- Назва засобу (Nazva) – назва засобу;
- Тип (Typ) – тип , до якого належить конкретний засіб;
- Фото засобу (Foto) – шлях до файлу, де знаходиться фото даного засобу;
- Технічні характеристики (Tech) – технічні характеристики засобу;
- Функціональне забезпечення(Funk) – функціональне забезпечення засобу;
- Комплектація (Komplect) – перелік елементів, якими комплектується конкретний засіб;
- Виробник (Vyrobnyk) – дані про виробника даного засобу;
- Ліцензія (Lizensia) – ліцензія або сертифікат конкретного засобу.

В другій таблиці (Zastos) будуть зберігатися дані про можливі застосування засобів. Поля даної таблиці будуть такими:

- Назва засобу(Nazva) – назва засобу;
- Застосування засобу (Zastos) – можливе застосування конкретного засобу.

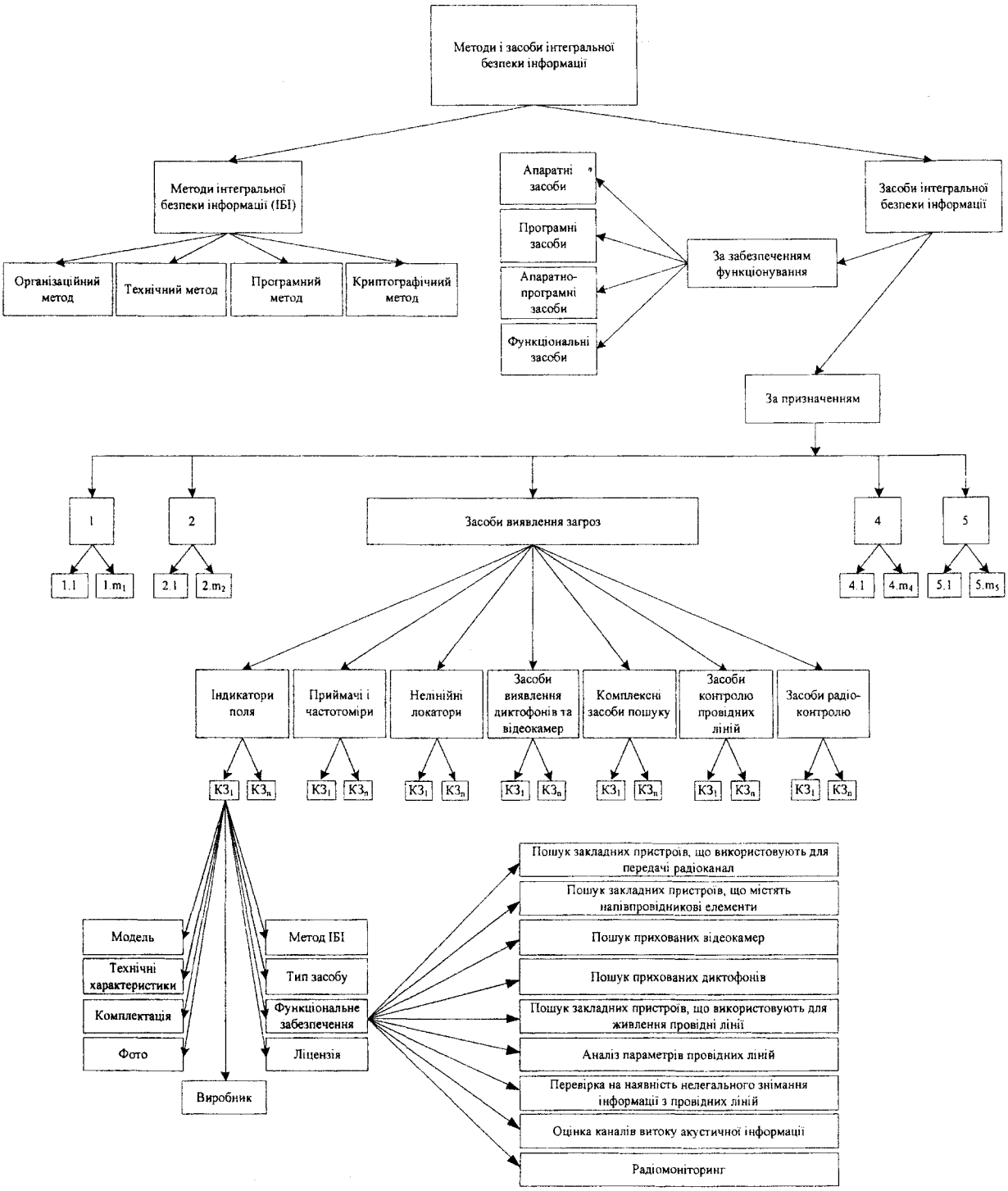

Рис. 5. Інформаційна модель бази даних підсистеми «Засоби виявлення загроз»

За допомогою третьої таблиці (Metod) можливо визначити – до якого методу інтегральної безпеки інформації відноситься певний тип засобів або конкретний засіб виявлення загроз. До цієї таблиці входять такі поля:

– Тип(Typ) – тип , до якого належить конкретний засіб;

– Метод ІБІ (MetodIBI) – метод, до якого відноситься певний тип засобів або конкретний засіб.

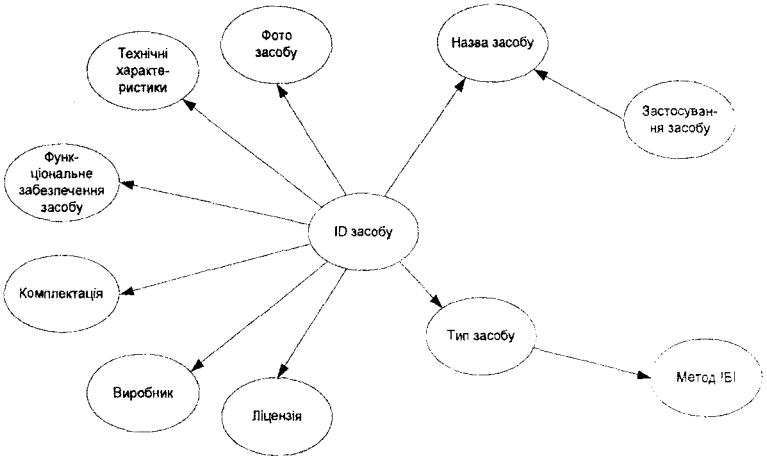

Рис. 6. Блок-схема функціональних залежностей

На рис. 7. зображена структура бази даних, де показані таблиці з яких складається БД, ваємозв'язки між ними, а також поля, що входять до складу цих таблиць.

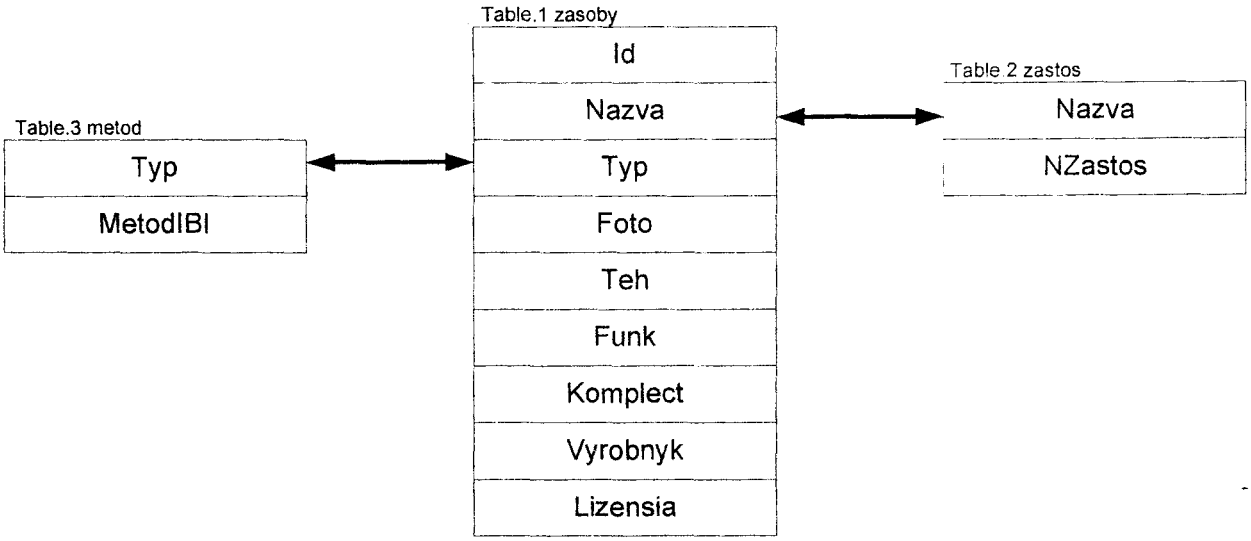

Рис. 7. Структура бази даних

3.3 Алгоритмічно-програмне забезпечення АСОД з ОД «Засоби виявлення загроз»

Алгоритм роботи автоматизованої системи показано на рис. 8. Програмне забезпечення АСОД з ОД: інтерфейс системи з обмеженим доступом реалізований на мові програмування PHP у вигляді веб-сторінки; загальне функціонування системи здійснюється на основі технології *Apache-MySQL-PHP.*

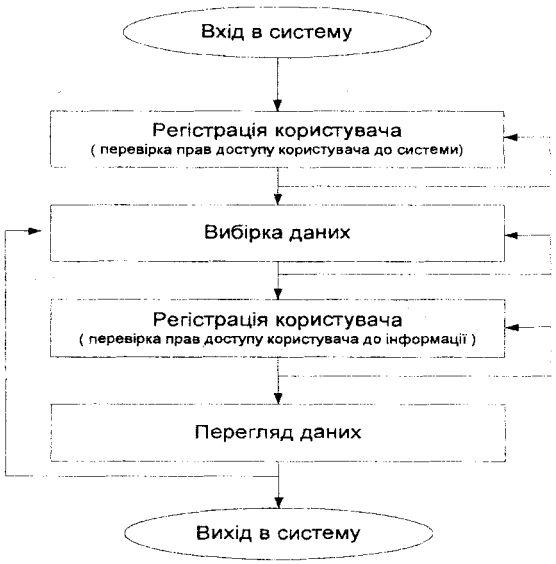

Рис.8. Алгоритм роботи АСОД з ОД

Висновки

На основі класифікації засобів інтегральної безпеки і системного підходу розроблена концептуальна модель предметної сфери «Інтегральні системи безпеки». Представлені основні аспекти розроблення АСОД з обмеженим доступом на основі інформаційної моделі підсистеми «Засоби виявлення загроз».

Список літератури

1. Ленков С. В. Методы и средства защиты информации. Том 2. Информационная безопасность / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. – Издательство Арий, 2008. – 344 с.

2. Ярочкин В. И. Информационная безопасность / В. И. Ярочкин. – М. : Академический Проект; Гаудеамус, 2-е изд. – 2004. – 544 с.

3. Norman T. Integrated security systems design: concepts, specifications and implementation / T. Norman. – Elsevier. – 2007. – 458 p.

4. Дудикевич В. Б. Концептуальні моделі захисту інформації для технологій стаціонарного, стільникового, супутникового зв'язку / В. Б. Дудикевич, Ю. Р. Гарасим, Г. В. Микитин // Вісник Національного університету «Львівська політехніка» «Автоматика, вимірювання та керування». – Львів, 2010. – № (665). – С. 18-26.

5. Дудикевич В. Б. Ієрархічна модель захисту даних в інформаційних технологіях / В. Б. Дудикевич, Г. В. Микитин, Ю. Р. Гарасим // Збірник тез доповідей II Міжнародної науково-практичної конференції «Проблеми і перспективи розвитку IT-індустрії». – Харків, 2010. – Вип. 7(88). – С. 212-213.

6. [Електронний ресурс] режим доступу: http://security.ukrnet.net.

7. [Електронний ресурс] режим доступу: http://www.bezpeka.com.

8. [Електронний ресурс] режим доступу: http://www.ccc.ru.

Рецензент: Корнійчук М.Т.
Надійшла 14.04.2011