УДК 681.3.06:519.248.681

В.М. Луценко

СИСТЕМА ІНТЕЛЕКТУАЛЬНОЇ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПРИ ПРОЕКТУВАННІ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Вступ

Методологія створення комплексних систем захисту інформації (КСЗІ) [1, 2] є напрямком, який на сьогодні перебуває в стані розвитку. Це визначає фактичну недосконаліть методологій проектування, а тому і невпорядкованість проектів діючих об'єктів інформаційної діяльності з погляду на об'єктивну єдність підходів до створення систем захисту інформації. Так, структурно та інформаційно однакові об'єкти можуть бути захищеними за допомогою використання різних систем захисту, причому різниця буває принциповою. Інакше кажучи, скільки виконавців проекту – стільки й варіантів рішень із проектування.

Згідно з підходом щодо порядку проведення робіт з технічного захисту інформації (ТЗІ) [2], такий захист реалізується на базі фрагментарного або комплексного підходу, причому різниця між ними є нечітко визначеною. Загалом при цьому немає значення, чи створюється проект у ручному режимі, чи за допомогою системи автоматизованого проектування (САПР), оскільки результат напрацювань САПР однозначно залежить від сформованих суб'єктом – проектантом даних. При використанні автоматизованого проектування краще вирішуються завдання підвищення ергономічності і зменшення витрат процесу створення проекту і, меншою мірою, завдання щодо об'єктивності та оптимізації прийнятих рішень.

Сказане вище є приводом для пошуку шляхів до загального підходу і надалі методології вирішення завдання кваліфікованого об'єктивного рішення щодо проектування КСЗІ на принципах уніфікації і автоматизації процесу проектування складних систем при неповних або суперечливих вхідних даних. Наприклад, до розробки залучаються онтологічні моделі властивостей зрілості процесів захисту інформації [3], що дає можливість вирішити завдання стратегічного планування складних процесів і технологій при вилученні з результату проектування вербальності та інтуїтивності рішень, що отримуються. Кінцевою метою при цьому є створення методології проектування, близької до універсальної, при якій процес захисту інформації здатний досягти запланованої мети та результатів відповідно саме до його призначення. Безумовно, такий підхід сприяє зробити крок вперед до створення системи проектування КСЗІ. Однак при цьому підході не враховується динаміка в часі ситуації щодо загроз для об'єкта, а врахування результатів аудиту безпеки в кожний момент часу є можливим тільки за рахунок перепроектування системи захисту об'єкта. Причиною цього є те, що із врахуванням таксономії [3] властивості вдосконалення захисту модель захисту може вдосконалюватись при зміні зовнішніх факторів, але при цьому не береться до уваги історія об'єкта при аналізі його поточного стану. Також при визначенні зрілості процесу створення системи захисту відсутня чітко визначена повторюваність прийнятих рішень різними виконавцями на основі попереднього досвіду з проектування КСЗІ.

Інший підхід базується на еволюційній архітектурі системи захисту інформації [4]. Його основано на поданні методу створення опису об'єкта захисту та моделі управління подіями (поточна поведінка в загальній послідовності) у вигляді деякого образу – Statechart. Набір моделей можливих поведінок (бібліотека можливих образів поведінки) подано також у вигляді образів поведінки – Viewchart. При цьому образи Viewcharts основані на Statecharts та одночасно розвивають їх. Створення опису об'єктів здійснюється через використання набору інструментів – Statemate. Таким чином, Statechart визначає, чим був об'єкт і яким він буде. Viewchart фактично є набором зображень даних (образів) із врахуванням тенденції щодо послідовності станів об'єкта. Канонічно, образами є гістограми станів чи в часовій послідовності, чи в послідовності можливих станів, які можуть створюватися або одночасно, або в часовій послідовності. При такому підході створення методології проектування зводиться до створення формалізованих, тобто математичних, інструментів (Statemate) для використання як функцій зв'язку між можливими та наявними Statecharts.

Такий підхід до створення моделей захисту дуже перспективний, але якісні показники проекту захисту, створеного на зазначених засадах, при цьому є невизначеними і проект захисту таким чином не являє собою кінцевий технологічний

продукт, а є лише одним із можливих варіантів кінцевого технологічного продукту. На таких засадах нема мови про об'єктивність рішень при проектуванні або про оптимізацію проекту щодо будь-якого параметра проектування.

Для створення об'єктивно оптимальної і статистично єдиноподібної системи проектування КСЗІ необхідно визначити перелік властивостей засобу проектування, здатного до вирішення такого завдання.

Постановка задачі

Метою статті є створення системи проектування КСЗІ із застосуванням методів і засобів створення систем підтримки прийняття рішень.

Огляд існуючих рішень систем автоматизації проектування для вирішення завдань захисту інформації

Об'єктом дослідження є система автоматизації проектування КСЗІ.

Предметом дослідження є система інтелектуальної підтримки прийняття рішень для проектування КСЗІ.

Якщо в галузях правових норм, нормативної бази і методичного забезпечення (навіть із врахуванням їх недоліків) особливих проблем немає, то в галузі ТЗІ і в тому числі його кінцевому пункті – створенні якісної моделі загроз та проектуванні систем захисту – спостерігається істотна недосконаліть. Загалом це пов'язано з об'єктивним відставанням розвитку в часі даного напрямку, який залишився в ринковій економіці України від попередніх часів, коли рішення із забезпечення безпеки інформації приймалися переважно за рахунок організаційних методів захисту. В таких умовах можливими є два шляхи виходу з технологічної кризи. Одним із них є намагання підвищити якість робіт у галузі інформаційної безпеки за допомогою використання досвіду більш розвинутих країн. Але на цьому шляху є серйозні перешкоди. Перша з них полягає в тому, що діюча в Україні регіональна і об'єктова інфраструктура не є досконало адаптованою до інформаційної інфраструктури, як це спостерігається на Заході, де така адаптація створювалася десятиліттями в рамках державних програм. Характер взаємодії цих інфраструктур постійно змінюється, що загалом може поглиблювати їх антагонізм. Друга перешкода полягає в тому, що намагання "наздогнати і перегнати" вимагає великих фінансових витрат, а особливо при наявності дієвої і масштабної програми.

Другий шлях виходу з технологічної кризи полягає в пошуку нового радикального рішення. Він за якісними показниками має забезпечити необхідний рівень проектування незалежно від специфіки ОІД, тобто від умов створення і використання проектів. При цьому найвищого ступеня досконалості можна досягти, якщо розглядати створення системи захисту об'єктів комплексно, тобто об'єднавши в єдиний процес етапи обстеження та опису об'єкта, проектування зрілої та фінансово оптимізованої системи захисту, післяпроектний аудит безпеки об'єкта. Розглядаючи такі етапи окремо, сучасні автори намагаються істотно вдосконалювати їх.

Таким чином, постає запитання, чи можуть бути базою до створення системи проектування КСЗІ продукти фірм-розробників систем аналізу і керування ризиками? Огляд такого підходу визначає, що методи аналізу й керування ризиками відрізняються великим різноманіттям. До найбільш поширених можна віднести [5–9]:

- метод CRAMM (the UK Government Risk Analysis and Management Method, Велика Британія, 1985 р.), який є універсальним інструментом, призначеним для обстеження інформаційної системи (ІС), аналізу ризиків, проведення аудиту на відповідність вимогам *Британського* уряду та стандарту BS 7799:1995 – Code of practice for information Security Management BS 7799, розробку політики безпеки і плану забезпечення безперервності бізнесу;
- метод Cobra (Consultative Objective and Bi-Functional Risk Analysis), який є засобом аналізу ризиків й оцінки відповідності інформаційної системи стандарту ISO 17799. Оцінка ризиків здійснюється кількісно. Метод реалізує інструменти для консалтингу і проведення оглядів безпеки, використовуючи велику кількість опитуючих, що призводить до суб'єктивності рішень, особливо якщо статистика опитувань є недостатньою, а визначення ступеня достатності є питанням складним і неоднозначним;
- метод RiskWatch (Америка), який реалізований у вигляді програмного продукту і є засобом аналізу та керування ризиками. Він використовує різні види аудиту безпеки, вибір яких відданий на розгляд користувачу;
- метод Buddy System компанії "Consultation Objective and Bi-Functional Risk Analysis", який є програмним продуктом, що реалізує як кількісний, так і якісний аналізи ризиків. Він

має розвинені засоби генерації звітів. Тут особлива увага приділяється ризикам, пов'язаним із порушеннями фізичної безпеки, а також керуванням проектів.

Якщо розглядати названі реалізації методів аналізу, то необхідно визначити ступінь адаптованості цих реалізацій до українських користувачів. При цьому слід враховувати особливості законодавства і стандартів України, особливості відношень між організаціями-користувачами в рамках діючої інфраструктури, місцеві і регіональні особливості в створенні структури ІС, вимоги до робочої та звітної документації і традиції. З такої точки зору найбільш близьким до вітчизняних вимог, мабуть, є продукт Buddy System.

Результатом аудиту все частіше стає сертифікат на відповідність обстежуваної ІС вимогам міжнародних стандартів. Це забезпечує конкурентні переваги, пов'язані з більшою довірою з боку клієнтів. При цьому стандарти ISO 17799 і ISO 15408 є основою для проведення будь-яких робіт у сфері інформаційної безпеки й аудиту. Німецький стандарт BSIMT є найбільш змістовним довідником із забезпечення безпеки ІТ.

Як видно, проблемою для нас є відсутність єдиного ДСТУ, який мав би повну адаптованість до місцевих умов роботи об'єктів, до законодавства України. Тому аудит безпеки досі є завданням, що перебуває на етапі розробки і використання продуктів, якими реалізуються названі методи, слабко адаптовані до створення проектів захисту, а направлені більше на аналіз існуючих проектів.

Стосовно діючих САПР і систем прийняття рішень у сфері інформаційної безпеки, то широко відомі лише САПР "Кондор", "Авангард" та "Гриф". Ці продукти в повній відповідності до сказаного призначені лише для аналізу загроз та аудиту безпеки діючих проектів. Таким чином, дефіцит САПР КСЗІ залишається нагальною проблемою галузі інформаційної безпеки на Україні.

Створення системи інтелектуальної підтримки прийняття рішень для проектування комплексних систем захисту інформації

Визначення необхідних властивостей засобів проектування КСЗІ. Якщо поставити завдання створення системи проектування з підвищеним ступенем об'єктивності прийняття рішень, то тоді така система повинна мати властивості обох зазначених вище систем при умові відсутності наведених недоліків. Перелік необхідних властивостей можна сформулювати таким чином:

1) система має створюватись на базі принципово об'єктивного проектування незалежного від вподобань і кваліфікаційних властивостей авторів проектів;

2) система захисту є динамічною в часі і відкритою до можливості змін складових бібліотек методів та засобів захисту або умов життєдіяльності об'єкта, при цьому постійно враховується його історія;

3) проект системи має вважатися завершеним за умови, якщо у визначений термін часу повторне незалежне проектування дає однаковий результат. При цьому під визначеним терміном часу слід вважати настільки малий термін, по закінченні якого властивості об'єкта не змінюються.

Якщо розглядати наведені вимоги щодо методології моделювання складних процесів, то можна побачити, що система моделювання фактично має властивості системи інтелектуальної підтримки прийняття рішень при неповних або суперечливих даних. Результат її роботи – знаходження оптимальних рішень для складних процесів. Найважливішим для досягнення реальної працездатності системи при цьому є розв'язання задачі визначення ступеня близькості результату моделювання до оптимального рішення.

Створенню такої системи проектування присвячена дана стаття.

Вибір засобу моделювання. Системи з наведеними властивостями відомі з напрямку моделювання елементів штучного інтелекту [10–12]. В таких системах можуть використовуватися як перцептронні [13], так і сітьові моделі [12, 14].

До особливості перцептронів при їх використанні як асоціативної пам'яті (АП) можна віднести те, що при нарощуванні рівнів перцептрона можливі випадки зменшення ступеня оптимізації рішень відносно інваріантів. А в нашому випадку саме і передбачається використання моделей об'єктів великого розміру з великою кількістю елементів та параметрів, тобто необхідною є багаторівнева модель перцептрона.

Під сітьовими моделями розуміють ансамблеві асоціативно-проективні сіті. На їх основі будуються асоціативна пам'ять різного призначення, бази даних, експертні системи, системи прийняття рішень, системи інтелектуальної підтримки, впізнавання образів тощо. Базовою складовою функцією таких моделей є викорис-

тання АП, яка дає можливість знаходити рішення, близьке до оптимального або таке, яке задане згідно із заздалегідь створеною бібліотекою можливих рішень. Такі рішення у визначених випадках називаються інваріантами, а створення інваріантів, основане на процедурі навчання моделі, вважається інваріантним.

Сітьові ансамблеві моделі як АП відповідають названим вище властивостям системи проектування. Вони "терплячі" до помилок, реалізуються у великому розмірі (причому чим більший розмір, тим краще працюють), при кожному додатковому навчанні враховують попередній досвід і ефективно розв'язують задачі оптимізації рішень [15].

Структура системи автоматизованого проектування КСЗІ. Захист інформації – процес динамічний [16]. Таким чином, проектувати (розробляти заново чи в більшості випадків модифікувати діючу) КСЗІ необхідно для конкретного моменту часу. Виключити таку необхідність або автоматизувати процес модифікації чи первинного проектування і є нагальним завданням, на вирішення якого направлена дана стаття. При цьому сама структура системи автоматичного проектування може бути різною, наприклад такою, яка розробляється на кафедрі "Комп'ютерні технології і системи" у Брянському державному технічному університеті [17]. Схему такої САПР КСЗІ зображено на рис. 1.

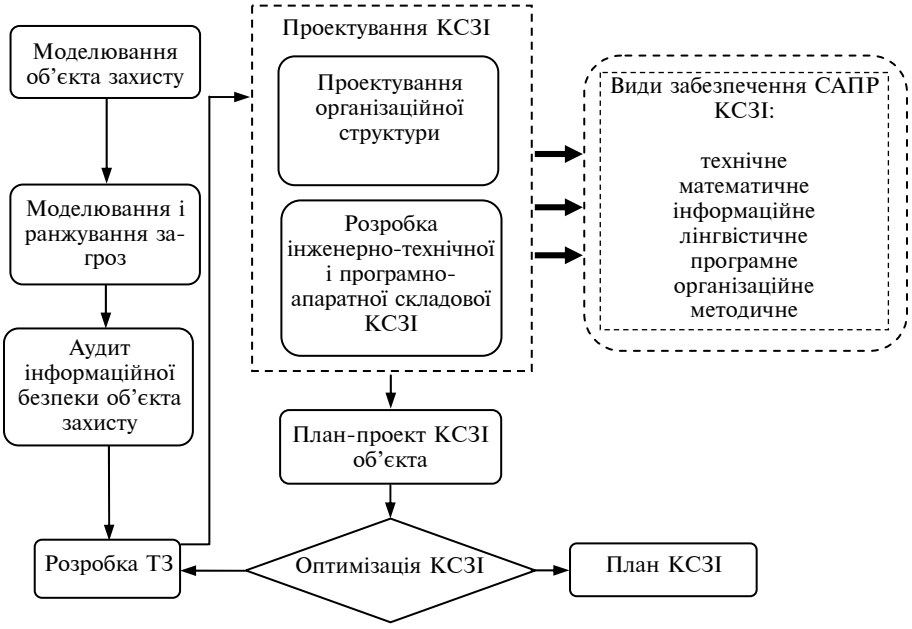

Рис. 1. Структурно-функціональна схема САПР КСЗІ

Складовими елементами КСЗІ є такі системи захисту, як:

- *правовий захист інформації* – захист інформації, що базується на використанні статей конституції і законів держави. Він регламентує права і обов'язки суб'єктів інформаційних відносин та є основою для морально-етичних норм у галузі захисту інформації;
- *організаційний захист інформації* – комплекс напрямків і методів керівного, обмежувального та технологічного характеру, які визначають основи і зміст *системи захисту*, вимагає від персоналу виконувати правила захисту конфіденційної інформації;
- *інженерно-технічний захист інформації* – захист інформації при її обробці технічними засобами, який здійснюється також технічними засобами спеціального призначення;
- *програмний захист інформації* – захист інформації спеціальними програмними засобами;
- *криптографічний захист інформації* – захист інформації через її криптографічне перетворювання.

Відносно автоматизованих систем обробки даних поняття КСЗІ можна визначити як єдиний комплекс правових норм, організаційних заходів та технічних, криптографічних і програмних засобів, використаних згідно з визначеною політикою безпеки.

На початковому етапі проектування отримується модель об'єкта захисту за рахунок структурування інформації і визначаються (або задаються) характеристики процесу проектування (з "нуля" або модифікація діючого об'єкта), визначається категорія автоматизованої системи або об'єкта інформаційної діяльності, можливі обмеження. Далі моделюються загрози інформації за типовою методикою. На наступному етапі здійснюється передпроектний аудит безпеки, що дає можливість оцінювати ефективність системи захисту, та визначаються напрямки модернізації або розробки. В результаті отримують ТЗ на проектування КСЗІ.

Згідно з ТЗ вибираються методи і засоби захисту, починаючи з визначення організаційної структури об'єкта захисту. Результатом роботи САПР КСЗІ для автоматизованої системи обробки даних є розробка політики безпеки автоматизованої системи.

Очевидно, що прийняття рішень на кожному кроці етапів проектування не вимагає використання навченої АП. Визначені етапи проектування алгоритмуються і прийняття рішень здійснюється через жорсткі правила. Тому розробці з використанням АП з навчанням підлягають лише такі фрагменти процесу проектування, де рішення може прийматися або завдяки досвіду проектанта, або експертним способом.

Дослідженню головних фрагментів процесу проектування з використанням АП присвячений наступний матеріал. При подальшому розгляді передбачається, що система проектування розглядається як модель до тих пір, поки АП, що використовується на визначених етапах у вигляді ансамблевих нейроподібних сіток, перебуває в процесі навчання. САПР стає системою проектування тільки з моменту, коли для АП процес навчання завершений.

Моделювання з використанням АП при створенні КСЗІ. Загальна структура та елементи КСЗІ можуть ілюструватися по-різному. Один із варіантів наведено на рис. 2. Зліва від "об'єкта" визначеною є послідовність формування моделі загроз, на основі якої формуються можливі та необхідні напрямки захисту в рамках бази даних доступних напрямків. Подання здійснюється у вигляді переліку дій (елементів поведінки), направлених на забезпечення захисту. Послідовність дій формує поведінкову характеристику. Сукупність наведених елементів є 1-м рівнем формування моделі. В результаті проходження 1-го рівня визначаються правила, за якими захищається об'єкт із врахуванням притаманних об'єкту індивідуальних особливостей. Таким чином, створюється образ системи захисту, а модель проходить шлях від інтегрального образу порушника до інтегрального образу "захисника" в межах бази даних таких образів.

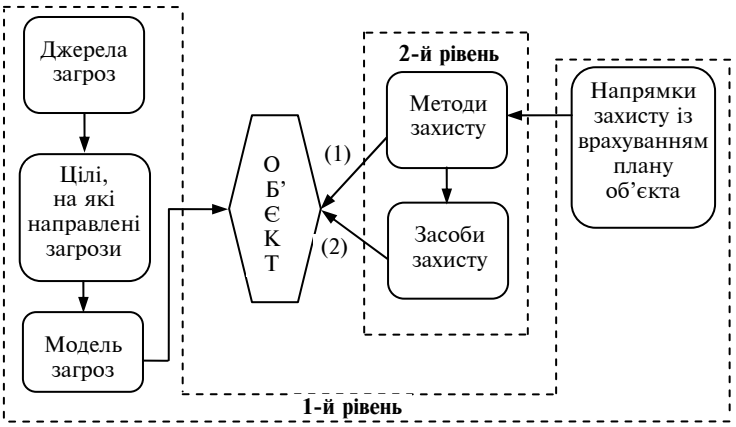

Рис. 2. Варіант узагальненої структури КСЗІ

Другий рівень більш прагматичний. У рамках створеної заздалегідь бази даних методів захисту з усієї множини методів формується їх підмножина, характерна для даного об'єкта. Визначення інтегрального образу підмножини методів захисту, мабуть, не є раціональним тому, що елементи такого образу можуть бути не залежними один від одного і загальний їх образ не є інформативним, тобто не створює ідентифікатора. В результаті даного етапу формується перелік необхідних для даного об'єкта організаційних заходів (на рис. 2 позначка (1)). Визначені заходи можуть при необхідності підтримуватися підмножиною (на рис. 2 позначка (2)) з переліку технічних засобів захисту, які визначені в рамках заздалегідь створеної бази даних засобів захисту. При формуванні методології створення моделі системи проектування завдання полягає в тому, щоб визначити ті фрагменти структури системи (переходи від одного елемента наведеної структури до іншого), які є сенс моделювати на засадах АП у вигляді сіток з навчанням. Вибір має бути таким, щоб виключити вплив індивідуальних властивостей проектанта при розв'язанні задачі вибору того чи іншого рішення на кожному етапі проекту. Така властивість забезпечується за рахунок організації зазначених баз даних шляхом їх формування у вигляді ансамблевих сіток великого розміру, навчання яких здійснюється за рахунок пред'явлень великої кількості реально створених проектів діючих об'єктів, причому необхідною умовою є такий вибір проектів, де є проекти, виконані різними проектантами, і чим їх більше, тим краще. Що стосується історії об'єкта, то в сітках формуються активовані зв'язки між елементами сіті (нейроподібними елементами) при кожному навчанні і в подальшому зв'язки зберігаються, якщо штучно їх не знищувати (процедура забування). При послідовному подальшому пред'явленні проектів нових об'єктів чи нових джерел загроз існуючим об'єк-

там ці зв'язки або підтверджуються (якщо нові фрагменти збігаються, або є близькими до вже існуючих), або формуються нові зв'язки. Чим більше нових пред'явлень (таких, що образно відрізняються від існуючих), тим у більшій мірі сіть починає реагувати на таке пред'явлення, яке є характерним для проектів нових пред'явлень. Інакше кажучи, поведінка сіті адаптується до нових пред'явлень (образів) із врахуванням статистики їх властивостей. Такий підхід забезпечує постійне підвищення об'єктивності проектування з нарощуванням кількості пред'явлень. Сіть набуває об'єктивного "досвіду". Важливо, щоб кількість пред'явлень була такою, при якій працює закон великих чисел, тобто АП на базі сіті стала б статистичною.

Із врахуванням зазначеного фрагменти структури системи у вигляді АП мають сенс на переходах: "Джерела загроз"–"Модель загроз", "Модель загроз"–"Напрямки захисту", "Напрямки захисту"–"Методи захисту". В інших фрагментах доступною є жорстка алгоритмізація проекту, причому при визначенні засобів захисту в рамках переліку засобів захисту (позначка (2) на рис. 2) нескладно використовувати оптимізацію за фінансово-економічним показником.

Висновки

Створення моделей систем інтелектуальної підтримки прийняття рішень при проектуванні КСЗІ за рахунок використання нейроподібних сіток має забезпечити впорядкованість процесу проектування та прийняття оптимальних (квазіоптимальних) рішень на кожному етапі. Якщо життєдіяльність сітьової моделі не переривається, нарощування загальної бази даних АП усіх фрагментів структури системи безперервно вдосконалює модель та автоматично адаптує до зміни умов життєдіяльності об'єктів, змін у методичній базі технічного захисту інформації, вдосконалюванні способів інформаційної атаки. Саме такі властивості мають забезпечувати підвищення об'єктивності та оптимальності майбутніх проектів.

В.Н. Луценко

СИСТЕМА ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ ПРОЕКТИРОВАНИИ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Рассмотрены проблемы анализа свойств ансамблевых сетей для создания проектов систем защиты информации. Определены основные свойства таких проектов. На основе сетевого нейровидного моделирования предложена методика проектирования комплексных систем защиты информации.

V.M. Lutsenko

MODELLING OF THE INTELLECTUAL SUPPORT SYSTEMS OF ACCEPTANCE DECISIONS AT DESIGNING COMPLEX SYSTEMS OF THE INFORMATION PROTECTION

The paper considers problems of analyzing properties of assembly networks for creating projects of information protection systems. The basic properties of such projects are given. Relying on the network neuronal modeling, the technique of complex system designing for information protection is developed.

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 // Прикл. радиоэлектроника. Тем. выпуск, посвященный проблемам обеспечения безопасности информации. – 2009. – **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 Інтернеті www.sciencedirect.com).
5. *Гордиевский М.Д., Поляков А.А.* Управление рисками в высокотехнологичных проектах: состояние и подходы

управления // Методи та засоби програмної інженерії. – 2008. – **1**. – С. 311–319.

6. *Липаев В.* Оценка качества программных средств // ИСП РАН “Сетевой журнал”. – 2002. – № 3. – С. 37–41.
7. *Груздо И.В.* Повышение качества программного проекта за счет управления рисками. НАУ им. Н.Е. Жуковского “ХАИ”. – Харьков: [Электронный ресурс]. – Режим доступу до статті: http: //www.nbuv.gov.ua/natural /soi/2009_1/Gruzdo.pdf. – Заголовок з екрана.
8. *Медведовский И.* Современные методы и средства анализа и контроля рисков информационных систем компаний CRAMM, RiskWatch, Гриф. – [Электронный ресурс]. – Режим доступу до статті: idm@dsec.ru. 17.01.04.
9. *Астахов А.* Анализ рисков и управление ими. Центр аудита информационной безопасности. – [Электронный ресурс]. – Режим доступу до статті: http: //bezpeka.ladimir.kiev.ua/pg/show/risks/page2.html. – Заголовок з екрана.
10. *Луценко В.Н.* Особенности построения многопроцессорных вычислительных устройств для моделирования нейронных сетей: Автореф. дис. ... канд. техн. наук. – К., 1988. – 15 с.
11. *Луценко В.Н.* Подготовка данных и формирование инвариантов в системах искусственного интеллекта. – Киев, 1992. – 21 с. – (Препр. / НАН Украины. Ин-т кибернетики им. В.М.Глушкова; 92-2).
12. *Амосов Н.М., Касаткин А.М., Касаткина Л.М.* О возможной организации системы принятия решений // Нейроподобные сети в робототехнике. – К.: ИК АН УССР, 1979. – С. 58–72.
13. *Перцептрон* – система разпознавания образов / Под ред. А.Г. Ивахненко. – К.: Наук. думка, 1975. – 432 с.
14. *Hopfield J.J.* Neural networks and physical systems with emergent collective computational abilities // Proc. Natl. Acad. Sci. USA. – 1982. – **79**. – С. 2554–2558.
15. *Hopfield J.J., Tank D.W.* Neural Computation of Decisions in Optimization Problems // Biological Cybernetics. – 1985. – **52**, N 3. – P. 141–152.
16. *Аверченков В.И., Рытов М.Ю.* Организация защиты информации: Учеб. пособие для вузов. – Брянск: БГТУ, 2005. – 184 с.
17. *Аверченков В.И., Рытов М.Ю., Грабежов И.Е., Гайнулин Т.Р.* Автоматизация проектирования комплексных систем защиты информации. – Брянск: Брянский гос. техн. ун-т. – [Электронный ресурс]. – Режим доступу до статті: http://conference.kemsu.ru/GetDocsFile?id=9264&table=papers_file&type=0&conn=confDB. – Заголовок з екрана.

Рекомендована Радою
Фізико-технічного інституту
НТУУ “КПІ”

Надійшла до редакції
10 лютого 2010 року