УДК 004.43(031):681.3.01(02)

В.М. ЛУЦЕНКО

Науково-технічний університет України «КПІ», Київ

ПРОЕКТУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ З ВИКОРИСТАННЯМ ТЕХНІЧНИХ ЗАСОБІВ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

Анотація. Розглядаэться проблема аналізу властивостей методів та засобів підтримки прийняття рішень для створення проектів систем захисту інформації. Визначено основні властивості таких проектів. Запропоновано підхід до створення нової методики проектування системи захисту інформації від несанкціонованого доступу.

Ключові слова: Захист інформації; комплексна система захисту; асоціативна пам'ять; нейроподібна сіть.

Аннотация. Рассматривается проблема анализа свойств методов и средств поддержки принятия решений для создания проектов систем защиты информации. Определены основные свойства таких проектов. Предложен подход к созданию новой методики проектирования систем защиты информации от несанкционированного доступа.

Ключові слова: Защита информации; комплексная система защиты; ассоциативная память; нейроподобная сеть.

Annotation. The paper considers problem of analyzing of property of means of support of acceptance of decisions for information security systems projects. The basic properties of such projects are given.The technique of complex system designing for non-authorized access protection is developed on the basis of means of support of acceptance of decisions.

Keywords: Protection of the information; complex system of protection; associative memory; neuronal network..

Вступ

Згідно НД ТЗІ 1.1-003-99 [1] несанкціонований доступ до інформації визначається таким чином: НСД до інформації (unauthorized access to information) — доступ до інформації, здійснюваний з порушенням правил розмежування доступу (ПРД). Таке визначення поширюється і на комп’ютерні системи. Причому згідно [2] несанкціоновані дії щодо інформації в системі - дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства. Якщо не зосереджуватись на комплексних системах захисту інформації (КСЗІ), а розглядати питання використання систем захисту інформації (СЗІ) у вигляді ще й комплексу технічного захисту інформації на об’єкті інформаційної діяльності згідно положень НД ТЗІ 1.1-005-07 [3], тоді загалом не має значення чи мова йде про захист об’єктів інформаційної діяльності (ОІД) де циркулює інформація з обмеженим доступом (ІзОД), включаючи виділені приміщення (ВП), призначені виключно для проведення конфіденційних переговорів, нарад, доповідей, тощо, чи про автоматизовану систему (АС) як тіло інформаційно-комунікаційної або комп’ютерної системи. Сукупність обох видів об’єктів можна умовно називати об’єктом захисту загальної структури (ОЗЗС). Загальний хід проектування для обох випадків однаковий. Різниця спостерігається у визначенні сенсу та місця рубежу захисту та визначенні сенсу імен і факторів що складають загрози з одного боку та напрямки захисту з визначенням методів і засобів захисту з другого боку. Оскільки створення КСЗІ передбачається як на об’єктах АС і комп’ютерних системах, так і на ОІД (наприклад у ВП), тоді при створенні автоматизованих систем проектування захисту інформації має сенс розглядати КСЗІ (як технічного захисту, так і від несанкціонованого доступу) для ОЗЗС, а не тільки для АС. Згідно з чинниками, визначеними в [4,5], автоматизація проектування системи захисту інформації як технічними каналами так і від НСД на ОІД є завданням проектування складних систем.

Створення складних систем, які передбачають необхідність прийняття рішень при протирічних або неповних даних є напрямком, котрий має тенденцію до розвитку. Це стосується і інформаційно-комунікаційних систем і об’єктів інформаційної діяльності [6,7].

Як зазначено в [5] керований розвиток є процесом, котрий передбачає шлях для досягнення декотрої мети. Наприклад, при створенні методології проектування КСЗІ, ціллю може бути напрацювання комплекту документів, за допомогою яких кваліфікований виконавець здійснює процес 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 [8], визначення об’єктивної відповідності моделі загроз умовам існування об’єкту, об’єктивність опису об’єкту що складає його образ [9] при застосуванні методів формалізації опису змінюються безперервно. Крім того, наразі не є реально визначеною кінцева ціль шляху до досконалості проекту КСЗІ, не є навіть 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.

Іншим підходом на шляху створення єдиної, універсальної та адаптованої до часових змін існування об’єкту системи проектування може бути система, створена на засадах інтелектуальної підтримки прийняття рішень. Така система може використовувати асоціативну пам'ять (АП) з навчанням для визначення шляху трансформації вихідних даних у кінцеве рішення на підставі накопиченого досвіду з 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 кваліфіковано атестованих діючих проектів. При такому підході принципово можливим є створення єдиної універсаль-

ної та відкритої до розвитку системи. Її якість роботи буде залежати від часу існування, тобто накопиченого досвіду.

Загалом, таке завдання здатне виконуватися з використанням асоціативно-проективних нейроподібних сіток [10]. Головною проблемою при цьому є спосіб формалізованого представлення вихідних, проміжних та кінцевих даних та розробка методу їх кодування.

На перший погляд саме ця проблема 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 сітьової моделі. Якщо ж розділити проектування на етапи таким чином, що визначеними будуть такі, що піддаються жорсткому алгоритмуванню і такі, що вимагають прийняття квазіоптимальних рішень при протирічних або неповних даних, тоді сіті можна використовувати фрагментарно, без збитків щодо якості проектів.

Одним з проблемних моментів при створенні КСЗІ є створення дієвої структури системи захисту інформації від НСД. Саме цьому моменту присвячена представлена стаття.

Актуальність

Реальні проекти захисту від НСД за якісними показниками мають об'єктивно відтворювати умови життєдіяльності об'єктів, але наразі, як зазначено вище, мають тенденцію до відставання від життєвих вимог. Для подолання такого відставання мають відтворюватися вимоги щодо життєдіяльності системи проектування окремо для кожного об'єкту у повному обсязі. Такі вимоги передбачають необхідність використання системи захисту що базується на принципово об'єктивному проектуванні, тобто такому, котре не залежить від якісних показників проектанта. Спроектована система захисту має бути динамічною у часі, тобто відкритою щодо можливості змін у часі складових методів та засобів захисту або умов існування об'єкту. Також актуальним є питання визначення необхідної та достатньої завершеності проекту системи захисту, а критерії завершеності наразі відсутні. Найголовнішою умовою завершеності проектів є формальна дієздатність системи захисту на даний час та відповідність реалізації спроектованої системи захисту фінансовим можливостям користувача.

Початком більш об'єктивного проектування має бути напрацювання методів та засобів отримання максимально повної та об'єктивної інформації про об'єкт на етапі його дослідження, а також інженерний аналіз для виявлення місць уразливості об'єкту, тобто визначення ступеня його стійкості до загроз.

Мета

Створення дієвої структури системи захисту інформації від НСД за рахунок досконалої системи проектування, принципово об'єктивного та незалежного від вподобань та кваліфікаційних властивостей проектантів.

Постановка задач

Створення життєздатної методики проектування систем захисту об'єктів від НСД, котра відповідає вимогам підвищеної об'єктивності проектів щодо реальних вимог захищеності. При цьому вимоги щодо життєдіяльності системи проектування можуть бути визначеними таким чином:

1. Система має створюватись на базі принципово об'єктивного проектування, незалежного від вподобань та кваліфікаційних властивостей авторів проектів.
2. Система захисту має бути динамічною у часі та відкритою до можливості змін складових бібліотек

методів і засобів захисту або умов життєдіяльності об'єкта, 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 котрого властивості об'єкта не змінюються.

Розв'язання задач

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

1. Обстеження інформаційної системи, АС або ОІД з підготовкою базових даних.
2. Розробка технічного завдання на створення системи контролю та обмеження доступу.
3. Розробка проекту.
4. Введення системи захисту в дію та оцінка захищеності.
5. Попередні випробування.
6. Дослідна експлуатація.
7. Експертиза системи відділом служби охорони.

Склад системи також складний. До нього відносять:

1. Службу охорони.
2. Комплекс засобів захисту від несанкціонованого доступу, контролю та обмеження доступу.

3. Інженерно-технічні заходи.
4. Фізичну охорону об’єкту.

При такому визначенні структура процесу моделювання об’єкту захисту має вигляд, як на рис.1.

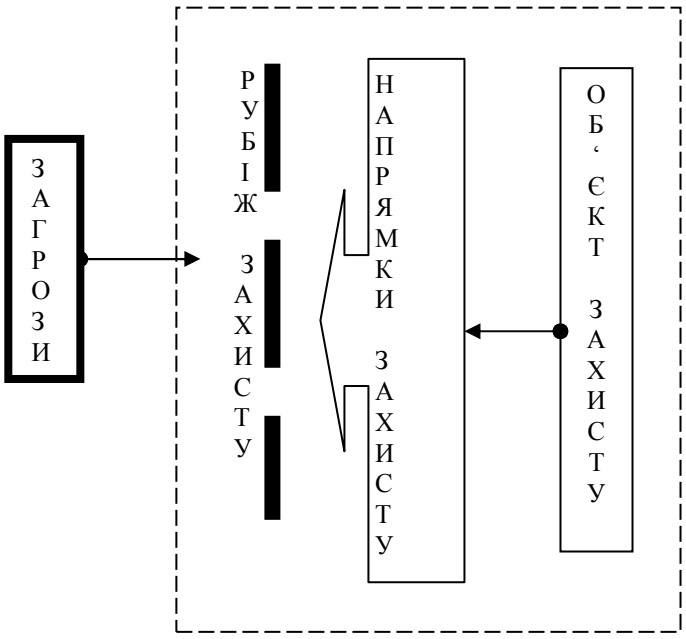

Рисунок 1 – Концептуальна модель процесу захисту інформації від НСД.

Якщо поставити завдання розподілити процес проектування системи захисту за етапами, то загалом зазначені етапи є послідовними багатокроковими процесами з складною структурою. Кожний етап забезпечується великою кількістю методологічних документів, котрі визначають лише загальну методику створення проекту захисту і можливість конкретизації кожного кроку не є реально можливою з причини великого різноманітності параметрів та об’єктів. Наприклад, моделювання методів і засобів захисту від НСД 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. Структура системи захисту від НСД для ОЗЗС має вигляд, як на рис.2.

Очевидно, що автоматизація процесу проектування навіть для такого, найбільш консервативного фрагменту зустрічає складності, наприклад, на етапі визначення пріоритету між випадковими або зловмисними діями порушника, чи розподілі пріоритетів при виборі засобів виявлення факту порушення між фізичною охороною та сигналізацією і відеоспостереженням.

Якщо перенести наведену ілюстрацію на всі етапи напрямків моделювання автоматизованої системи проектування, визначається низка переходів між етапами, де спостерігається невизначеність вибору подальших рішень. На практиці такі 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 його кваліфікації. 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 двох основних етапів, на основі котрих формується проект захисту, а саме: визначення джерел загроз; визначення моделі порушника, котрий реалізує загрози.

Визначення джерел загроз є фрагментом, котрий піддається жорсткій алгоритмізації і не вимагає втручання моделювання з використанням засобів інтелектуальної підтримки за рахунок сітьового моделювання. Подальший шлях проектування передбачає перехід до моделі порушника з визначенням цілей, на котрі направлені загрози.

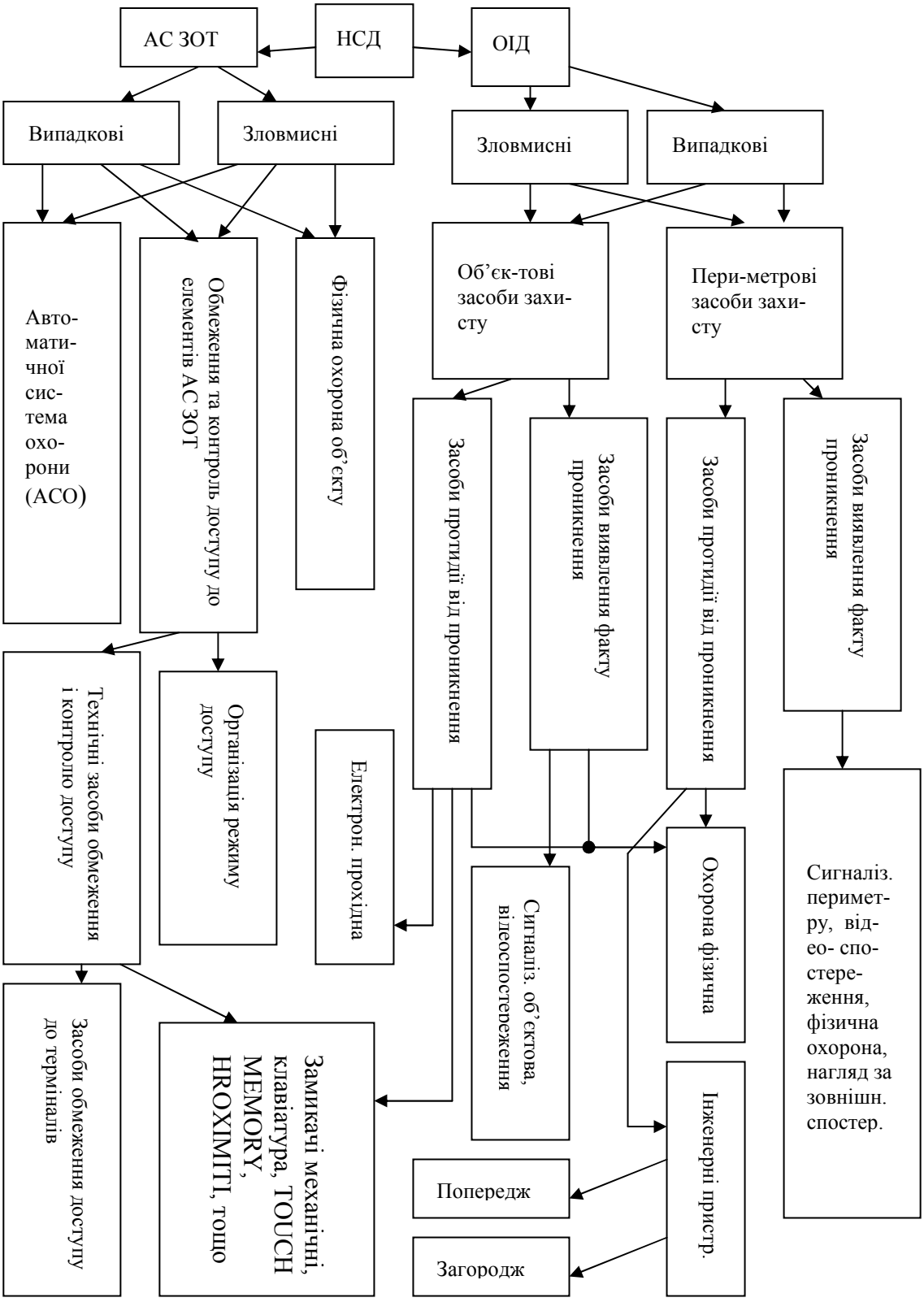

Рисунок 2 – Структура системи захисту ОЗЗС від НСД.

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 об'єкту що розглядається, з загальної множини можливих цілей, 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 моделі нейроподібної асоціативно-проективної ансамблевої сіті [11,12], 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.

Висновки:

Аналогічно виглядає моделювання наступного етапу, а саме перехід 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, що є умовою для реального створення системи проектування.

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.

Список літератури

1. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу»
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»
3. НД ТЗІ 1.1-005-07 «Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення»
4. В.М.Луценко. Система інтелектуальної підтримки прийняття рішень при проектуванні комплексних систем захисту інформації. «Наукові вісті», Наук. Тех.. журнал, НТУУ «КПІ» ВПІ ВПК «Політехніка», 2010, №5, с.с.68-74.
5. Мачуський Є.А., Луценко В.М. Використання елементів засобів інтелектуальної підтримки прийняття рішень при проектуванні систем інформаційної безпеки. X международная научная конференция имени Т.А.Таран «Интеллектуальный анализ информации ИАИ-2010», 18-21 мая 2010 г., Сборник трудов. – К.: «Просвіта», -с.207-213.]
6. 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.
7. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
8. 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.
9. 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).
10. Байдык Т.Н. О возможной организации системы принятия решений – В кн. Нейроподобные сети в робототехнике. – Киев: ИК АН УССР, 1979, с. 58-72.
11. J.J. Hopfield, D.W. Tank. “Neural” Computation of Decisions in Optimization Problems. “Biological Cybernetics”, vol. 52, No 3, 1985, p. 136,141-152.
12. 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.

.

Відомості про авторів

Луценко Володимир Миколайович – доцент фізико-технічного інституту (ФТІ) , докторант ФТІ НТУУ «КПІ», в.о. завідувача каф. Фізико-Технічних Засобів Захисту Інформації, кандидат технічних наук, Київ-03056, Проспект Перемоги 37, корп.11. тел. (044) 406-81-04, 097-7962914. e-mail: tarcomevl@ukr.net