1. Проблеми розвитку нормативної та методичної баз системи захисту інформації

УДК 004.43(031):681.3.01(02)

МОЖЛИВІСТЬ АВТОМАТИЗАЦІЇ ПРОЕКТУВАННЯ КСЗІ

Луценко Володимир
КПІ ім. Ігоря Сікорського

OPPORTUNITY OF AUTOMATION OF DESIGNING OF CSPI

Lutsenko Volodymir
Igor Sikorsky Kyiv Polytechnic Institute

Анотація: **Аналізується можливість та особливості автоматизації проектування комплексних систем захисту інформації.**
Ключові слова: **Інформація, захист інформації, комплексна система захисту інформації, автоматизація проектування.**
Summary: **The opportunity and features of automation of designing of complex systems of protection of the information is analyzed.**
Keywords: **The information, protection of the information, complex system of protection of the information.**

Вступ

Методи аналізу й керування ризиками відрізняються помітним різноманіттям. До найбільш поширених відносять: метод CRAMM [1], метод Cobra [2], метод Risk Watch, Buddy System, EBIOS, MEHARI, OCTAVE, CORAS, Гриф і т.п., і при їх використанні необхідно враховувати ступінь адаптованості цих реалізацій до особливостей українських користувачів. Німецький стандарт BSIMT є найбільш змістовним довідником із забезпечення безпеки ІТ. Але проблемою є відсутність єдиного ДСТУ, котрий мав би адаптованість до місцевих умов роботи об'єктів, тобто до законодавства України, особливості відношень між організаціями-користувачами в рамках діючої інфраструктури, місцеві та регіональні особливості в створенні структури ІС, вимоги до робочої та звітної документації, традиції., тощо. Але розглядати ці продукти з аудиту безпеки в якості засобів проектування, тим більше автоматизованими, було б некоректно. При цьому і аудит безпеки досі є завданням, що знаходиться на етапі розробки. При використанні стандарту BSIMT визначають шляхом обстеження конкретного об'єкту великого розміру перелік загроз. Навіть маючи повний перелік можливих контрдій, залишається невирішеною головна задача – знайти відповідність між можливими контрдіями і конкретними загрозами. Це залишається завданням для проектанта з його суб'єктивністю (вподобаннями, кваліфікацією, досвідом і. т.д.). Тому і виникають зовсім різні проекти комплексних систем захисту інформації (КСЗІ) для фактично однакових об'єктів, особливо великих, розподілених територіально та функціонально залежних, або автономних.

Враховуючи складності, які виникають в даному випадку на шляху автоматизації проектування КСЗІ, виникає питання – а чи є така можливість за умови єдності прийняття рішень проектантом доказової однозначності (об'єктивності таких рішень), мінімізації фінансового навантаження на результат проектування, тобто, на спроектовану систему захисту за умови достатності рівня захищеності об'єкту захисту (ОЗ)?

Формалізація складових проектування як об'єктів захисту

Початковим етапом завдання автоматизації проектування КСЗІ є етап формалізації складових проектів, тобто всіх можливих об'єктів автоматизації. Визначення, які наведені у статті можуть відрізнятись від загальноприйнятих і слугують для постановки задачі автоматизації проектування систем захисту. Зокрема це стосується об'єктів інформаційної діяльності (ОІД) та ін. Видів таких об'єктів декілька. Це інформаційно телекомунікаційні системи (ІТКС), об'єкти, які не вміщують у своєму складі ІТКС, наприклад, за визначенням, виділені приміщення (ВП), які будемо називати для спрощення просто ОІД, та уся сукупність комбінацій ІТКС та ОІД, яку для спрощення будемо називати об'єктами захисту загальної структури (ОЗЗС). Поєднання ОІД та ІТКС у вигляді ОЗЗС вимагає визначення мінімуму структурних варіантів типів об'єктів захисту, тобто базису структурних елементів. До них мають відноситися ті, що наведені у табл.1.

Таблиця 1.

Структури ОЗЗС

1.	ОІД, котрий не вміщує у своєму складі ІТКС
2.	ОІД, у склад котрого входить ІТКС, або декілька ІТКС, у тому числі, мережа загального користування (наприклад мережа INTERNET, або телефонна мережа)
3.	ІТКС, у склад якої входить ОІД, або декілька ОІД призначених для обслуговування ІТКС за її функціональним призначенням, або призначених також для її обслуговування за допоміжним функціональним призначенням (офісні приміщення, склади товарів, технологічні та виробничі приміщення, тощо)
4.	ОЗЗС, котрі визначені як головна ІТКС, у склад якої входить підлегла ІТКС'. У склад ІТКС' входять також і ОІД з своїм, визначеним для цього ІТКС' призначенням, що не несе функціональні обов'язки, характерні для головної ІТКС. Назвемо такі ОЗЗС гібридними ОЗЗС першого типу
5.	ОЗЗС, котрі визначені як головний ОІД у склад якого входять також і ІТКС з своїм, визначеним для цього ОІД призначенням, та ОІД' у складі цієї ІТКС. Причому, цей підлеглий ОІД' або несе, або не несе функціональні обов'язки, характерні для головного ОІД – гібридні ОЗЗС другого типу

Відсутність ІТКС як окремої структурної одиниці зумовлена тим, що інформації без носія бути не може.

З таких структурних елементів складається структура будь-якого ОЗЗС в рамках якогось інфраструктурного рівня, наприклад окрема кімната в межах структури підприємства або установи, що дислокується у межах району, який у свою чергу є складовою структури міста, а той є складовою структури області, котра у свою чергу структурується у регіонально-територіальному масштабі чи взагалі загальнодержавному. Найпростішим варіантом структури об'єкту захисту є такий, який не пов'язаний з локальним розташуванням. Фактично, така структура і є характерною, але наразі створення служби захисту інформації (СЗІ) та КСЗІ об'єктів захисту здійснюється без урахування їх приналежності до загальної структури цих об'єктів. Тобто, наприклад, характерним є випадок, коли розробляється КСЗІ ОІД у вигляді нового регіонального офісного приміщення. Це офісне приміщення є фрагментом більш загальної структури, наприклад системи зв'язку ІТКС', яка у свою чергу входить у більш загальну ІТКС для системи мобільного зв'язку (гібридний ОЗЗС першого типу). При цьому для цієї ІТКС КСЗІ вже є розробленою та діючою системою. Але розробка КСЗІ даного нового офісу може здійснюватися незалежно від КСЗІ його ІТКС, у тому числі і різними виконавцями. При цьому формуються умови життєдіяльності ОІД, вимоги до СЗІ, модель загроз, і.т.д., хоча ця робота вже є

проведеною для усього ОЗЗС і немає ніяких гарантій того, що проект захисту даного офісу буде вміщувати складові, що не мають протиріч з КСЗІ ІТКС. Загалом, КСЗІ офісу має повторювати пункти КСЗІ його ІТКС, або має створюватися як копія фрагменту КСЗІ його ІТКС. Таким чином, КСЗІ складних об'єктів має виглядати як ієрархічна структура жорстко пов'язаних між собою КСЗІ об'єктів нижнього рівня, узагальнення пунктів КСЗІ котрих складає КСЗІ об'єктів наступного, вищого рівня, і так далі до КСЗІ загального ОЗЗС. В інших випадках, навпаки, КСЗІ загального ОЗЗС має розподілятися на свої фрагменти у вигляді КСЗІ його ОІД та КСЗІ його ІТКС і знову ж таки створювати ієрархічну структуру у котрій об'єкт захисту нижнього рівня є відповідним фрагментом КСЗІ ОЗЗС. У будь якому випадку КСЗІ нижнього рівня не може вміщувати будь-яких вимог, яких немає у КСЗІ вищого рівня.

Таким чином, щодо правил формування КСЗІ складних об'єктів, то з огляду на викладене вище можна визначитися з положеннями щодо підходу до проектування КСЗІ у випадках коли ОЗЗС є розгалуженою однорівневою і коли ОЗЗС є ієрархічною багаторівневою структурою.

Якщо застосовувати структурний підхід, то тоді правила формування КСЗІ для ОЗЗС [3] можуть формулюватися для випадків, згідно табл. 2.

Таблиця 2.

Правила формування КСЗІ

Для ієрархічного розподіленого ОЗЗС:	
a) Випадок, коли ОЗЗС будується починаючи з нульового, вищого рівня структури, передбачаючи ієрархічність структури, що створюється, або обстежується	
1	До складу ТЗ на КСЗІ вищого рівня мають входити усі загальні вимоги до ТЗ КСЗІ нижчих рівнів
2	До складу ТЗ на КСЗІ нижчих рівнів не можуть включатися будь-які вимоги, котрі є відсутніми у складі ТЗ на КСЗІ нульового рівня
3	Проект КСЗІ для вищого рівня ОЗЗС має вміщувати у своєму складі проекти КСЗІ всіх об'єктів захисту нижнього рівня у якості своїх складових
b) Випадок, коли ОЗЗС будується починаючи з нижчого рівня структури, а майбутня ієрархічність загальної структури ОЗЗС є невизначеною	
1	КСЗІ для окремих ОЗЗС визначеного рівня створюються незалежно один від одного та без урахування майбутньої ієрархічності структури ОЗЗС
2	При появі фрагменту ОЗЗС наступного, вищого рівня, ТЗ на його КСЗІ та проект захисту створюється як сукупність пунктів ТЗ та проектів КСЗІ об'єктів нижчого рівня
3	ТЗ та проекти КСЗІ об'єктів вищого рівня можуть включати пункти, специфічні для ОЗЗС даного рівня за умови, якщо вони не мають протиріч з ТЗ та КСЗІ, визначених для будь-яких ОЗЗС нижчих рівнів
4	ТЗ та проект КСЗІ для ОЗЗС кожного наступного рівня має вміщувати усі пункти ТЗ та проектів КСЗІ, які були визначеними для усіх ОЗЗС попередніх, більш нижчих рівнів, у тому числі, специфічні за п.3 даного переліку, для попереднього рівня
Для однорівневого розподіленого ОЗЗС	
1	ТЗ та проект КСЗІ розробляється для кожного ОЗЗС незалежно один від одного
2	Пункти ТЗ та проектів КСЗІ будь-якого ОЗЗС не повинні мати протиріч з будь-якими пунктами ТЗ та проектів КСЗІ інших ОЗЗС
3	ТЗ та пункти проектів КСЗІ, що є специфічними для окремого ОЗЗС структури, додаються до його ТЗ та проекту КСЗІ у вигляді окремого пункту, тобто не можуть включатися як підпункт до вже існуючого переліку пунктів, визначених для інших ОЗЗС даної структури

При виконанні таких правил виникає можливість створення КСЗІ будь-яких видів ОІД, які складатимуть єдину технологічно-інформаційну структуру будь-якого рівня, у тому числі і державного рівня. В таку структуру включаються усі ОІД незалежно від їх призначення, масштабу та складності. Крім того, вперше з'являється реальна можливість створення методології побудови КСЗІ будь-якої складності у тому числі і за рахунок використання автоматизованої системи проектування. Тобто процес проектування отримує принципову можливість автоматизації за єдиною універсальною методикою.

За такого підходу, та при умові розробки відповідних ДСТУ і нормативно - методичної документації, з'являється можливість створення єдиного методу проектування ОЗЗС, що відрізняється досконалістю за рахунок прийняття рішень при реалізації проекту, незалежних від суб'єктивних властивостей проектанта.

Нагальність створення такого методу є безумовною, оскільки у діючій методиці проектування СЗІ (КСЗІ для АС ІТКС) базою є комплект ДСТУ, нормативні та методичні документи, що у своїй сукупності характеризуються взаємною неузгодженістю [4]. Наразі проекти КСЗІ створюються в умовах об'єктивної неможливості виконання усіх вимог діючої нормативно-методичної документації, а підхід, що розглядається, передбачає можливість вирішення зазначених протиріч.

Визначення та правила щодо моделювання комплексних систем захисту інформації

Змістовно, для будь-якого ОЗЗС, структура, яка ілюструє процедуру проектування, може бути представленою як на рис. 1.

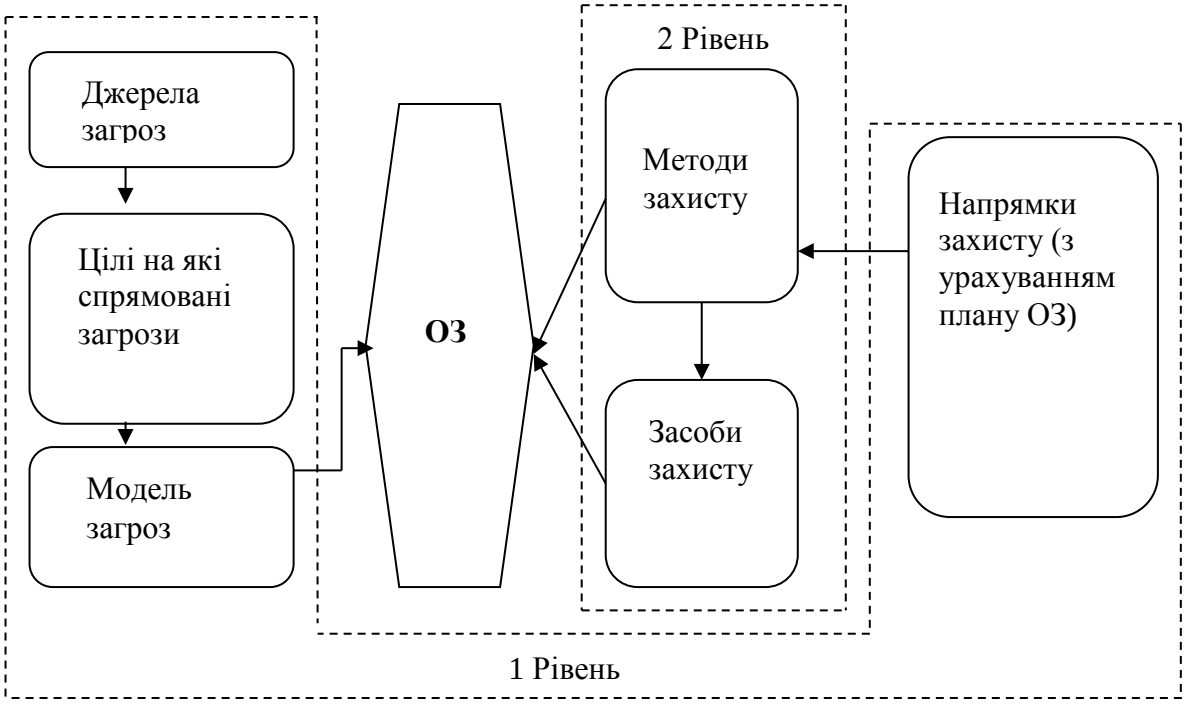

Рис. 1 – Варіант узагальненої структури проектування КСЗІ

Вхідним чинником для визначення структури КСЗІ є перелік I елементів $i \in I$, з яких складається об'єкт, що вимагає захисту, та стан S(I) множини цих елементів I, що визначаються на рівні «1» проектування згідно рис.1. Для створення переліку засобів та методів ЗІ (контрдій на рівні проектування «2» згідно рис. 1) є стан таких елементів $S(I_i)$, тобто i-й варіант переліку I, і відповідний перелік дестабілізуючих факторів (DF) для

кожного стану (тобто загроз). Саме ці два фрагменти послідовності проектування є такими, які не можуть бути жорстко алгоритмовані за рахунок введення переліку правил переходів від DF до загроз, та від загроз до засобів ЗІ, тобто вимагають використання підходів на засадах сітьового моделювання з використанням «пам'яті з адресацією за змістом запиту» . При цьому засоби захисту можуть розглядатися і як рішення про використання технічних пристроїв, і як рішення про використання такого методу захисту, для якого його технічна реалізація є однозначно регламентованою процедурою, тобто такою, що виконується згідно відомої діючої методики відомими засобами. Якщо означити перелік DF як $F=(\text{the list DF})$, тоді: $F=f(S(I))$, а перелік засобів та методів захисту для кожного окремого випадку ОЗЗС (підмножинаY_i) з загальної сукупності відомих методів та засобів (множина Y) використовує вибірку F в якості свого аргументу, тобто $Y_i = f(F_i(S(I)))$, де *i* є знаком приналежності до конкретного випадку ОІД чи ІТКС. З цього витікає, що процедура визначення переліку F_i та процедура визначення засобів та методів захисту Y_i є послідовністю двох процедур (два етапи проектування). На першому етапі визначається перелік загроз ОЗЗС, а на другому етапі здійснюється пошук технічних засобів та методів ЗІ. Різні автори по різному представляють поняття DF та поняття загроз, тобто, або ототожнюють їх, або розділяють. Якщо ототожнити DF та їх причини як загрози, тоді на їх основі можна визначати групи порушень, що можуть бути визначені з реалізацією загроз. Якщо розділити DF та їх причини, то тоді вводять поняття DF та джерел DF. При цьому частіше за все для ІТКС до причин DF відносять людський фактор (окремі особи, або групи осіб, які мають відношення до порушень захищеності інформації), технічні пристрої, математичне забезпечення (моделі, алгоритми, програми), технологію функціонування АС (рішення конкретних задач), зовнішнє середовище. До DF відносять можливий результат дії причин у вигляді кількісної недостатності, якісної недостатності, відмов, збоїв, помилок, стихійного лиха, зловмисних дій та побічних явищ. Але для ОЗЗС у вигляді ОІД такі визначення не є логічними. Тому єдність у підході до проектування вимагає визначення DF фактично як джерела DF, а загрозами будемо визнавати і DF і відповідне формулювання описів загроз, що не входять до DF. Тоді термінологія та змістовний сенс загроз та DF стає єдиним для будь-якої структур ОЗЗС, таких які наведені у табл. 1. Крім того, за такого підходу при створенні моделі проекту КСЗІ забезпечується єдність у описі DF та загроз і для структури системи захисту ОЗЗС технічними каналами і для структури системи захисту ОЗЗС від несанкціонованого доступу (НСД).

Таким чином, формується множина опису елементів ОІД ($i \in I$), їх стану S(*I*), переліку DF ($F=f(S(I))$) та рішень щодо засобів та методів захисту $Y_i = f(F_i(S(I)))$. Множину опису елементів ОІД можна характеризувати як декотрий образ об'єкта. Сукупність опису мають складати відповідні бази даних (БД).

Базис структур ОЗЗС та визначення засобів захисту

Кожний елемент ОІД представляється у вигляді відповідного образу (наприклад, переліку, або діаграми) його властивостей *i* з загальної множини образів елементів об'єкту I, $i \in I$. Змістовно кожна властивість *i* є визначенням (деяким текстом, фразою або декількома фразами), що описується розробником (випадок втручання оператора) як деякий елемент об'єкту. Кожна окрема фраза *i* має сенс одної з властивостей елементу об'єкту. Так, окремий комп'ютер має опис, що може складатися з таких фраз:

*i*1 – обчислювальна машина персональна; *i*2 – типом машини є машина загального користування (або серійна, або неспеціалізована, тощо); *i*3 – фірмою виготовлювачем є фірма IBM (або Siemens Nixdorf, або інша); *i*4 – призначенням є виготовлення документів з грифом ДСК (або таємно, або цілком таємно, тощо); *i*5 – місце розташування і.т.д.

Тоді набір таких *i*-фраз (або окремих слів) і є образом елемента (специфікація властивостей елемента) даного об'єкта. Фрази можуть формуватися довільно, або з деякої кінцевої бібліотеки (множини) фраз, тобто з бази даних БД описів елементів. У будь-якому випадку будемо вважати, що БД вміщує загалом I можливих фраз $i \in I$ (їх іноді називають реалізаціями фраз). Тоді відповідна сукупність таких реалізацій визначає стан відповідного елемента об'єкта $S(I_i)$ з усієї сукупності можливих станів $S(I)$ усіх можливих елементів (тобто: $S(I_i) \in S(I)$, що і є визначеним вище. Формально, така реалізація $S(I_i)$ також є образом стану.

На таких засадах види об'єктів захисту та базис структур ОЗЗС (за табл.1) можна представити у вигляді діаграм Ейлера-Вена (рис. 2 та 3 відповідно).

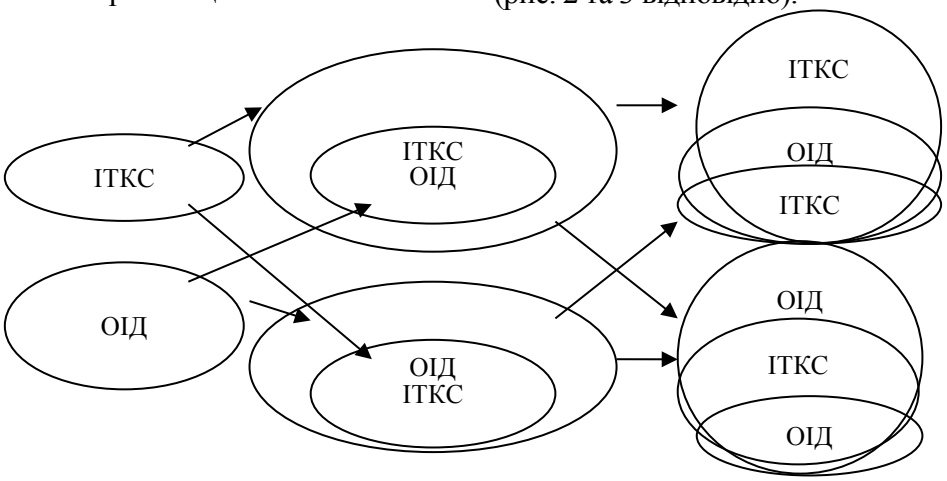

Рис. 2 – Види об'єктів захисту

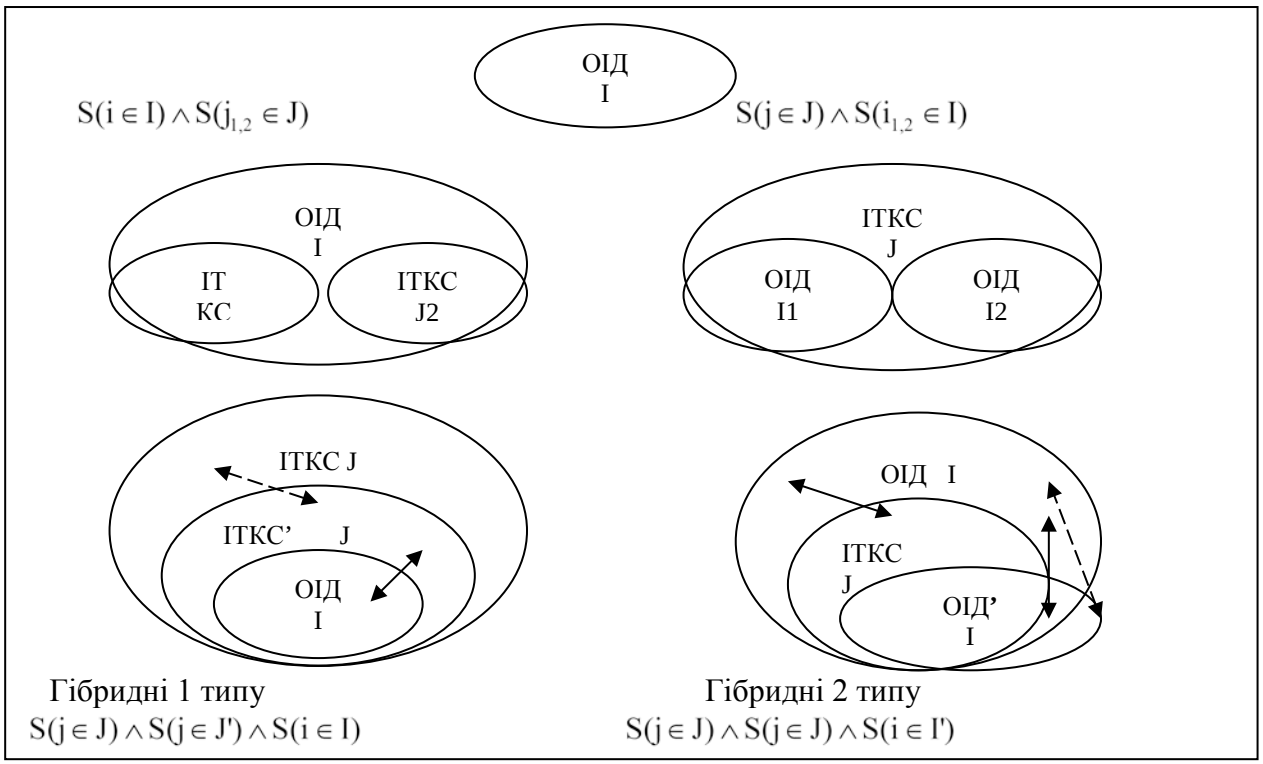

Рис. 3 – Базис структур ОЗЗС
$I_1, I_2, \ldots, I_N$ – образи елементів об'єктів захисту №№ 1, 2,…,N типу ОІД;
$J_1, J_2, \ldots, J_N$ - образи елементів об'єктів захисту №№ 1, 2,…,N типу ІТКС.

Якщо БД DF створювати аналогічним чином, то тоді перелік *F* (тобто – специфікація або образ як сенсовий зміст специфікації) тих DF, які відносяться до даного елемента даного об'єкту і отримані в результаті «спеціального обстеження» дослідником – розробником (випадок втручання оператора) загалом є вибіркою, що залежить (є деякою функцією) від стану S елемента *I* , тобто $F=f(S(I))$.

Сенсовий зміст F є функцією зв'язку між станом елементу об'єкту та отриманою специфікацією DF_i з сукупності можливих специфікацій DF $(DF_i \in DF)$. Специфікацію DF (образ DF_i для даного *i*-го елемента) логічно позначати F_i. Тоді, за визначенням формальних зв'язків, загрозою Y для даного *i*-го елемента є образ Y_i, котрий визначається як вплив $DF_i \in DF$ на стан S(*I*). Логічний зв'язок між образом загрози та образом стану з відповідними DF може бути представлений як: $Y_i=f(DF_i \wedge S(i \in I))$, де: - символ $\wedge$ є кон'юнктивною функцією (поєднання множин); функція f є функцією зв'язку між сенсовим змістом стану елемента та впливом DF на нього.

Можливим є представлення множин елементів що відтворюють зазначені образи, у вигляді діаграм Ейлера-Вена (рис. 4 та 5).

Рис. 4 – Представлення окремих образів *I,* DF та S

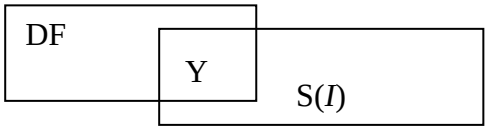

Рис. 5 – Представлення образу загроз Y

Специфікація загроз, які створюють образ загроз, є вихідними даними для подальшого визначення засобів ЗІ, що складають результуючу мету проектування.

Образ загроз Y визначає напрямки захисту, але для визначення засобів захисту необхідно спиратися на можливості протидії загрозам, а саме на БД можливих засобів захисту, що складають образ БД. Позначимо БД можливих засобів захисту образом Z. Таким чином, виділення з БД засобів захисту (множини засобів) тієї частини засобів, котра є необхідною для обслуговування поточного ОЗЗС, становить завдання визначення відповідної підмножини $Z_i \in Z$. Підмножина Z_i є образом засобів захисту поточного ОЗЗС. Відповідним образом загроз поточного ОЗЗС є підмножина $Y_i \in Y$.

Множина засобів захисту як образ Z складається з чотирьох кластерів (образів підмножин) засобів, до яких можуть відноситися активні засоби захисту $Z(A_i)$, пасивні засоби захисту $Z(P_i)$, заборони (обмеження) у використанні тих чи інших засобів (у найбільшій мірі – активних) $Z(N_i)$, криптографічні засоби $Z(K_i)$, яке представлено на рис. 6.

Тобто образ усіх можливих засобів Z складається з чотирьох образів Z(A,P,N,K). Початковими умовами використання засобів захисту при проектуванні Z(A,P,N,K є образ усіх можливих засобів, а кінцевим результатом проектування є відповідний до поточного ОЗЗС образ засобів $Z(A_i,P_i,N_i,K_i)$. Символ *i* означає відповідність образів засобів захисту до образу загроз $Z_4(A_i) \in Z(A)$ $Y_i \in Y$ поточного ОЗЗС.

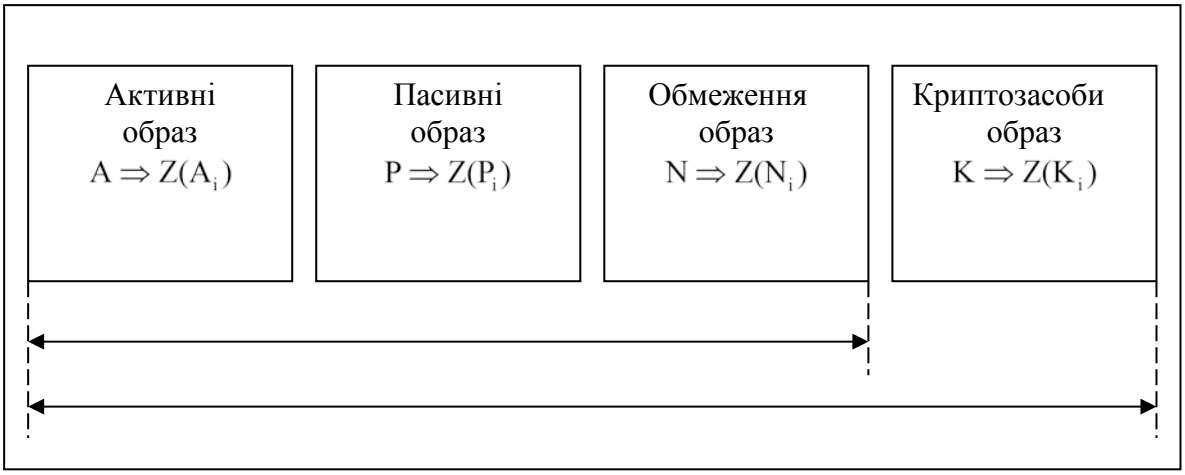

Рис. 6 – Кластери засобів захисту ОЗЗС

Розглядаючи процедуру визначення засобів захисту як пошукову процедуру в термінології кінцевих автоматів FSM (FSM – Finite State Machines), визначимо початковий стан образом $Y_i \in Y$, кінцевий стан – образом $Z(A_i,P_i,N_i,K_i)$, а інструментом переходу з початкового до кінцевого стану є алгоритм роботи АП як предикат АП. Необхідно визначити умови, за якими можливою є процедура переходу від початкового до кінцевого стану, тобто існування квантора:

$$\forall(Y_i \in Y)\ \exists\ (Z(A_i,P_i,N_i,K_i))=\text{TRUE}$$

Для цього розглянемо варіанти можливих образів підмножин засобів захисту для ОЗЗС довільної архітектури.

$$(Y_i \in Y) \rightarrow Z(A,P,N,K) = \begin{cases} Z(P) \leftrightarrow \neg Z(A) \wedge \neg Z(K) & (1) \\ Z_1(A_j) \in Z(A) \leftrightarrow \neg Z(N) \wedge \neg Z(K) \wedge \left[Z(P) \vee \left(Z(P_j) \notin Z(P) \right) \right] & (2) \\ Z_2(A_i) \in Z(A) \leftrightarrow \neg Z(N) \wedge \neg Z(K) \wedge Z(P) & (3) \\ Z_3(A_i) \in Z(A) \leftrightarrow \neg Z(N) \wedge Z(P) \wedge Z(K) & (4) \\ Z_4(A_i) \in Z(K) \leftrightarrow \neg Z(N) \wedge \neg Z(P) & (5) \\ Z(P) \leftrightarrow \neg Z(A) \wedge Z(K) & (6) \\ Z(K) \leftrightarrow \neg Z(A) \wedge \neg Z(P) & (7) \end{cases}$$

Тут символ j підкреслює приналежність тільки до тієї частини j-х активних засобів, які дозволяють компенсувати недостатність пасивних засобів $Z(P_j) \notin Z(P)$. Цим виразом виділення образу Z(A,P,N,K) як події, котра відбулася в результаті події, що створила стан ($Y_i \in Y$), підкреслюється, що образи загроз є аргументом майбутньої появи образу засобів захисту Z(A,P,N,K).

Наведені вирази (1) – (7) мають відповідні відображення у вигляді діаграм Ейлера-Вена, наведені для поточного ОЗЗС за рис.7.

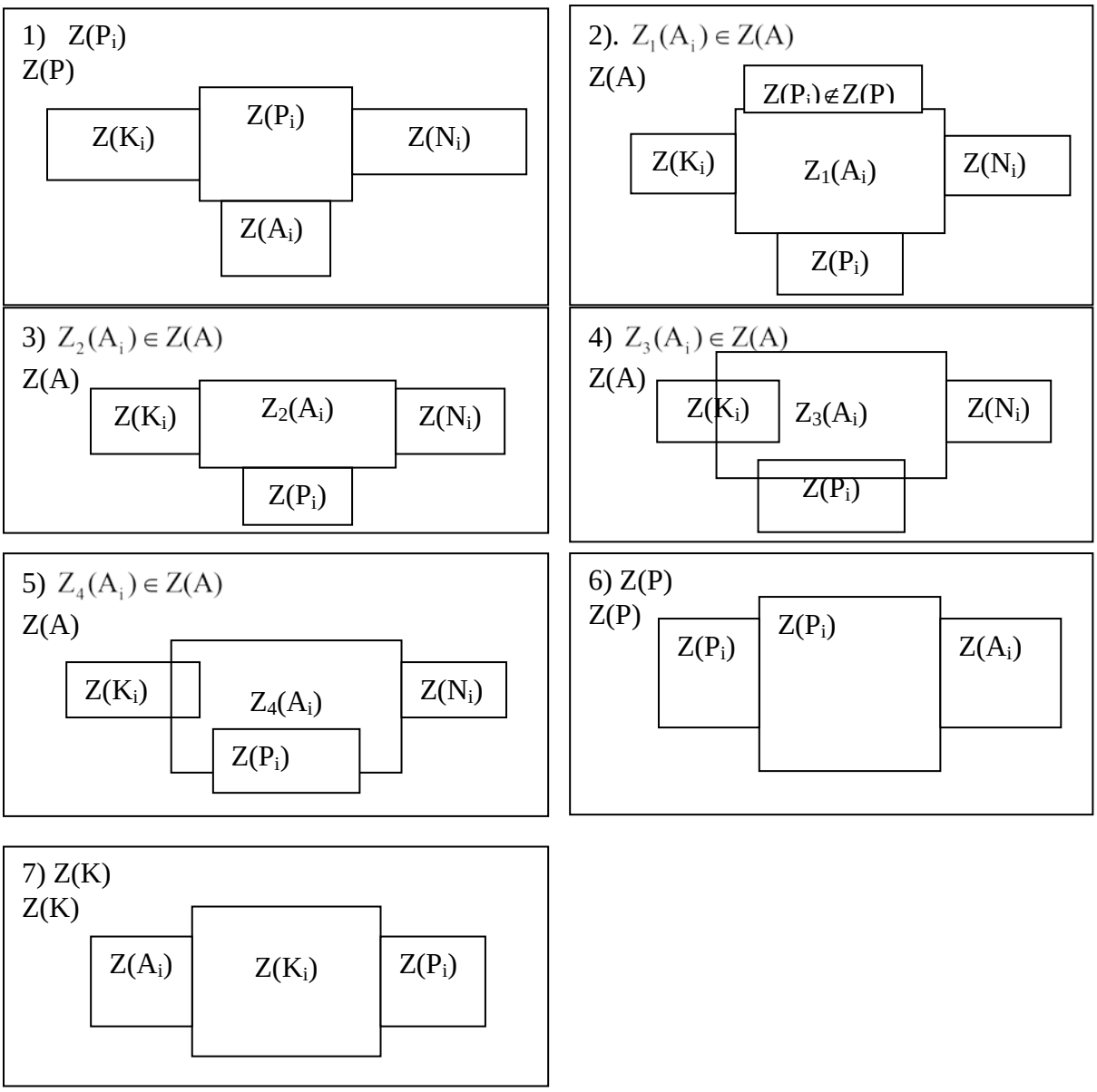

Рис. 7 – Діаграми Ейлера-Вена за виразами (1) – (7)

Вирази (1) – (7) мають сукупний сенс при умові введення деяких заборон та обмежень, наведених в табл. 3. Тобто при умові, коли заборони та обмеження N є апріорно визначеними для будь-якого об'єкту у вигляді кінцевої специфікації і з аргументу Z переводиться до параметру {Z(A,P,K),N=const}.

Таблиця 3.

Заборони та обмеження щодо використання активних засобів

1. Активні засоби Z(A) використовуються тільки при доведеній неможливості використання пасивних засобів Z(P), або коли вже залучені пасивні засоби Z(P) об'єктивно не здатні забезпечити необхідний заданий результат захисту, що може ілюструватися загальним виразом $Y_i \in Y$. За такої умови *i* наведений вираз $Z(P_j) \notin Z(P)$, а символ *j* підкреслює, що вибірка Y_i з символом *i* не має відношення до формування такої забороненої вибірки $Z(P_j)$. Тоді стає зрозумілим, що номери 1,2,3 та 4 у визначенні $Z_1(A_j)$, $Z_2(A_j)$, $Z_3(A_j)$ та $Z_4(A_j)$ відповідно, означають випадки:
а) Z_1 – випадок, коли активні засоби використовуються без пасивних засобів (або визначені

пасивні не забезпечили необхідний результат) та без криптометодів. б) Z_2 – випадок, коли активні засоби застосовуються разом з пасивними засобами при відсутності криптометодів та відсутності заборон на активні засоби. в) Z_3 – випадок використання активних разом з пасивними засобами та криптографічними. г) Z_4 – випадок, коли активні засоби суміщені виключно з криптографічними.
2. Заборони та обмеження Z(N) поширюються тільки на активні методи захисту. Загалом, активні методи захисту мають наступні недоліки: а) використання активних методів захисту приводить до нездоланних демаскуючих признаків об'єкту. б) наявність засобів активного захисту порушують електромагнітну сумісність наявних на об'єкті технічних засобів. в) за умов використання багатоканальних засобів перехоплення та довготривалому накопиченні інформації що перехоплюється засобами розвідки зберігається можливість виділення інформативних компонентів з сигналів що захищаються і вірогідність позитивних або негативних наслідків атаки не є визначеною. г) за умови використання активного захисту для захисту оточуючого простору радіоканалом медичні показники присутності є негативними. д) у присутності криптозахисту зашумлення радіоефіру не має сенсу.
3. Забезпечення необхідної та достатньої величини ентропійного коефіцієнту якості шуму, який утворюють активні засоби захисту, вимагає достовірної доведеності.

Зазначені недоліки та обмеження активного захисту, наведені в пункті 2 табл. 3, повністю підтверджують змістовність обмежень, наведених у пункті 1 табл. 3.

До пасивних засобів захисту тут відносяться засоби захисту від витоку каналами ПЕМВН та акустичними каналами, а також заходи та засоби захисту від НСД до носіїв інформації. Поєднання Z(P) з захистом від НСД не створює протиріч з загальною методологією ТЗІ.

Якщо розглянути п'ять типів структур ОІД, наведених у Таблиці 1, то тоді застосування виразів (1) – (7) до кожної з них дозволяє систематизувати образи засобів захисту для різних структур ОЗ:

1. Для структури 1 згідно таблиці 1 з загалу виразів (1) – (7) виділяються пасивні засоби та пасивні засоби у присутності дозволених активних засобів типу Z_2.

$$Z(A_i,P_i,N_i,K_i)=\begin{cases} Z(P) \leftrightarrow \neg Z(A) \wedge \neg Z(K), \\ Z_2(A_j) \in Z(A) \leftrightarrow \neg Z(N) \wedge \neg Z(K) \wedge Z(P). \end{cases}$$

Можливим є поєднання цих двох виразів за формулою логічних зв'язків:

$$Z(A,P,N,K)=Z(P) \vee \{Z(P) \wedge [Z_2(A_i) \wedge \neg Z(N)]\}.$$

2. Для структури 2 згідно табл. 1 можливим є використання дозволених активних типу Z_2 засобів у присутності пасивних або пасивні засоби та засоби криптографічного захисту.

$$Z(A,P,N,K) = Z(P)\ [\ Z2(Ai)\quad Z(K)],$$

або:

$$Z(A,P,N,K) = Z(P) \wedge [Z_2(A_i) \vee Z(K)].$$

3. Для структури 3 згідно табл. 1 можливим є використання пасивних методів захисту, поєднаних з криптографічними та дозволених активних типу Z_2 у присутності пасивних методів:

$$Z(A_i,P_i,N_i,K_i) = \begin{cases} Z(P) \leftrightarrow \neg Z(A) \wedge Z(K), \\ Z_2(A_j) \in Z(A) \leftrightarrow \neg Z(N) \wedge \neg\ Z(K) \wedge Z(P). \end{cases}$$

4. Для структури 4 згідно табл. 1 можливим є використання пасивних методів захисту, поєднаних з криптографічними, та дозволених активних типу Z_2 у присутності пасивних

методів. А це співпадає з використанням методів захисту для 3 структури.

5. Для структури 5 згідно таблиці 1 можливими є два варіанти. Якщо ОІД' не має загального призначення з головним ОІД, тоді він не має загального призначення і з ІТКС. Тобто ОІД є окремим об'єктом захисту і для нього можливим є використання методів захисту зазначених для 1 структури. Якщо ж ОІД', входячи до складу ІТКС, має загальне призначення з головним ОІД, то тоді призначення ОІД' співпадає з призначенням ІТКС і для нього можливим є використання методів захисту, зазначених для 3 структури.

Оскільки $Z(A_i,P_i,N_i,K_i)$ для структури 3 як виявляється є комбінацією засобів, що використовуються в якості засобів захисту для структур 1 та 2, то загальний вираз логічних зв'язків для сукупності розглянутих структур має вигляд:

$$Z(A,P,N,K) = Z(P) \wedge [Z(K) \vee Z_2(A_i)] \leftrightarrow \min[Z(P), Z(K) \vee Z_2(A_i)] . \quad (8)$$

Можливість зведення (1) – (7) до лаконічного виду (8) має логічне обґрунтування. Дійсно, оскільки активні методи мають обмеження за пунктом 1 таблиці 3, то тоді засоби, зазначені формулами (2), (4) та (5), можуть не використовуватися. Відсутність (7) логічно пояснюється тим, що виключно криптографічний метод захисту ОІД в рамках розробки КСЗІ не має сенсу з причини відсутності логіки для випадку, коли інформаційний потік захищається, а носій інформації відсутній. Теоретично існують два випадки, коли можливим є використання виключно криптографічного методу захисту. Ще один випадок, це використання окремого пристрою (чи абонентського комплекту) захисту *мовної* інформації, такого, як маскіратор, скремблер, вокодер або ліпредер у телефонних каналах зв'язку, або при використанні приймально-передавальної апаратури (рації) у радіоканалі сумісно з зазначеними пристроями. Іншим випадком є використання пристроїв спеціального зв'язку при виконанні тактичних операцій підрозділами спеціального призначення. В обох випадках ніякої мови про КСЗІ не йдеться по причині фактичної відсутності об'єкту захисту, або ІТКС.

Висновки

Права частина виразу (8) $\min[Z(P),Z(K) \vee Z_2(A_i)]$ змістовно означає, що при виконанні 4-х умов, а саме:

1. коли об'єкти захисту представити згідно структурам ОЗЗС;

2. структури ОЗЗС класифікувати за типами згідно табл. 1;

3. при умові використання засобів захисту на засадах обмежень та заборон згідно табл. 3;

4. на трьох наступних етапах проектування:

- *визначення загроз та контрдій;*
- *визначення зв'язку між складовими переліку порушень та кожною складовою КСЗІ;*
- *при процедурі визначення технічних засобів захисту за напрямками захисту.*

Необхідно використовувати саме пам'ять з адресацією за змістом запиту у якості БД DF, БД порушень та БД методів та засобів захисту. Тоді за результатом проектування має бути прийнятим рішення щодо використання методів та засобів захисту у їх мінімальному об'ємі. Це автоматично мінімізує і фінансове навантаження на систему захисту в цілому.

Наявність єдиного рішення за виразом (8) свідчить також про те, що при проектуванні за зазначеною логікою доцільно вважати доведеним унеможливлення ситуації, коли однакові, або майже однакові об'єкти, отримують зовсім різні рішення щодо їх КСЗІ.

Таким чином предикат (8) є достатнім єдиним виразом, котрий описує логіку вибору при комплектуванні системи захисту будь-якого ОЗЗС. Враховуючи вираз (8) можна вважати, що алгоритм формування БД DF, БД загроз, БД засобів захисту та зв'язків між ними з логікою роботи є таким, який повинен та може привести до прийняття єдиного для кожного окремого ОЗЗС рішення. Причому сам вираз (8) не є описом послідовності дій, за якою визначається процес моделювання.

Доведеність дійсності предикату (8) означає, що для будь якого реального об'єкту (тобто такого, для якого виконуються обмеження згідно табл. 3) існує тільки одне рішення у виборі методів та засобів захисту, котре об'єктивно має логічний сенс, має властивість достатності обраних методів та засобів захисту для вирішення задачі захисту та не включає у свій склад зайвих, повторюваних елементів захисту. Тобто для таких об'єктів існує рішення з ознаками об'єктивності. У це і вкладається сенс достовірності та оптимальності рішень при проектуванні.

Перелік посилань

[1] BS 7799:1995 – *Code of practice for information Security Management BS 7799.* http://bezpeka.ladimir.kiev.ua/pg/show/risks/page2.html.

[2] ГОСТ Р ИСО/МЭК 17799-2005 *«Информационная технология. Практические правила управления информационной безопасностью»*.

[3] В. М. Луценко, *Комплексні системи захисту інформації довільної складності* / Луценко Володимир Миколайович // «Захист інформації». наук. тех. журнал. К.: – 2012. - НАУ, №2 (55). - с. 15-18.

[4] В. М. Луценко, *Відповідність етапів побудови систем захисту інформації стадіям створення автоматизованих систем* / Луценко Володимир Миколайович // «Захист інформації». Наук. тех. журнал. – К.: - 2011. НАУ, №3 (52). - с.52-56.

References

[1] BS 7799:1995 – *Code of practice for information Security Management BS 7799.* http://bezpeka.ladimir.kiev.ua/pg/show/risks/page2.html.

[2] HOST R YSO/МЭК 17799-2005 *«Ynformatsyonnaia tekhnolohyia. Praktycheskye pravyla upravlenyia ynformatsyonnoi bezopasnostiu»*.

[3] V. M. Lutsenko, *Kompleksni systemy zakhystu informatsii dovilnoi skladnosti* / Lutsenko Volodymyr Mykolaiovych // «Zakhyst informatsii». nauk. tekh. zhurnal. K.: – 2012. - NAU, №2 (55). - s. 15-18.

[4] V. M. Lutsenko, *Vidpovidnist etapiv pobudovy system zakhystu informatsii stadiiam stvorennia avtomatyzovanykh system* / Lutsenko Volodymyr Mykolaiovych // «Zakhyst informatsii». Nauk. tekh. zhurnal. – K.: - 2011. NAU, №3 (52). - s.52-56.

Реферат

Луценко Володимир

Можливість автоматизації проектування КСЗІ

Аналізується можливість та особливості автоматизації проектування комплексних систем захисту інформації. Враховуючи складності, які виникають при автоматизації такого проектування, виникає питання про можливість автоматичного проектування, за умов єдності прийняття рішень проектантом, доказової однозначності (об'єктивності таких рішень), мінімізації фінансового навантаження на результат проектування, тобто, на спроектовану систему захисту за умови достатності рівня захищеності об'єкту захисту. Для вирішення такого питання наведений підхід, що дозволяє формалізувати опис будь-якого об'єкту захисту мовою теорії нечітких множин. Наведений формальний опис об'єктів захисту довільної складності. Для цього вперше введеним э поняття об'єкту захисту загальної структури. Опис можливих структур системи захисту довільних об'єктів здійснено мовою предикатів. За цей рахунок доведено, що при проектуванні систем захисту інформації за визначеною методикою для будь-якого реального об'єкту існує тільки одне рішення у виборі методів та засобів захисту, котре об'єктивно має логічний сенс, має властивість достатності обраних методів та засобів захисту для вирішення задачі захисту та не включає у свій склад зайвих, повторюваних елементів захисту. Тобто для таких об'єктів існує рішення з ознаками об'єктивності при умові мінімізації фінансового навантаження на результат проектування.

Луценко Владимир

Возможность автоматизации проектирования КСЗИ

Анализируется возможность и особенности автоматизации проектирования комплексных систем защиты информации. Учитывая сложности, которые возникают при автоматизации такого проектирования, возникает вопрос о возможности автоматического проектирования при условии единства принятия решений проектантов, доказательной однозначности (объективности принятия решений), минимизации финансовой нагрузки на результата проектирования, т.е. на спроектированную систему защиты при условии уровня защищенности объекта защиты. Для решения такой задачи приведен подход, позволяющий формализовать описание произвольного объекта защиты языком нечетких множеств. Приведено формальное описание объектов защиты любой сложности. Для этого впервые введено понятье объекта защиты общей структуры. Описание возможных структур системы защиты произвольных объектов приведено языком предикатов. За счет этого доказано, что при проектировании систем защиты информации по определенной методике для любого реального объекта существует только одно решение при выборе методов и средств защиты, которое имеет объективный логический смысл, обладает свойством достоверности в выборе методов и средств защиты и обеспечивает достаточность средств защиты в своем составе. Это означает, что для таких объектов существует решение с признаками объективности при условии минимизации финансовой нагрузки на результат проектирования.

Lutsenko Volodymir

Opportunity of automation of designing of CSPI

The opportunity and features of automation of designing of complex systems of protection of the information is analyzed. Taking into account complexities which arise at automation of such designing, there is a question on an opportunity of automatic designing under condition of unity of acceptance of decisions designers, demonstrative unambiguity (objectivity of acceptance of decisions), minimization of financial loading on result of designing, i.e. on the designed system of protection under condition of a level of security of object of protection. For the decision of such task the approach is given, allowing to formalize the description of any object of protection by language of indistinct sets. The formal description of objects of protection of any complexity is given. For this purpose the concept of object of protection of the general structure for the first time is entered. The description of possible structures of system of protection of any objects is given by language of predicates. Due to it is proved, that at designing systems of protection of the information by the certain technique for any real object there is only one decision at a choice of methods and means of protection which has objective logic sense, has property of reliability in a choice of methods and means of protection and provides sufficiency of means of protection in the structure. It means, that for such objects there is a decision with attributes of objectivity under condition of minimization of financial loading on result of designing.

Відомості про автора

Луценко Володимир Миколайович

Освіта: Вища, інженер Радіотехнік (1980).

Науковий ступінь: Кандидат технічних наук (1989).

Вчене звання: Доцент, старший науковий співробітник Національної академії наук України.

Місце роботи: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Область знань: Інформаційна безпека, кібернетика та інформаційні технології, фізика.

Наукові інтереси: Інформаційна безпека, штучний Інтелект, квантові комунікації.

Email: *lutsenkovn@ukr.net*