де: D_{t_Y} – висновок по каналу яскравості Y; $D_{t_{C1}}$ – висновок по колірному каналу C_1; $D_{t_{C2}}$ – висновок по колірному каналу C_2.

Висновок. У роботі розроблено підхід до ідентифікації межі образу балістичного тіла на цифровому зображенні із використанням нечіткого логічного висновку.

Формування функцій належності фону, тіла та межі відбувається на основі статистичного аналізу значень яскравості точок фрагменту зображення балістичного тіла.

Висновок про належність кожної окремої точки робимо на основі правил нечіткого логічного висновку, який базується на оцінці значень належності самої точки та її оточення. Матриця знань будується на базі експертних висновків.

Література

1. Лобанов А.Н. Фотограмметрия : учебник [для студ. ВУЗов] / А.Н. Лобанов. – Изд. 2-ое, [перераб. и доп.]. – М. : Изд-во "Недра", 1984. – 552 с.

2. Петров М.Н. Компьютерная графика : учебник (+CD) / М.Н. Петров, В.П. Молочков – СПб. : Изд-во "Питер", 2003. – 736 с.

3. Руденко В.М. Математична статистика : навч. посібн. / В.М. Руденко. – К. : Центр навч. літ-ри, 2012. – 304 с.

4. Ротштейн А.П. Медицинская диагностика на нечеткой логике / А.П. Ротштейн. – Винница: Континент – ПРИМ, 1996. – 132 с.

5. Заде Л. Понятие лингвистической переменной и ее применение в принятию приближенных решений / Л. Заде. – М. : Изд-во "Мир", 1976. – 167 с.

Шабатура Ю.В., Кузьменко Р.В. **Определение реальной границы изображения баллистического тела на цифровом фото и снимке методами нечеткой логики**

В контексте широкой задачи по исследованию параметров траектории средствами фото-, видеорегистрации разработаны метод определения реального контура цифрового изображения баллистического тела. Метод основывается на применении нечеткого логического вывода о принадлежности каждой отдельной точки цифрового изображения.

Ключевые слова: баллистическое тело, цифровое изображение, нечеткая логика.

Shabatura Yu.V., Kuzmenko R.V. **Determination of actual limit of image of ballistic body on digital snapshot by methods of fuzzy logic**

In the context of wide task on research of parameters of trajectory by facilities of photo-, video-registrations are developed method of determination actual the contour of digital representation of ballistic body. A method is based on application of unclear logical conclusion about belonging of every separate point of digital representation.

Keywords: ballistic body, digital representation, fuzzy logic.

УДК [004.042]: 621.391

Ад'юнкт З.П. Сташевський; проф. Ю.І. Грицюк, д-р техн. наук – Львівський ДУ БЖД

ОСОБЛИВОСТІ ПРОБЛЕМИ СИНТЕЗУ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ У СТРУКТУРНИХ ПІДРОЗДІЛАХ МНС УКРАЇНИ

Розглянуто особливості проблеми синтезу сучасних систем захисту інформації (СЗІ), які планується впроваджувати у структурні підрозділи МНС України. Встановлено, що сучасні СЗІ, будучи складовою частиною глобальних інформаційних систем, є складними технічними системами. Розв'язання задач аналізу і синтезу СЗІ вимагає врахування значної кількості методів оцінювання якості їх функціонування, тобто інтенсивності її використання як активного засобу виконання операцій забезпечення конфіденційності оброблення, зберігання та передачі інформації. Комплексним показником оцінювання якості цих операцій виступає вироблене експертами оцінювальне судження відносно придатності заданого способу дій фахівців щодо захисту інформації, або пристосованість засобів захисту інформації до різних проявів джерел загроз.

Ключові слова: глобальна інформаційна система, проектування систем захисту інформації, конфіденційність оброблення інформації, задачі аналізу і синтезу, джерела загроз, теорія нечітких множин і лінгвістичної змінної.

Актуальність дослідження. За останні декілька десятиліть значно зросла кількість втручань зловмисників [11, 20] у роботу сучасних систем захисту інформації (СЗІ). Значення та вагомість наслідків таких втручань з часом збільшилися настільки, що навіть розвинені держави, їх промислові та фінансові структури стали заручниками своїх інформаційних технологій.

Якщо раніше проблема захисту інформації була надбанням тільки спеціальних служб, то згодом вона стала актуальною для всіх організацій та підприємств, у тому числі і структурних підрозділів МНС України, так чи інакше пов'язаних з інформаційними потоками. У будь-якому випадку усі стратегічні та тактичні дії щодо проектування та впровадження сучасних СЗІ [2, 3] вимагають системного аналізу проблеми [10] і дослідження операцій [17], які супроводжуються складними інформаційними процесами, більшість з яких мають конфіденційний характер.

Отож *метою роботи* є виявлення особливостей проблеми синтезу систем захисту інформації у структурних підрозділах МНС України. Для цього потрібно вирішити такі основні завдання:

1) з'ясувати проблему оцінювання якості функціонування сучасних СЗІ;
2) виявити коректність постановки задач забезпечення безпеки СЗІ;
3) встановити обсяг та структуру досліджень, пов'язаних з проектуванням і впровадженням СЗІ, та очікувані основні результати;
4) охарактеризувати узагальнені моделі сучасної СЗІ;
5) з'ясувати особливості методів оцінювання якості функціонування СЗІ та обґрунтувати вимоги до них.

1. Проблема оцінювання якості функціонування сучасних систем захисту інформації

Оцінювання якості функціонування сучасних СЗІ при високому рівні невизначеності початкових умов і обмежень має виконуватися з використанням комплексу взаємоузгоджених математичних моделей, які легко адаптуються до конкретних об'єктів інформаційної безпеки і, як наслідок, мають передбачати можливість постійного їх удосконалення з урахуванням наявних і потенційних джерел загроз [12].

При синтезі сучасних СЗІ, які планується впровадити у структурні підрозділи МНС України, мають використовуватися такі положення [8]:

- вибір чутливого критерію ефективності об'єкта інформаційної безпеки здійснюють відповідно до архітектури СЗІ, а також наявної чи впровадженої технології оброблення інформації;

- формулювання завдань захисту інформації враховують усі апріорні відомості про об'єкт інформаційної безпеки, а також вирішуються відповідно до прийнятого критерію ефективності.

Підсумком вирішення проблеми синтезу сучасної СЗІ та кінцевою метою її впровадження у структурні підрозділи МНС України мають бути такі змістовні результати [14]:

- архітектура оптимальної СЗІ та функціональної можливості;
- кількісна оцінка ефективності функціонування СЗІ відносно якості обслуговування до вартості оброблюваної інформації;
- методика оцінювання чутливості критерію ефективності СЗІ до потенційних відхилень від апріорних даних;
- фізична реалізація синтезованої СЗІ, а також її консолідація з іншими інформаційними системами обміну даними;
- відповідність технології оброблення інформації заданому рівню її захисту.

Під ефективністю функціонування СЗІ у структурних підрозділах МНС України розумітимемо інтенсивність її використання як активного засобу виконання операцій забезпечення конфіденційності оброблення, зберігання та передачі інформації [8]. При цьому комплексним показником оцінювання якості цих операцій виступає вироблене експертами оцінювальне судження відносно придатності заданого способу дій фахівців щодо захисту інформації, або пристосованість засобів захисту інформації до різних проявів джерел загроз. Введення кількісного показника використання СЗІ вимагає визначення критерію її ефективності, який даватиме змогу співставляти між собою різні стратегії захисту інформації, кожна з яких характеризується різним ступенем досягнення кінцевої мети, з цінністю оброблюваної інформації, а також здійснювати вибір ефективної стратегії з множини допустимих.

Теоретичні основи побудови оптимальних СЗІ надзвичайно складні та далекі від досконалості, незважаючи на значну кількість та інтенсивність виконуваних досліджень в цій предметній області знань [2, 8, 12]. Водночас відсутність на сьогодні достатньо загальної теорії, яка б формувала методологічні підстави дослідження явищ з невизначеними чинниками, робить не завжди придатними байєсовскі методи класичної теорії статистичних досліджень [4] для синтезу оптимальних СЗІ.

Під методологією оптимізації СЗІ розумітимемо розроблення досконалого комплексу математичних моделей, що пов'язують її ієрархічну структуру, логічну організацію, методи і засоби її реалізації, які дають змогу сформулювати векторну цільову функцію вибору підмножини найкращих стратегій з множини допустимих. Оптимальними вважатимуться стратегії, які в передбачуваних умовах функціонування СЗІ якнайкраще задовольняють умови та обмеження конкретної постановки задачі. Оптимальність розв'язку такої задачі досягається за рахунок найбільш раціонального розподілу виділених ресурсів, які витрачатимуться на вирішення поточних і перспективних питань захисту інформації.

У процесі проектування оптимальної СЗІ, яку планується впровадити у структурні підрозділи МНС України, може виникати потреба коректування деяких вимог до самого об'єкта інформаційної безпеки. Труднощі їх подолання полягають в тому, що появляються значні невизначеності переважно стохастичного характеру, які характеризуються [18]:

- наявністю цілеспрямованої протидії з боку опозиційних СЗІ, способи дій яких не завжди відомі як розробникові, так фахівцям з їх експлуатації;
- не достатньою вивченістю деяких явищ, які раніше супроводжували процес функціонування наявної СЗІ;
- не достатньо чітким представленням мети операцій забезпечення конфіденційності обробляння, зберігання та передачі інформації, яке призводить до неоднозначного трактування реальних результатів реалізацій операцій за відношенням до нормативних.

2. Коректність постановок задач забезпечення безпеки системи захисту інформації

На сьогодні проблема забезпечення безпеки інформаційних технологій стикається зі значними труднощами їх дослідження та реалізації, які так чи інакше сприяють невизначеності умов функціонування СЗІ. Тому постановка задачі забезпечення безпеки СЗІ є не коректною, оскільки найчастіше не враховує її поведінку в нестандартних і, особливо, екстремальних ситуаціях. Вплив невизначеності особливо відчутно проявляється в адаптованих, слабко організованих СЗІ, які, як правило, є нестабільними через неповноту, неточність, не нормованість та низьку достовірність інформації, якою володіють фахівці з їх експлуатації.

Відомі на сьогодні постановки задач забезпечення безпеки інформаційних технологій [11, 20], як правило, не мають оптимального розв'язку, ефективність якого визначається ступенем обліку множини допустимих обмежень та умов використання, характерних для конкретного об'єкта інформаційної безпеки. Для підвищення рівня коректності постановок задач забезпечення безпеки СЗІ у структурних підрозділах МНС України необхідно підвищувати знання про конкретні умови їх функціонування, які часто залежать не тільки від наявних і потенційних джерел загроз, але й умов їх експлуатації. У зв'язку з цим процес отримання знань [7] розробником СЗІ та використання набутого досвіду має здійснюватися безпосередньо під час її функціонування на конкретному об'єкті інформаційної безпеки шляхом поступового накопичення необхідних даних, подальшого їх аналізу і застосування при реалізації системою заданої цільової функції в умовах взаємодії внутрішнього і зовнішнього динамічного середовища.

Відомі на сьогодні математичні моделі [4, 15], які використовуються для опису ієрархічної структури СЗІ, її поведінки і процесу управління не завжди є придатними при навіть коректних постановках задачі, тобто не дають бажаного результату. Тому потрібно розробляти досконалі математичні моделі, нові методи і алгоритми їх реалізації, орієнтовані на сучасну специфіку захисту інформації у структурних підрозділах МНС України.

Для отримання інформації про поведінку СЗІ на конкретному об'єкті інформаційної безпеки потрібно виділити групи параметрів її стану і визначити періоди перевірки їх значень. При цьому беруться до уваги особливо значущі та математично чутливі параметри, які безпосередньо випливають на

реалізацію мети функціонування СЗІ. Процес перевірки значень таких параметрів, а також їх детальний аналіз здійснюється для підвищення знань про особливості функціонування СЗІ, які згодом мають забезпечити можливість прийняття своєчасних і адекватних рішень, спрямованих на коректування її поведінки при відхиленні від нормативних даних. Тому у сучасних СЗІ обов'язково має передбачатися процедура контролю її працездатності та діагностики станів у визначені та випадкові періоди перевірки.

Прийняття управлінських рішень під час експлуатації СЗІ у структурних підрозділах МНС України здебільшого може базуватися на експертних оцінках [1, 4, 8, 13] із залученням провідних фахівців у даній області знань. Проте в умовах невизначеності початкових даних і постійної некоректності постановок задач процесу управління ці оцінки можуть мати додаткову некоректність, які так чи інакше впливатимуть на прийняття поточних рішень, збільшивши цим самим початкову невизначеність умов функціонування СЗІ.

3. Структура досліджень системи захисту інформації та основні їх результати

Вирішення проблем проектування сучасних СЗІ, які планується впровадити у структурні підрозділи МНС України, вимагає поетапного виконання такого комплексу теоретичних і прикладних досліджень [2, 6].

1. З'ясування принципів, методів і засобів реалізації сучасних СЗІ, які дадуть змогу скоротити розмірність її опису, складається з реалізації таких основних задач:

- аналіз ієрархічної структури СЗІ та взаємозв'язків між задачами, які в ній розв'язуються;
- аналіз динамічних характеристик задач, які розв'язуються у кожній ієрархічній структурі СЗІ;
- аналіз кореляційних залежностей між параметрами станів кожної ієрархічної структури СЗІ, які є результатами розв'язання окремих задач у кожній із них;
- виділення сукупностей задач, результат розв'язання кожної з яких дає змогу визначити як мінімум один з контрольованих параметрів станів кожної ієрархії СЗІ зокрема і всієї системи загалом.

Внаслідок розв'язання цих задач мають бути сформульовані вимоги і рекомендації щодо раціональної організації ієрархічної структури СЗІ, скомпонованої за рівнями контролю параметрів їх стану та загальним процесом управління. Це дасть змогу проводити подальші дослідження в умовах мінімальної розмірності опису СЗІ загалом і кожної її ієрархії зокрема.

2. Процес розроблення алгоритмів, методів і засобів розв'язання задач, які дадуть змогу забезпечити безпеку СЗІ за умов невизначеності вхідних даних і очікуваних результатів, складається з дослідження таких питань:

- коректності постановок задач при не завжди достатньому розумінні очікуваних результатів і цілей їх розв'язання за умов, які постійно змінюються;
- використання невизначеності (неповноти, неточності, низької достовірності та ін.) початкових даних при розв'язуванні задач забезпечення безпеки СЗІ на конкретному об'єкті інформаційної безпеки.

Результатом виконання таких досліджень мають стати розроблені математичні моделі, методи і засоби розв'язання не завжди коректно поставлених задач за умов невизначеності вхідних даних і очікуваних результатів.

3. Процес розроблення алгоритмів, методів і засобів адаптивного контролю параметрів функціонування та діагностування стану СЗІ складається з реалізації таких задач [6]:

- формування динамічних зон (нормального функціонування, попередження, тривоги, катастрофи), які характеризують різні стани СЗІ, встановлення динамічних порогів, які розділяють ці зони, а також виділення динамічних характеристик інтегральних векторів індикації станів системи;
- розроблення стратегії та тактики виконання адаптивного (за часом проведення, за кількістю та номенклатурою контрольованих параметрів) контролю параметрів інтегральних векторів індикації станів СЗІ, прогнозування тенденцій зміни їх значень в процесі її функціонування;
- розроблення методів і алгоритмів адаптивного поодинокого і групового контролю значень параметрів векторів індикації станів СЗІ, а також прогнозування допустимих відхилень від їх заданих значень;
- розроблення методів і алгоритмів розпізнавання та ідентифікації належності станів СЗІ динамічним зонам і порогам чутливості на підставі аналізу поточних і прогнозованих значень окремих параметрів і векторів індикації;
- розроблення методів і алгоритмів діагностування станів СЗІ на основі аналізу результатів ідентифікації за усіма параметрами векторів індикації.

Внаслідок розв'язання цих задач має бути створена методика, математичні методи і програмно-технічні засоби для організації адаптивного контролю параметрів функціонування та діагностування станів СЗІ.

4. Процес розроблення принципів, методів і засобів самоорганізації СЗІ складається з реалізації таких задач [6]:

- побудова адаптивних моделей опису ієрархічної структури СЗІ та її поведінки за різних режимів роботи, прогнозування допустимих значень її параметрів на кожному ієрархічному рівні системи зокрема та усієї системи загалом;
- побудова адаптивних моделей процесу формування підмножин контрольованих параметрів і контролю діапазонів значень їх динамічних зон на підставі заданих вимог до функціональної стійкості СЗІ за різних режимів роботи;
- побудова адаптивних моделей контролю працездатності СЗІ за різних режимів роботи і діагностування порушень, які впливають на її працездатність;
- самоорганізація та самовдосконалення груп моделей опису ієрархічної структури СЗІ, її поведінки, прогнозування, контролю та діагностування, забезпечення потрібної функціональної стійкості системи з урахуванням впливу чинників внутрішнього і зовнішнього середовища.

Результатом розв'язання таких задач мають бути створені адаптивні моделі на підставі відомих і спеціально розроблених методів і засобів їх реалізації, які дадуть змогу адекватно описувати ієрархічну структуру і поведінку СЗІ за різних режимів роботи, а також здійснювати контроль показників функціонування та діагностування, а також прогнозування допустимих значень параметрів її станів.

5. Процес розроблення алгоритмів, методів і засобів систем підтримки прийняття рішень при управлінні СЗІ складається з реалізації таких задач:

- розроблення методів і засобів вибору рішень з множини альтернатив на підставі аналізу стану і поведінки СЗІ з урахуванням вимог процесу управління та обмежень реального ресурсу, а також кваліфікованих оцінок близьких і віддалених наслідків виконання прийнятих рішень;

- розроблення методів і засобів декомпозиції прийнятих рішень за ієрархічними рівнями процесу управління СЗІ;
- розроблення методів і засобів систем підтримки прийняття рішень щодо самоорганізації СЗІ в процесі її функціонування та вдосконалення усіх видів перерахованих вище моделей і їх груп.

Розв'язання зазначених вище задач базується на використанні усіх раніше отриманих результатів, а усі вони загалом орієнтовані на створення банку знань [7] про удосконалену СЗІ, яка згодом експлуатуватиметься у структурних підрозділах МНС України.

Для вирішення перерахованих вище, а також інших теоретичних і прикладних проблем, пов'язаних з проектуванням сучасних СЗІ, потрібна цілеспрямована організація комплексу досліджень, які виконуватимуться у рамках державних програм і на єдиній концептуальній та методологічній основі, кінцевим результатом якої має бути узагальнена модель СЗІ.

4. Характеристика узагальнених моделей систем захисту інформації

Основне призначення узагальнених моделей СЗІ полягає в створенні передумов для об'єктивної оцінки загального її стану щодо ступеня уразливості джерелами загроз або рівня захищеності інформації в ній від несанкціонованого доступу [13]. Потреба в таких оцінках зазвичай виникає при аналізі загальних умов функціонування СЗІ з метою вироблення стратегічних рішень при організації процесу захисту інформації на конкретному об'єкті інформаційної безпеки.

Узагальненими моделями СЗІ і процесу оброблення інформації у ній вважаються такі, які дають змогу визначати (оцінювати) загальні показники її функціонування та параметри станів системи і процесів, які відбуваються в ній, на відміну від моделей локальних і часткових, а також забезпечують можливість визначення (оцінювання) деяких локальних або часткових характеристик систем або процесів.

Системну класифікацію узагальнених моделей СЗІ на сьогодні зробити надзвичайно важко, оскільки, для цього немає достатніх відомостей про них, а також через малу кількість таких моделей, які на сьогодні експлуатуються у структурних підрозділах МНС України. Тому класифікацію узагальнених моделей СЗІ представимо простим переліком і короткою характеристикою тільки деяких з них [12].

Узагальнена модель процесу захисту інформації в загальному вигляді та для загального об'єкта інформаційної безпеки має відображати процес захисту інформації як процес взаємодії дестабілізаційних чинників, які впливають на безпеку інформації, та методів і засобів її захисту, які перешкоджають дії цим чинникам. Підсумком такої взаємодії буде той або інший рівень захищеності інформації в системі її захисту.

Узагальнена модель системи захисту інформації, будучи подальшим розвитком узагальненої моделі процесу захисту інформації, має відображати ієрархію процесів її захисту, які здійснюються в ній, з метою їх раціонального впорядкування. Такі процеси в найзагальнішому вигляді можуть бути представлені як процеси розподілу і використання наявних ресурсів, що виділяються на захист інформації.

Модель загальної оцінки джерел загроз інформації в основному спрямована на оцінювання не просто наявних чи потенційних джерел загроз інформації, а ще й на оцінювання тих втрат, які можуть виникати після їх проявів. Моделі цього напряму важливі ще і тим, що саме за допомогою них найбільше було виявлено ті умови функціонування СЗІ, при яких результати такого оцінювання є адекватними реальним процесам захисту інформації;

Моделі аналізу систем розмежування доступу до ресурсів СЗІ призначені для забезпечення процесу розв'язання задач аналізу і синтезу систем (механізмів) розмежування доступу до різних видів ресурсів СЗІ і, насамперед, до бази даних, записи якої містять засоби управління нею. Виділення цих моделей в самостійний клас загальних моделей пов'язане з тим, що механізми розмежування доступу до ресурсів СЗІ належать найбільш істотним її компонентам, від ефективності функціонування яких значною мірою залежить загальна ефективність самого процесу захисту інформації.

5. Особливості методів оцінювання якості функціонування систем захисту інформації та обґрунтування вимог до них

Сучасні СЗІ, які широко використовуються у різних організаціях і підприємствах, у тому числі структурних підрозділах МНС України, з одного боку є складовою частиною глобальних інформаційних систем, а з іншого боку – вони самі є складними технічними системами. Розв'язання задач аналізу і синтезу СЗІ ускладнюється потребою врахування значної кількості методів оцінювання якості їх функціонування [5], основними з яких є:

- складний опосередкований взаємозв'язок критеріїв ефективності функціонування СЗІ з показниками роботи адитивної інформаційної системи;
- потреба обліку великої кількості вимог щодо якості роботи СЗІ при оцінюванні та виборі її раціонального варіанта;
- переважно якісний, а не кількісний, характер вимог, які враховуються при аналізі та синтезі СЗІ;
- значний взаємозв'язок і взаємозалежність цих вимог, які часто мають суперечливий характер і неоднозначність трактування;
- складність отримання початкових даних, необхідних для розв'язування задач аналізу і синтезу СЗІ, особливо на ранніх етапах їх проектування.

Вказані особливості методів оцінювання якості функціонування СЗІ роблять практично неможливим застосування традиційних математичних методів, у тому числі методів математичної статистики і теорії ймовірності, а також класичних методів оптимізації [18] для розв'язування прикладних задач аналізу і синтезу СЗІ.

Складність процесу прийняття управлінських рішень при проектуванні сучасних СЗІ для потреб структурних підрозділах МНС України, відсутність досконалого математичного апарату призводять до того, що при оцінювані якості її функціонування та виборі допустимих альтернатив можливо, а часто просто необхідно, використовувати і обробляти якісну експертну інформацію фахівців, які безпосередньо експлуатують такі системи. Перспективним напрямом розроблення методів прийняття управлінських рішень при експертній початковій інформації є лінгвістичний підхід на базі теорії нечітких множин і лінгвістичної змінної [5, 15].

Теорія нечітких множин [5] характеризується однією особливістю, відомою усім дослідникам: застосовуваний у ній формальний апарат за своїми потенційними можливостями і точністю має бути адекватний змісту і точності початкових даних. Математична статистика і теорія ймовірності [4] здебільшого використовує експериментальні дані, які мають строго певну точність і достовірність. Водночас теорія нечітких множин має справу з "людськими знаннями", які прийнято називати експертною інформацією.

Відомо, що експерт (від лат. expertus – досвідчений; англ. expert) – фахівець, який здійснює експертизу. Водночас, експертиза (від лат. expertus – досвідчений, знавець; англ. examination) – розгляд, дослідження експертом-фахівцем якихось справ чи питань, що потребують спеціальних знань. У найбільш загальному вигляді експертиза – це спосіб аналізу причинно-наслідкових зв'язків не тільки стосовно того, що вже відбулося, але й того, що очікується, має або може відбутися [19].

Проведення експертиз в Україні регламентується Законом про наукову і науково-технічну експертизу та Законом про судову експертизу, іншими нормативно-правовими актами [16]. Наукова і науково-технічна експертиза – діяльність, метою якої є дослідження, перевірка, аналіз та оцінка науково-технічного рівня об'єктів експертизи і підготовка обґрунтованих висновків для прийняття управлінських рішень щодо таких об'єктів [9].

Стосовно СЗІ, то основними завданнями наукової та науково-технічної експертизи є:

1) об'єктивне, комплексне дослідження об'єкта інформаційної безпеки;
2) перевірка відповідності об'єкта інформаційної безпеки вимогам і нормам чинного законодавства;
3) оцінка відповідності об'єкта інформаційної безпеки сучасному рівню наукових і технічних знань, тенденціям науково-технічного прогресу, принципам державної науково-технічної політики, вимогам екологічної безпеки, економічної доцільності;
4) аналіз рівня використання науково-технічного потенціалу, оцінка результативності науково-дослідних робіт і дослідно-конструкторських розробок;
5) прогнозування науково-технічних, соціально-економічних і екологічних наслідків реалізації чи діяльності об'єкта інформаційної безпеки;
6) підготовка науково обґрунтованих експертних висновків.

Підставами для проведення наукової та науково-технічної експертизи об'єкта інформаційної безпеки можуть бути договори на її проведення, укладені структурним підрозділом МНС України з відповідною експертною установою та організацією чи фізичними особами. За чинним українським законодавством наукова і науково-технічна експертиза проводяться у формі державної, громадської та іншої експертизи. Державну наукову і науково-технічну експертизу проводять:

- органи виконавчої влади у сфері наукової та науково-технічної діяльності;
- підприємства, установи та організації, тимчасові експертні колективи, компетентні у відповідній галузі наукової та науково-технічної діяльності, за дорученням державних органів.

Наукову і науково-технічну експертизу СЗІ на об'єкті інформаційної безпеки структурного підрозділу МНС України можуть проводити наукові і науково-технічні установи, підприємства та організації різних форм власності і підпорядкування, а також спеціально створені експертні організації, статутна діяльність яких передбачає проведення наукових і науково-технічних експертиз, з ініціативи фізичних та юридичних осіб, заінтересованих в отриманні експертних висновків.

Експертний висновок – документально оформлений результат експертизи, який надається Адміністрацією Державної служби спеціального зв'язку та захисту інформації України (далі – Адміністрація Держспецзв'язку) за проведеним аналізом результатів експертних досліджень. Експертне дослідження СЗІ проводиться на основі комплексного і системного вивчення законодавства, наукової літератури, вивчення стану справ на конкретному об'єкті інформаційної безпеки і узагальнень фахової практики експлуатації аналогічних систем на інших об'єктах.

Висновок державної наукової та науково-технічної експертизи є обов'язковим для прийняття структурним підрозділом МНС України до розгляду та врахування при обґрунтуванні структури і змісту пріоритетних напрямів удосконалення СЗІ, проведення наукових і науково-технічних її досліджень, впровадження екологічних програм і проектів, реалізації наукової та науково-технічної діяльності обслуговувального персоналу, проведення аналізу ефективності використання його науково-технічного потенціалу.

Висновки:

1. З'ясовано, що усі стратегічні та тактичні дії щодо проектування та впровадження сучасних СЗІ вимагають системного аналізу проблеми, яка супроводжуються складними інформаційними процесами, більшість з яких мають конфіденційний характер.
2. Встановлено, що під ефективністю функціонування СЗІ розуміють інтенсивність її використання як активного засобу виконання операцій забезпечення конфіденційності оброблення, зберігання та передачі інформації. Комплексним показником оцінювання якості цих операцій виступає вироблене експертами оцінювальне судження відносно придатності заданого способу дій фахівців щодо захисту інформації, або пристосованість засобів захисту інформації до різних проявів джерел загроз.
3. Виявлено, що постановка задачі забезпечення безпеки СЗІ є не коректною, оскільки найчастіше не враховує її поведінку в нестандартних і екстремальних ситуаціях. Вплив невизначеності особливо відчутно проявляється в адаптованих, слабко організованих СЗІ, які є нестабільними через неповноту, неточність, не нормованість та низьку достовірність інформації, якою володіють фахівці з їх експлуатації.
4. Встановлено, що для вирішення теоретичних і прикладних проблем, пов'язаних з проектуванням сучасних СЗІ, потрібна цілеспрямована організація комплексу досліджень, які виконуватимуться у рамках державних програм і на єдиній концептуальній та методологічній основі, кінцевим результатом якої має бути узагальнена модель СЗІ.

5. Складність процесу прийняття управлінських рішень при проектуванні сучасних СЗІ для потреб структурних підрозділах МНС України, відсутність досконалого математичного апарату призводять до того, що при оцінювані якості її функціонування та виборі допустимих альтернатив можливо, а часто просто необхідно, використовувати і обробляти якісну експертну інформацію фахівців, які безпосередньо експлуатують такі системи.

Сташевский З.П., Грыцюк Ю.И. **Особенности проблемы синтеза систем защиты информации в структурных подразделениях МЧС Украины**

Рассмотрены особенности проблемы синтеза современной системы защиты информации (СЗИ), которую планируется внедрять в структурные подразделения МЧС Украины. Установлено, что современные СЗИ, будучи составной частью глобальных информационных систем, являются сложными техническими системами. Решения задачи анализа и синтеза СЗИ требует учета значительного количества методов оценивания качества их функционирования, то есть интенсивности ее использования как активного средства выполнения операции обеспечения конфиденциальности обработки, хранения и передачи информации. Комплексным показателем оценивания качества этих операций выступает выработанное экспертами оценивающее суждение относительно пригодности заданного способа действий специалистов относительно защиты информации, или приспособленность средств защиты информации к разным проявлениям источников угроз.

Ключевые слова: глобальная информационная система, проектирование системы защиты информации, конфиденциальность обработки информации, задачи анализа и синтеза, источники угроз, теория нечетких множеств и лингвистической переменной.

Stashevsky Z.P., Grycyuk Yu.I. **Features of problem of synthesis of systems security of information are in structural subdivisions of ministry of emergency measures of Ukraine**

The features of problem of synthesis of the modern systems security of information (SSI), which it is planned to inculcate in structural subdivisions of ministry of emergency measures of Ukraine are considered. It is set that modern SSI, being component part of the global informative systems, are the difficult technical systems. Requires the decision of task of analysis and synthesis of SSI account of far of methods of evaluation of quality of their functioning, that intensity of its use as active mean of implementation of operation of providing of confidentiality of treatment, storage and information transfer. Mine-out experts estimating judgement comes forward the complex index of evaluation of quality of these operations in relation to the fitness of the set method of actions of specialists in relation to a security of information, or adjusted of facilities of security of information to the different displays of sources of threats.

Keywords: global informative system, planning of the systems security of information, confidentiality of treatment of information, tasks of analysis and synthesis, sources of threats, theory of fuzzy sets and linguistic variable.

Література

1. Айзерман М.А. Выбор вариантов: основы теории / М.А. Айзерман, Ф.Т. Алескеров. – М. : Изд-во "Наука", 1990. – 432 с.

2. Алексеев А.В. Интеллектуальные системы принятия проектных решений / А.В. Алексеев, А.Н. Борисов, Э.Р. Вилюмс, Н.Н. Слядзь, С.А. Фомин. – Рига : Изд-во "Зинатне", 1997. – 246 с.

3. Арсеньев Ю.Н. Принятие решений. Интегрированные интеллектуальные системы : учебн. пособ. [для студ. ВУЗов] / Ю.Н. Арсеньев, С.И. Шелобаев, Т.Ю. Давыдова. – М. : Изд-во ЮНИТИ-ДАНА, 2003. – 424 с.

4. Бешелев С.Д. Математико-статистические методы экспертных оценок / С.Д. Бешелев, Ф.Г. Гурвич. – Изд. 2-ое, [перераб. и доп.]. – М. : Изд-во "Статистика", 1980. – 263 с.

5. Борисов А.Н. Принятие решения на основе нечетких моделей: примеры использования / А.Н. Борисов, О.А. Крумберг, И.П. Федоров. – Рига : Изд-во "Знание", 1990, 184 с.

6. Варфоломеев В.И. Принятие управленческих решений : учебн. пособ. [для студ. ВУЗов] / В.И. Варфоломеев, С.Н. Воробьев. – М. : Изд-во КУДИЦ-ОБРАЗ, 2001. – 422 с.

7. Гаврилова Т.А. Базы знаний интеллектуальных систем / Т.А. Гаврилова, В.Ф. Хорошевский. – СПб. : Изд-во "Питер", 2000. – 342.

8. Джексон П. Введение в экспертные системы : пер. с англ. : учебн. пособ. / П. Джексон. – М. : Изд-во "Вильяме", 2001. – 246 с.

9. Закон України "Про наукову і науково-технічну експертизу" (Відомості Верховної Ради України (ВВР), 1995, № 9, ст. 56). [Електронний ресурс]. – Доступний з http:// zakon2.rada.gov.ua/laws/show/51/95-вр

10. Згуровський М. З. Основи системного аналізу / М. З. Згуровский, Н. Д. Панкратова. – К. : Вид-ча гр. BHV, 2007. – 544 с.

11. Мирошников Б.Н. Борьба с киберпреступлениями – одна из составляющих информационной безопасности Российской Федерации. [Електронний ресурс]. – Доступний з http://www.crime-research.org/library/Mirosh1.html.

12. Нейлор К. Как построить свою экспертную систему / К. Нейлор. – М. : Энергоатомиздат, 1991. – 354 с.

13. Панкова Л.А. Организация экспертизы и анализ экспертной информации / Л.А. Панкова, А.М. Петровский, Н.В. Шнейдерман. – М. : Изд-во "Наука", 1984. – 214 с.

14. Попов Э.В. Экспертные системы: решение неформализованных задач в диалоге с ЭВМ. – М. : Изд-во "Наука", 1987. – 432 с.

15. Поспелов Д.А. Нечеткие множества в моделях управления и искусственного интеллекта / Д.А. Поспелов. – М. : Изд-во "Наука", 1986. – 312 с.

16. Судово-експертна діяльність: довідник для суддів. – Вид. 2-ге, [перероб. та доп.]. – К. : Вид. Дім "Ін Юре", 2003. – 908 с.

17. Таха Хемди А. Введение в исследование операций / Хемди А. Таха : пер. с англ. – М. : Изд. дом "Вильямс", 2005. – 912 с.

18. Черноруцкий И.Г. Методы оптимизации в теории управления / И.Г. Черноруцкий. – СПб. : Изд-во "Питер", 2004. – 324 с.

19. Экспертиза в современном мире: от знания к деятельности / под ред. Г.В. Иванченко, Д.А. Леонтьев. – М. : Изд-во "Смысл", 2006. – 456 с. [Електронний ресурс]. – Доступний з http://www.publishing.smysl.ru/annot.php?id_books=174.

20. Шиндер Д.Л. Киберпреступность: перед лицом проблемы / Д.Л. Шиндер. [Електронний ресурс]. – Доступний з http://www.crime-research.ru/library/cybercrimes3.html