УДК 004.43(031):681.3.01 **Луценко В.М.**

АВТОМАТИЗАЦІЯ ПРОЕКТУВАННЯ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ЗАСОБІВ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

У статті розглянутою є проблема автоматизації проектування комплексних систем захисту інформації. Наголос зроблений на питанні використання засобів підтримки прийняття рішень у вигляді моделі пам'яті з вибіркою за змістом запиту для створення проектів систем захисту. Модель пам'яті з вибіркою за змістом запиту запропоновано реалізувати на основі сітьового ансамблевого з навчанням нейроподібного моделювання.

Ключові слова: системи захисту інформації; модель складної системи; проект захисту; асоціативна пам'ять; підтримка прийняття рішень

Постановка проблеми. Методологія створення комплексних систем захисту інформації (КСЗІ) є напрямком, котрий наразі відрізняється недосконалістю методології проектування, а тому і невпорядкованістю проектів діючих об'єктів інформаційної діяльності (ОІД). Перш за все відсутньою є об'єктивна єдність підходів до створення систем захисту інформації. Структурно та інформаційно однакові об'єкти можуть бути захищеними різними системами захисту і різниця може бути принциповою. Згідно [1] захист інформації реалізується на базі фрагментарного або комплексного підходу, де фрагментарний захист забезпечує протидію певним загрозам, а комплексний – одночасну протидію безлічі загроз, причому різниця між ними є нечітко визначеною. В таких умовах створення ефективної системи автоматизованого проектування (САПР) є завданням надскладним, адже результат САПР однозначно залежить від сформованих даних суб'єктом - проектантом. Тобто скільки виконавців проекту стільки і варіантів рішень, що впливає на об'єктивність та досконалість проектів. Тому в області технічного захисту інформації (ТЗІ) при створенні моделі загроз та проектуванні систем захисту спостерігається недосконалість, а стосовно діючих САПР та систем прийняття рішень у сфері інформаційної безпеки широко відомі лише «Кондор», «Авангард» та «Гриф», котрі призначені лише для аналізу загроз та аудиту безпеки діючих проектів [2,3,4,5,6]. Причиною є об'єктивне відставання розвитку у даного напрямку, котрий залишився з попередніх часів, коли рішення з безпеки інформації приймалися переважно за рахунок організаційних методів. В таких умовах необхідним є радикально нове рішення, котре має забезпечити необхідний якісний рівень проектування незалежно від специфіки ОІД. При цьому найвищого ступеня досконалості можна досягти якщо розглядати створення системи захисту об'єктів у комплексі, тобто поєднавши в єдиний процес етапи обстеження та опису об'єкту, проектування зрілої та фінансово оптимізованої системи захисту, післяпроектний аудит безпеки об'єкту. Розглядаючи такі етапи окремо сучасні автори намагаються суттєво вдосконалювати кожний з них поодинці.

Метою статті є викладення підходу до створення методики проектування КСЗІ з застосуванням методів та засобів систем підтримки прийняття рішень (ППР). При цьому нагальною є розробка підходу до створення методології об'єктивно дієвого автоматизованого проектування. Пропонується моделювати процедуру проектування КСЗІ на окремих її етапах за рахунок використання досвіду проектування вже діючих реальних об'єктів з урахуванням статистики їх життєдіяльності. Таке моделювання використовуються виключно на таких етапах проектування, де неможливим є прийняття рішень за рахунок жорсткої алгоритмізації [7]. При цьому показники життєдіяльності розглядаються в якості параметрів якості їх проектів КСЗІ. Таким чином створення нових проектів враховує історію вже діючих.

Оскільки така робота спрямована на забезпечення інформаційної незалежності Держави в умовах колективного міждержавного інформаційного простору *актуальність* її є безумовною.

Огляд останніх досліджень і публікацій. Ключовим моментом використання технічних засобів систем підтримки прийняття рішень на базі нейросітьового моделювання є створення, або адаптація існуючої сітьової моделі. Опис та аналіз діючих систем проектування наведений в [7]. Що стосується засобів підтримки прийняття рішень з використанням сітьових нейроподібних моделей, у тому числі, з навчанням. Це і алгоритми

Кохонена, Гросберга, просторово-часове навчання Коско-Клопфа, сіті Хопфілда [8], Амосова [9,10,11,12] та ін. В [7] були проаналізовані можливості одного з видів асоціативної пам'яті (АП) та її властивості щодо використання при проектуванні КСЗІ. Було прийнято до уваги, що у даному випадку система ППР є реалізованою на АП, котра в свою чергу обслуговує виключно текстову інформацію, формуючи базу даних (БД) текстів рішень на окремих етапах проектування. Структура обміну інформацією між БД та вихідними даними від проектанта є визначеною, як зазначено в [13,14]. Але при цьому не є визначеною структура АП у складі БД.

*Виклад основного матеріалу***.** В якості можливого підходу до створення системи автоматизованого проектування КСЗІ пропонується використання моделі так званої нейроподібної ансамблевої сіті з навчанням. Завданням такої сіті є виконання функцій асоціативної пам'яті (АП) з вибіркою за змістом запиту та подальшим прийняттям квазіоптимальних рішень за методом Хопфілда. Оскільки структура сіті має повторювати структуру БД необхідно визначитися з головними властивостями структури БД.

Залежать структура БД від того, у якому вигляді інформація потрапляє до БД від проектанта. Очевидно, що список фраз бібліотеки рішень має бути жорстко визначеним. Наприклад, на етапі обслідування ОІД рішеннями є формулювання груп порушень (наприклад зі списку, наведеному в [15]). Цей список пред'являється АП, що сформована у вигляді сітьової моделі, на етапі «навчання» і надалі зберігається як БД поки не змінюється список з [15]. Вхідними даними є список дестабілізуючих факторів (ДФ), котрі виявив дослідник ОІД. Цей список формує бібліотеку вихідних даних. Завданням АП є поставити у відповідність до кожного виявленого ДФ або один, або декілька груп порушень з списку порушень. Зв'язки між ДФ та групами порушень формуються при навчанні сіті за ваговим принципом. Чим більшою є вага зв'язку, тим більшим є зв'язок між поточним ДФ та декотрим порушенням (або декількома порушеннями) з БД груп порушень. Фактично, сіть необхідна для збереження ваги кожного такого зв'язку. Результатом роботи АП є виділення одного, або декількох порушень у вигляді записаних фраз за принципом найближчого сенсового змісту (квазиоптимальний пошук за методом Хопфілда [8]). Очевидно, що алгоритм порівняння складається з етапів. Так, етапу визначення змісту порушення як фрази передує визначення загальної ваги зв'язків між словами, з котрих складена фраза. А визначенню слів з БД порушень, відповідних за змістом до слів з котрих складена фраза ДФ, передує визначення загальної ваги зв'язків між літерами, з котрих складене слово. Цей, останній за розглядом етап, може бути виключеним, якщо дозволити і БД порушень і фразам, що визначають ДФ, користуватися тільки визначеним набором словосполучень.

У будь-якому разі АП і її сіть є ієрархічною структурою (іноді її називають асоціативно-проективною моделлю нейроподібної сіті [10]) або двох-, або трьох- чи більше рівневою. Кількість рівнів залежить від обмежень, котрі допускає модель у своїй структурі. У наведеному прикладі - якщо набір слів може бути довільним, тоді ієрархія сіті (літери – слова – фрази) має три рівні.

Така структура може ілюструватися як на рис.1.

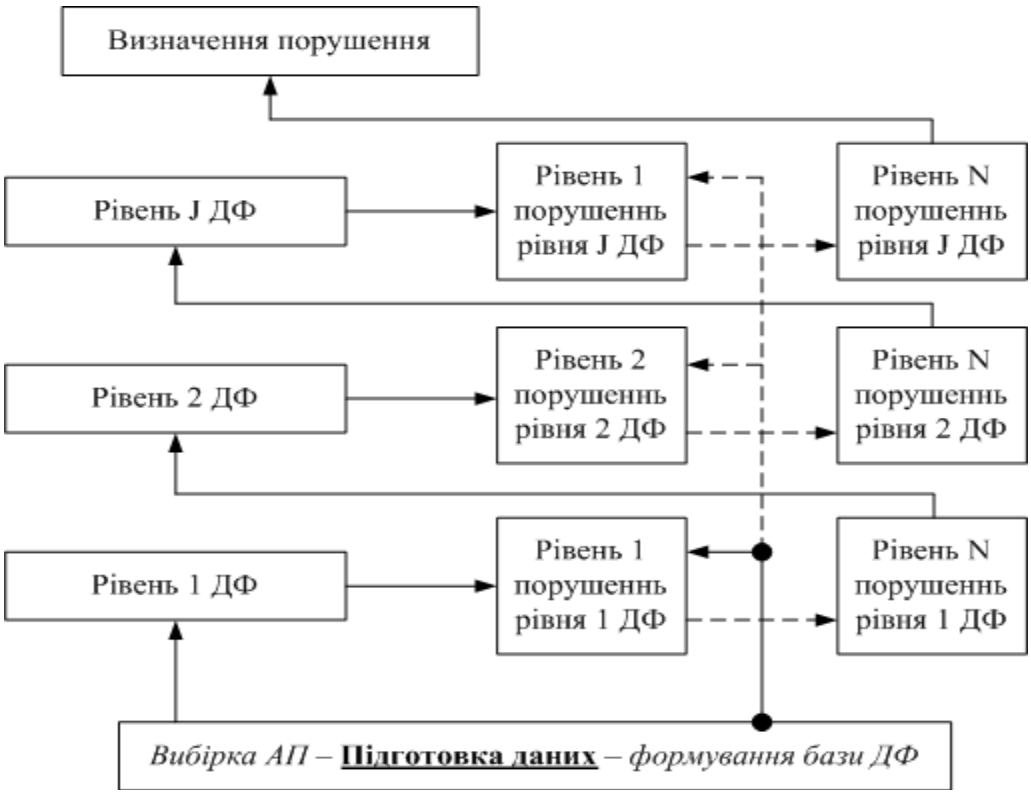

Рис.1. Схематична структура ієрархічної АП в якості сітьової моделі.

На нижньому рівні «Підготовка даних» здійснюються дві процедури.

По-перше, заздалегідь, здійснюється заповнення бази ДФ визначеннями з фраз сенсового змісту ДФ та відповідними визначеннями порушень. Набір фраз, як було визначено раніше, або є довільним, або є визначеним набором словосполучень (наприклад, з списку, наведеному в [15]). Змістовно, це є процедура «навчання» сіті бази ДФ за відомим алгоритмом [10] з формуванням вагових коефіцієнтів між елементами сіті що відповідають сукупності декотрих ДФ та відповідними визначеннями порушень. Зв'язки між ДФ та порушеннями формуються з якнайбільшої сукупності таких зв'язків у вже діючих об'єктах, тобто з якнайбільшої кількості проектів діючих об'єктів. При цьому формуються множини елементів сіті БД ДФ, поєднаних сенсовим змістом, за визначеними згідно алгоритму правилами. Ця частина процедур над сіттю передує життєвому циклу системи проектування і має сенс початкового навчання сітьової моделі. Надалі, БД ДФ та зв'язків з відповідними порушеннями (надалі БД ДФ) зберігається в процесі життєдіяльності моделі і може поповнюватися (процедура «донавчання»). З плином часу декотрі елементи сіті можуть «повільно забуватися» за відомим алгоритмом зменшення ваги зв'язків між елементами сіті [10,16] при накопиченні з часом сіттю БД все більшої кількості елементів (фраз) з близьким, але не повністю співпадаючим змістом. Таким чином, з часом, якщо сенс декотрої статистично значимої частини БД ДФ почне змінюватися, набуваючи нового змісту, сіть здатна автоматично реагувати на такі зміни повільно зменшуючи вагу «старих» зв'язків, та одночасно формуючи «нові» на їх місце. Так властивість є принципово суттєвою для даного випадку, оскільки забезпечує відповідне до поточного стану нормативно-правової та методичної бази ТЗІ переналаштування БД ДФ при наявності відкритості цієї БД, що забезпечує її розвиток та адаптацію до нових умов існування на життєвому циклі, причому незалежно від властивостей чи вподобань проектанта. Тобто, забезпечується принципова об'єктивність прийняття рішень при здійсненні процесу проектування системи захисту будь-якого ОІД.

По-друге, рівень підготовки даних готує вихідні дані у вигляді «вибірка АП» для пред'явлення сіті в заданому вигляді (форматі), зрозумілому сіті. Ця процедура здійснюється при обстеженні кожного нового об'єкту коли БД ДФ вже є заповненою (сіть вже є навченою). Саме ця процедура супроводжує життєвий цикл системи проектування. Кожна

нова вибірка для АП пред'являється до сіті, котра за принципом АП знаходить у БД ДФ відповідні до ДФ порушення.

Розподіл за рівнями 1 – J реалізує методологію формування ієрархічної структури літер – слів – фраз що може забезпечити повну автономність системи проектування у термін життєвого циклу.

Таким чином, загалом, здійснюється алгоритм роботи представленої АП. За такого підходу, представлені властивості сітьової АП мають забезпечити такі властивості системи проектування:

1. Сіть є здатною до забезпечення асоціативної відбірковості за змістом запиту при наявності визначеної близькості змісту вихідних текстових даних, що характерні для проектів КСЗІ згідно діючої нормативної бази ТЗІ;

2. Метод підготовки даних при навчанні і в життєвому циклі визначений тим, що вихідними даними є тексти (фрази з кінцевим змістом) сенсовий зміст яких має визначати сіть. Тобто ефективність підготовки даних визначається наявністю подробиць, що формують сенс фрази. Така наявність забезпечується на етапі «навчання» сіті, тобто може бути теоретично будь-якою. Таким чином, дані можуть бути представленими настільки ефективно, щоб забезпечити можливість квазіоптимальних рішень для ситуацій щодо ДФ на реальних ОІД;

3. Щодо способу представлення вихідної вибірки інформації за способом кодування очевидно, що може здійснюватися або позиційне кодування або стохастичне [7] Стохастичне кодування вихідних даних забезпечує нечутливість сіті до збоїв або неповних чи протирічних даних. Але має оцінюватися достовірність виділення вибірок за змістом запиту в АП. Тобто необхідно розробити критерій визначення ступеня змістовної достовірності вибірок. При цьому близькість за Хемінговською відстанню не можна розглядати як повний еквівалент змістовної близькості або відмінності. Це означає, що стохастичне кодування відрізняється меншою точністю представлення даних і це питання вимагає подальшого аналізу.

4. З моменту початку життєвого циклу системи проектування об'єктивність прийняття рішень вже не залежить від кваліфікації проектанта, а громіздкість системи та швидкість її роботи залежить від рахувальних можливостей комп'ютера – проектувальника, що є технічною задачею і не має принципових обмежень.

Якщо розглянути діючі системи проектування, можна визначити місце запропонованого підходу щодо проектування КСЗІ.

Наразі відомі і широко використовуються системи післяпроектного аудиту безпеки CRAMM, Cobra, RiskWatch, Buddy System, діючі САПР зазначені на початку статті та використовуються різноманітні методи проектування від графоаналітичних до морфологічних та таких, що враховують онтологічні властивості зрілості проектів, тобто, реально, немає єдиної системи, здатної до автоматизації для реального обслуговування різноманітних діючих об'єктів від «виділених приміщень» до глобальних систем зв'язку за типом телефонних мереж або Internet. Тому і нормативно-методична база та база стандартизації в галузі ТЗІ, а особливо при створенні КСЗІ ОІД та інформаційно-комунікаційних систем, відрізняється надмірним перевантаженням слабко узгоджених між собою документів, реально здатних лише частково забезпечити КСЗІ для інформаційно-комунікаційних систем. Запропонований підхід не вимагає такої розгалуженої документації і принципово дозволяє створити єдиний методичний підхід до складання ДСТУ для ОІД будь-якого типу та масштабу. Тому зазначений підхід є більш прогресивним, ніж намагання вдосконалити діючу систему стандартизації та методики і норми ТЗІ.

Висновки. У структурі АП може бути закладеним зміст усіх (або більшості) признаків незахищеності ОІД будь-якого типу за рахунок того, що асоціативний характер вибраних фрагментів текстів проявляється автоматично. Це надає великі переваги сітьовим АП над АП інших типів і дозволяє створити САПР для КСЗІ уніфікований і до умов існування і до складності реальних об'єктів.

Однак реалізація такої системи проектування зустрічає складність. Необхідність заповнення БД ДФ даними, отриманих від діючих проектів реальних об'єктів, є масштабним завданням, котре вимагає організаційних заходів що не мають аналогів. Для цього потрібно накопичити інформацію щодо проектів таких ОІД на території держави, котрі витримали перевірку часом, тобто захист котрих є дієвим і не вимагає вдосконалення вже певний час. Термін часу, котрий може бути достатнім для визначення властивості реальної стійкості об'єкта від загроз, має складати роки. Кількість об'єктів, проектами котрих необхідно скористуватися, повинна бути настільки великою, щоб забезпечити статистичну достатність (об'єктивність) інформації, котру накопичить АП. Враховуючи те, що доступ до проектів діючих ОІД має, з об'єктивних причин, зустріти супротив власників ОІД, процедура збору даних є складною, а достовірність отриманої інформації має вимагати перевірки (регламент котрої також є невизначеним). Таким чином, створення БД у даному разі вимагає проведення робіт в рамках держпрограми з можливістю використання допоміжних повноважень при отримані даних від діючих ОІД та їх аудиту.

ЛІТЕРАТУРА

1. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. www.dsszzi.gov.ua/dstszi/control/ru/publish/category

2. Гордиевский М.Д. Управление рисками в высокотехнологичных проектах: состояние и подходы управления / М.Д.Гордиевский, А.А.Поляков//Методи та засоби програмної інженерії.-2008.-1.-с. 311-319.

3. Липаев В. Оценка качества программных средств/ В.Липаев // ИСП РАН «Сетевой журнал».-2002.-№3.-с.37-41.

4. И.В.Груздо. УДК 681.518. Повышение качества программного проекта за счет управления рисками. НАУ им. Н.Е.Жуковского «ХАИ», Харьков. – [Электрон. ресурс]. – Доступ до статті: http://www/nbuv.gov.ua/natural/soi/2009_1/Gruzdo.pdf

5. И. Медведовский. Современные методы и средства анализа и контроля рисков информационных систем компаний CRAMM, RiskWatch, Гриф. – [Электрон. ресурс]. – Режим доступу до статті: idm@dsec.ru. 17.01.04.

6. А. Астахов. Анализ ристков и управление ими. Центр аудита информационной безопасности. – [Электронный ресурс]. – Доступ до статті: http://bezpeka.ladimir.kiev.ua/pg/show/risks/page2.html. - Заголовок з екрану.

7. Луценко В.М. Можливості автоматизації проектування КСЗІ з використанням інтелектуалізованих технічних засобів підтримки прийняття рішень. //Проблеми створення, розвитку та застосування інформаційних систем спеціального призначення». 18-а науково-практична конфер. Збірка. наук. праць. Житомир, ЖВІ, НАУ, МО України, 2011, №5, с. 77-87.

8. Hopfield J.J., Tank D.W. Neural Computation of Decisions in Optimization Problems.// Biological Cybernetics – 1985. – 52, No. 3. – p. 141-152.

9. Амосов Н.М., Касаткин А.М., Касаткина Л.М., Талаев С.А. Автоматы и разумное поведение. –Киев: Наук думка, 1973. -370 с.

10. Луценко В.Н. Особенности построения многопроцессорных вычислительных устройств для моделирования нейронных сетей. Автореф. на соиск. к.т.н., спец. 05.13.13 – «вычислительные машины, комплексы, системы и сети», ИК АН УССР им. В.М.Глушкова. 1988. 15 с.

11. Подготовка данных и формирование инвариантов в системах искусственного интеллекта./Луценко В.Н. – Киев, 1992.-21 с. – (Препр./АН Украины, Ин-т кибернетики им. В.М.Глушкова; 92-2), 1992, 21 с.

12. Мачуський Є.А., Луценко В.М. Використання елементів засобів інтелектуальної підтримки прийняття рішень при проектуванні систем інформаційної безпеки. X международная научная конференция имени Таран Т.А. «Интеллектуальній анализ информации ИАИ-2010», 18-21 мая 2010 г., Сб. трудов. – К.: «Просвіта», с. 207-213.

13. Луценко В.М., Худяков В.О. Визначення уразливості об'єктів інформаційної діяльності як складова порядку розробки систем захисту інформації. //Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. .-К.: ЧП «ЕКМО», НИЦ «ТЕЗИС» НТУУ «КПИ», 2010. Вип. 2 (21) с. 49-55.

14. Луценко В.М. Системи інтелектуальної підтримки прийняття рішень при проектуванні комплексних систем захисту інформації. Наук. вісті. Наук. тех. Журнал.-К: НТУУ «КПІ» ВПІ ВПК «Політехніка». №5, 2010, с.68-74.

15. Герасименко В.А. Защита информации в автоматизированных системах обработкиданных. Кн. 1. – М.: Энергоатомиздат, 1994. – 400 с.

16. Стохастические нейроподобные сети с ансамблевой организацией / Н.М.Амосов, Э.М.Куссуль, А.М.Касаткин, Л.М.Касаткина. – Киев, 1989. – 30 с. –(Препр./АН УССР, Ин-т кибернетики им. В.М.Глушкова; 89-25).

Надійшла: 15.12.2011

Рецензент: д.т.н., проф. Конахович Г.Ф.