НАУКОВО-ТЕХНІЧНИЙ ЖУРНАЛ «ЗАХИСТ ІНФОРМАЦІЇ» №1, 2011

УДК 004.43(031):681.3.01(02) **Луценко В.М. (НТУУ «КПІ»)**

ПРОЕКТУВАННЯ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З ВИКОРИСТАННЯМ ТЕХНІЧНИХ ЗАСОБІВ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

Розглянуто проблеми аналізу властивостей засобів підтримки прийняття рішень для створення проектів систем захисту інформації. Визначено основні властивості таких проектів. Запропоновано підхід до створення загальної методики проектування комплексної системи захисту інформації.

Вступ

Створення складних систем, які передбачають необхідність прийняття рішень при протирічних або неповних даних є напрямком, котрий має тенденцію до розвитку. Це стосується також і систем захисту інформації, а особливо комплексних (КСЗІ) для інформаційно-комунікаційних систем та інформаційних систем на об’єктах інформаційної діяльності [1,2].

Керований розвиток є процесом, котрий передбачає шлях для досягнення такої мети. Наприклад, при створенні методології проектування КСЗІ, ціллю може бути напрацювання комплекту ДСТУ, нормативних та методичних документів, за допомогою яких кваліфікований виконавець здійснює проектування. Однак з плином часу умови існування об’єктів інформаційної діяльності, такі, як зовнішнє середовище, внутрішні властивості, шляхи інформаційних атак, тощо, змінюються. Таким чином, проект захисту та реальні властивості об’єкту, такі, як властивості зрілості процесів захисту [3], визначення об’єктивної відповідності моделі загроз умовам існування об’єкту, об’єктивність опису об’єкту що складає його образ [4] при застосуванні методів формалізації опису, змінюються безперервно. Крім того, наразі не є реально визначеною кінцева ціль шляху до досконалості проекту КСЗІ, не є визначеною завершеність необхідного переліку безсумнівних властивостей КСЗІ. У таких умовах процес проектування носить дещо випадковий, суб’єктивний характер. Очевидним також є той факт, що реальні проекти за якісними показниками постійно відстають від життєвих вимог. Вимоги щодо життєздатності системи проектування об’єктів, як відомо, можна сформулювати таким чином:

1. Система має створюватись на базі принципово об’єктивного проектування, незалежного від вподобань та кваліфікації авторів проектів;
2. Система захисту має бути відкритою щодо можливості змін складових бібліотек методів та засобів захисту або умов життєдіяльності об’єкту, а тому має постійно враховувати його історію;
3. Проект системи має вважатися завершеним при умові, якщо у визначений термін часу повторне незалежне проектування дає однаковий результат. При цьому під визначеним терміном часу слід вважати настільки малий термін, при закінченні якого властивості об’єкту не змінюються.

При іншому підході на шляху створення єдиної, універсальної, адаптованої до часових змін існування об’єкту системи проектування може використовуватися система, створена з залученням засобів інтелектуальної підтримки прийняття рішень. Зазвичай, така система використовує асоціативну пам'ять (АП) з вибіркою за змістом та навчанням. Функцією АП є визначення шляху трансформації вихідних даних у кінцеве рішення на підставі досвіду що накопичується від проектів реально діючих об’єктів. Звісно, навчанням при цьому, є пред’явлення до АП великої (настільки великої, щоб можна було сподіватися на статистичну незалежність окремих проектів) кількості параметрів кваліфіковано створених діючих проектів. При такому підході принципово можливим є створення єдиної універсальної та відкритої до самостійного розвитку системи, якість роботи котрої буде залежати від часу існування (накопиченого досвіду).

Загалом, таке завдання здатне виконуватися з використанням асоціативно-проективних нейроподібних сіток [5]. Головною проблемою при цьому є спосіб формалізованого представлення вихідних, проміжних та кінцевих даних та розробка методу їх кодування.

На перший погляд вирішення саме цієї проблеми і є найбільш нереальною. Мабуть так і є, якщо намагатися створити методологію реалізації проектів виключно на сітках, тобто весь шлях проектування на усіх його етапах здійснювати за рахунок використання єдиної сітки. Якщо ж розділити проектування на етапи таким чином, що окремо визначеними будуть такі, котрі піддаються жорсткому алгоритмуванню і такі, що вимагають прийняття квазіоптимальних рішень при протирічних або неповних даних, тоді сіті можна використовувати виключно фрагментарно, без збитків щодо якості проектів.

1. Проблеми, щодо проектування КСЗІ

Загальний опис структури проектів захисту є складним і загалом неоднозначним завданням, а створення системи захисту можна звести до 9 етапів:

1. Обстеження інформаційної та інформаційно-комунікаційної системи з підготовкою базових даних;
2. Формування політики безпеки;
3. Розробка технічного завдання на створення системи захисту;
4. Розробка проекту;
5. Введення системи захисту в дію та оцінка захищеності;
6. Попередні випробування;
7. Дослідна експлуатація;
8. Державна експертиза системи;
9. Супроводження системи.

Склад системи також складний. До нього відносять:

1. Службу захисту інформації;
2. Комплекс засобів криптозахисту;
3. Комплекс засобів захисту від несанкціонованого доступу;
4. Інженерно-технічні заходи;
5. Фізичну охорону об’єкту;
7. Комплекс засобів блокування технічних каналів;
8. Регламентацію дій користувача.

При цьому нормативно-правове забезпечення є досить громіздким. Головні визначення наведені у Постанові Кабінету Міністрів України від 16.11.2002 № 1772 «Про затвердження порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах», де:

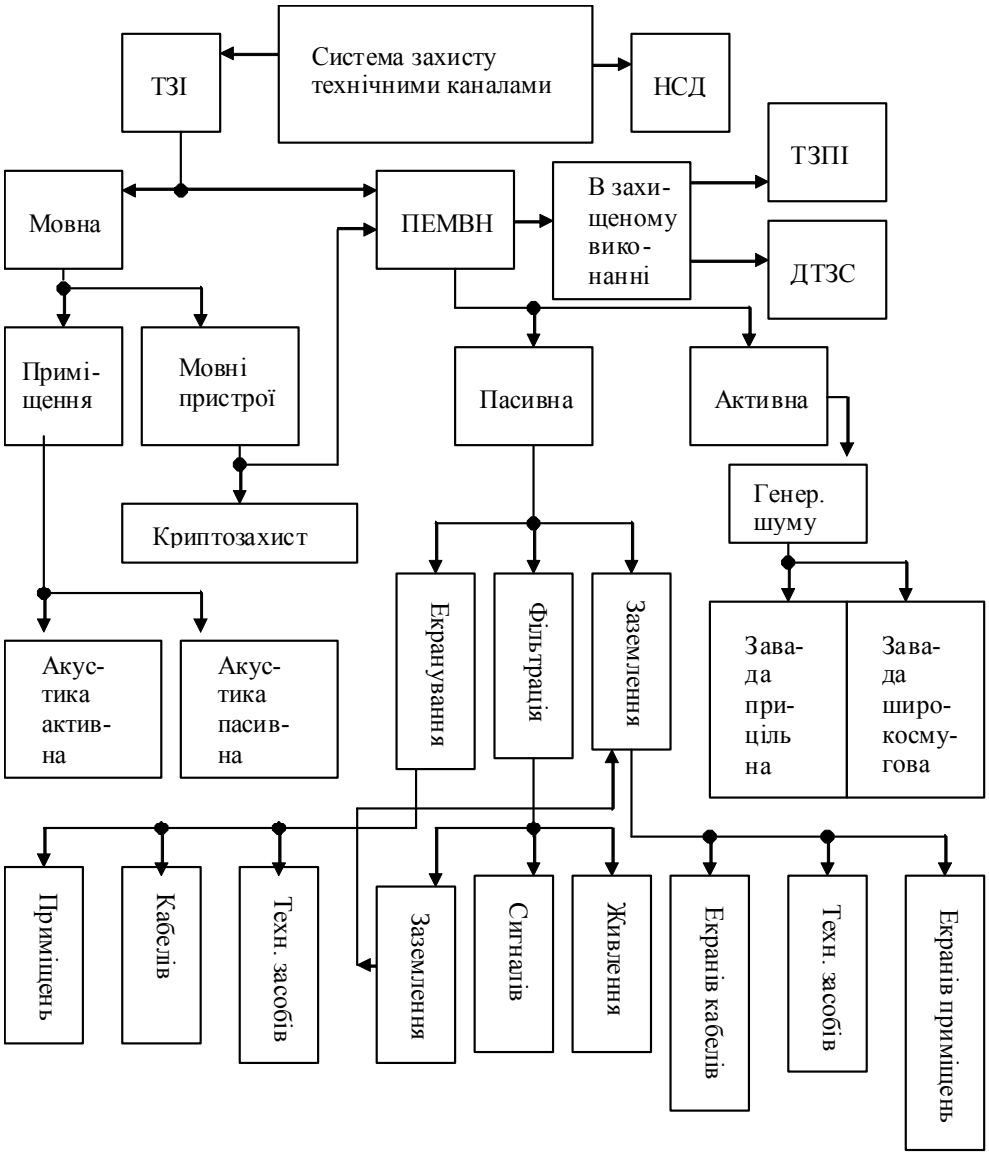
- інформаційна система є організаційно-технічною системою обробки інформації за допомогою технічних і програмних засобів;
- комплексна система захисту інформації є сукупністю організаційних, інженерно-технічних заходів, засобів і методів технічного та криптографічного захисту інформації;
- телекомунікаційна система є сукупністю технічних і програмних засобів, призначених для обміну інформацією шляхом передавання (випромінювання) або приймання сигналів, знаків, звуків, рухомих чи нерухомих зображень або іншим способом.

Якщо розглядати об’єкт захисту не тільки в якості інформаційно-телекомунікаційної системи, а і в якості буквального тлумачення наведеної вище інформаційної системи, тоді об’єктом захисту має бути будь-який об’єкт інформаційної діяльності (ОІД) на котрому циркулює інформація з обмеженим доступом, незалежно від наявного виду інформаційних комунікацій.

При такому визначенні загальна структура процедури моделювання об’єкту захисту має вигляд, наведений на рис.1.

Рис.1. Процедура моделювання при проектуванні КСЗІ.

Загалом зазначені етапи є послідовними багатокроковими процесами з складною структурою. Кожний процес забезпечується великою кількістю методологічних документів, котрі визначають лише загальну методику створення проекту захисту, а можливість конкретизації кожного кроку не є реальною з причини великої різноманітності об’єктів. Наприклад, моделювання методів і засобів захисту вміщує визначення напрямків захисту, котрі у свою чергу визначають методи захисту, котрі у свою чергу визначають можливі засоби захисту. Останні розділяються на організаційні та технічні, причому спрямовані як на забезпечення інтересів захисту технічними каналами так і захисту від несанкціонованого доступу. Для прикладу, структура системи захисту технічними каналами без урахування інтересів захисту від несанкціонованого доступу [6] має вигляд, наведений на рис.2.



ТЗІ – технічний захист інформації;
НСД – несанкціонований доступ;
ПЕМВН – побічні електромагнітні випромінювання та наведення;
ТЗПІ – технічні засоби перетворення інформації;
ДТЗС – допоміжні технічні засоби та системи.

Рис.2. Структура системи захисту інформації від витоку технічними каналами.

Зауважимо ще раз, що у даному випадку до розгляду не є залученою структура системи захисту комунікаційно-інформаційних та комп'ютерних систем зв'язку в якості окремих об'єктів технічних засобів перетворення інформації (ТЗПІ). Така система, аналогічно системі захисту від несанкціонованого доступу, в наданій структурі має бути представленою окремим відгалуженням від систем захисту технічними каналами.

Очевидно, що автоматизація процесу проектування навіть для такого, найбільш консервативного фрагменту зустрічає складності, наприклад, на етапі визначення пріоритету між криптозахистом та захистом від ПЕМВН, а захист каналами ПЕМВН має елемент неоднозначності між вибором засобів пасивного захисту, активного захисту, або використанням технічних засобів в захищеному виконанні.

Якщо перенести наведену ілюстрацію на всі етапи за напрямками моделювання, можна визначити цілу низку переходів між етапами, де спостерігається невизначеність вибору

подальших рішень. На практиці завдання щодо прийняття рішень вирішуються за рахунок кваліфікації та вподобань проектанта і згідно його досвіду. В результаті практичні проекти відрізняються невиправданою різноманітністю навіть у майже однакових умовах, а оптимізація проектів як за структурою і використанням засобів захисту, так і за кошторисом, залежить виключно від кваліфікації проектанта.

3. Місце інтелектуалізованих засобів підтримки прийняття рішень при створенні проектів КСЗІ

З наведеного витікає необхідність створення системи проектування незалежної від користувача та об'єктивно здатної до невипадкової оптимізації рішень, але не за рахунок декотрого розробленого алгоритму оптимізації, а за рахунок попереднього досвіду якнайбільшої кількості діючих проектів, тобто статистики вже отриманих рішень.

Так, напрямок моделювання загроз складається з трьох основних етапів, на основі котрих формується проект захисту, а саме: визначаються джерела загроз; визначаються цілі, на котрі направлені загрози; створюються моделі загроз.

При визначенні джерел загроз необхідно скласти їх список і за цим списком визначити перелік дестабілізуючих факторів (ДФ). Цей фрагмент піддається жорсткій алгоритмізації і не вимагає втручання сітьового моделювання. Подальший шлях проектування передбачає перехід від ДФ до моделі загроз за рахунок визначення цілей, на котрі направлені загрози. Проведення об'єктивного аналізу цілей загроз для об'єктів середньої та великої складності є завданням нечітким і на цьому етапі використання засобів підтримки прийняття рішень є виправданим. При цьому, сукупність цілей загроз об'єкту представляється підмножиною цілей характерних для того об'єкту що розглядається, з загальної множини можливих цілей для будь-якого об'єкту, тобто декотрих елементів образу об'єкту. Особливо вдалим у цьому випадку є те, що при переході від джерел загроз до моделі процедура визначення цілей загроз є необхідною тільки на попередньому етапі підготовки засобу підтримки прийняття рішень. Наприклад, при використанні в якості засобу підтримки прийняття рішень асоціативної пам'яті на базі відомої моделі нейроподібної асоціативно-проективної ансамблевої сіті [7,8], тоді попереднім етапом підготовки є етап навчання сіті. Тобто проектант захисту об'єкту є звільненим від складання переліку цілей. Його завданням на цьому етапі є тільки опис самого об'єкту без громіздкої та загалом неоднозначної експертизи ступеня його захищеності.

Аналогічно виглядає моделювання при переході від моделі загроз до напрямків захисту, котрі є головною складовою створення моделі методів і засобів захисту. При цьому в ансамблевому представленні мають бути визначені лише напрямки захисту.

Декотрі інші етапи проектування системи захисту також можуть моделюватися з використанням засобів підтримки прийняття рішень, що і є предметом поточних розробок фахівців з інформаційної безпеки.

Література

1. ДСТУ ISO/IEC TR 13335:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1: Концепції та моделі безпеки інформаційних технологій. Частина 2: Керування та планування безпеки інформаційних технологій. Частина 3: Методи керування безпекою інформаційних технологій.

2. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

3. Потій О.В. Онтологічні моделі властивостей зрілості процесів захисту інформації. Харьков. Прикладная радиоэлектроника. ISSN 1727-1290. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. 2009г., т. 8, №3, с.388-395.

4. Ayaz Isazadeh. Behavioral Views for Software Requirements Engineering. A thesis submitted to the Department of Computing and Information Science in conformity with the requirements for the degree of Doctor of

Philosophy Queen's University Kingston, Ontario, Canada, September 1996. (Досяжні в Інтернет www.sciencedirect.com).

5. Байдык Т.Н. О возможной организации системы принятия решений – В кн. Нейроподобные сети в робототехнике. – Киев: ИК АН УССР, 1979, с. 58-72.

6. Мачуський Є.А., Луценко В.М. Використання елементів засобів інтелектуальної підтримки прийняття рішень при проектуванні систем інформаційної безпеки. Интеллектуальный анализ информации ИАИ-2010. X международная научная конференция имени Т.А. Таран. Киев, 18-21 мая 2010 г.: сб. тр., -К.: Просвіта, 2010.- с. 207-213.

7. J.J. Hopfield, D.W. Tank. “Neural” Computation of Decisions in Optimization Problems. “Biological Cybernetics”, vol. 52, No 3, 1985, p. 136,141-152.

8. Амосов Н.М., Касаткин А.М., Касаткина Л.М., Куссуль Э.М. Нейроподобные сети в системах искусственного интеллекта. Нейроподобные сети и нейрокомпютеры: Сб науч тр. / АН УССР. Ин-т кибернетики им. В.М. Глушкова. Науч. Совет АН УССР по пробл. «Кибернетика». –Киев, 1990. – с. 4-13.

Надійшла: 16.03.11

Рецензент: д.т.н., проф. Квасніков В.П.