3. *Табаков А.Б.* Разработка моделей оптимизации средств защиты информации для оценки страхования информационных рисков. // Научный журнал Кубанского государственного аграрного университета. – К. – 2009. - Вып. 2. – С. 14 – 18.

4. *Завгородний В.И.* Комплексная защита информации в компьютерных системах. – М. – 1994. – 86 с.

Запропоновано загальний формальний опис небезпечних для комплексної системи захисту інформації загроз в інформаційно-телекомунікаційних системах.

Ключові слова: комплексна система захисту інформації, загрози.

Предложено общее формальное описание опасных для комплексной системы защиты информации угроз в информационно-телекоммуникационных системах.

Ключевые слова: комплексная система защиты информации, угрозы.

Proposed general formal description of the dangerous for integrated system of information security, threats to information and telecommunication systems.

Key words: integrated system of information security, threats.

Надійшла 29.10.2009

УДК 004.681:681.3.06

Дмитренко О.П., д.т.н., проф. Хорошко В.О. (ДУІКТ)

ПОБУДОВА СТРУКТУРНОЇ МОДЕЛІ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ СИНТЕЗУ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Вступ

Комплекс заходів із забезпечення безпеки інформації в інформаційній системі (ІС) розглядається на трьох рівнях:

- правовому;
- організаційному;
- технічному.

На технічному рівні, який нас більш цікавить, забезпечення безпеки інформації у ІС виробляють підходи щодо застосування технічних і програмно-технічних засобів, які реалізують визначені вимоги із захисту інформації. Розглядаючи різні варіанти реалізації технічного рівня забезпечення безпеки інформації, слід враховувати такі аспекти:

- експлуатація та супроводження засобів блокування технічних каналів витоку інформації;
- керування доступом до інформації та механізмів, що реалізують послуги безпеки;
- перевірка і забезпечення цілісності критичних даних на на всіх стадіях їх обробки в ІС;
- резервне копіювання критичних даних, супроводження архівів даних і програмних засобів;
- відновлення роботи ІС після збоїв, відмов, насамперед систем із підвищеними вимогами до доступної інформації;
- захист програмних засабів окремих компонентів ІС і системи в цілому від несанкціонованого внесення доповнень і змін;
- забезпечення функціонування засобів контролю, у тому числі засобів виявлення технічних каналів витоку інформації.

Враховуючі аспекти захисту інформації при проектування комплексної системи захисту інформації (КСЗІ) формуються вимоги до системи, які поділяються на такі групи:

- вимоги щодо захисту від НСД (відповідно НДТЗІ 2.5-004-99);
- вимоги щодо захисту від витоку технічними каналами (відповідно НДТЗІ 2.5-005-99, НДТЗІ 2.5-008-02 та НДТЗІ 2.5-010-03).

З усього цього можна зробити один важливий висновок - без застосування спеціальних заходів захисту існуєдуже велика ймовірність пошкодження інформації в ІС.

Отже, задачі захисту інформації в ІС є суперпозицією задач, яку спробуємо вирішити у цій роботі.

Аналіз останніх досягнень та публікацій

В роботах [1-5] проведено системний аналіз суті проблеми захисту інформації, розглянуто достатньо повний перелік вимог і критеріїв, які можуть бути взяті за основу в ході оцінки ефективності засобів і заходів захисту інформації. Розроблена концепція профілю і проекту захисту.

Однак у зазначених роботах відсутнє вирішення задачі синтезу системи захисту інформації. Тут необхідно вирішити задачу встановлення відповідності цілям захисту, що виражені через вимоги, множини засобів і механізмів, які маються в нашому розпорядженні.

Мета роботи

Кроком до вирішення задачі синтезу комплексної системи захисту інформації (КСЗІ) є побудова спеціалізованої структурної моделі інформаційної системи (ІС).

Основна частина

Цільовий підхід, який прийнято в актемному аналізі передбачає, що структурна модель залежить не тільки від самої системи, алей від цілей, які стоять перед проектувальниками. Тому при вирішенні задачі синтезу КСЗІ необхідна побудова не довільної загальної універсальної моделі, а саме спеціалізованої структурної моделі, яка дає можливість ідентифікувати можливі загрози і здійснювати побудову відповідних систем захисту.

З іншої сторони, аналіз загроз за критеріями цілісності, доступності конфіденційності, спостереженості [6] показує неможливість їх опису на довільному одному рівні структуризації. Якісь загрози можуть бути ідентифіковані тільки при розгляді ІС в цілому (рівень архітектури), якісь при розгляді окремих підсистем і окремих функцій. Таким чином, багаторівневій системі загроз повинна відповідати багаторівнева модель ІС.

Відповідно [7] одна з можливих моделей ІС включає чотири складових:

1. Інформаційне середовище (ІСр);
2. Технологічне середовище (ТСр);
3. Користувацьке середовище (КСр);
4. Робоче середовище (РСр).

Розглянемо побудову спеціалазованої структурної моделі на прикладі технологічного середовища, як найбільш складного і обширного середовища, яке підлягає захисту.

Технологічне середовище - сукупність програмно-апаратних засобів обробки інформації, які викконують функції створення, відображення, зберігання і передачі інформації.

Структурно вся інформаційна система S і кожна з її підсистем можуть бути описані в наступному вигляді:

$$S = I\{S_i\},\ i=0,1,K\,k \qquad (1)$$

де функція I - множина інформації, яка описує інформаційну систему як цілісну систему , що складається із S_i ;

S_i - множина підсистеми S.

Люба підсистема S_i знову ж може бути представлена і вигляді:

$$S = I\{S_{ij}\},\ i=0,1,Kl \qquad (2)$$

де функція I_i - множина інформації, яка описує підсистемі S_i як цілісну систему, що складається із S_{ij} ;

S_{ij} - множина підсистеми S_i.

Цей процес структуризації повинен продовжуватися до тих пір, поки на деякому кроці множина підсистеми $S_{ij...k}$ не виявиться пустою.

Дану структуризацію можна уявити у вигляді графу, де вузол описується двома параметрами (I_{ijKk}, S_{ijKk}), а звязки - матрицею суміжності.

У відповідності з (1), (2), структурну модель технологічного середовища (ТС) опишемо у вигляді:

$$TC = \{I^T, MT\}$$

де I^T - множина інформацій, яка описує технологічне середовище як цілісну систему;

MT - множина складових технологічного середовища.

Множина *MT* може бути описана у вигляді:

$$MT = \{T_i, i \in I^T\}$$

де: T_i - територіально-локалізовані складові технологічного середовища.

Множина T_i може бути иописана у вигляді:

$$T_i = \{A_i, P_i\}$$

де A_i - множина апаратних засобів, *i*-ого ТС;

P_i - множина програмних засобів, *i*-ого ТС.

Множина A_i може бути описана у вигляді

5.

$$A_i = \{I_i^A, \{O_i, P_{ri}, C_i, t_{ri}, D_i\}\}$$

де I_i^A -множина інформації, яка описує апаратні засоби *i*-ого ТС як єдине ціле;

O_i - множина засобів створення і обробки інформації;

P_{ri} - множина засобів відображення і опису інформації;

C_i - множина засобів управління інформацією;

t_{ri} - множина засобів передачі інформації;

D_i - множина засобів збереження інформації.

Множини O_i можуть бути інтерпретовані як множини комп'ютерів даного ТС.

Множина P_{ri} може бути описана у вигляді

$$P_{ri} = \{Dis_i, Din_i, \Pr int_i, Pl\}$$

де Dis_i - множина дисплеїв даного ТС;

Din_i - множина динаміків даного ТС;

$Print_i$ - множина принтерів даного ТС;

Pl_i - множина плотерів даного ТС

Множина C_i може бути описана у вигляді:

$$C_i = \{Pc_i, M_i, Km_i\}$$

де Pc_i - множина можливих пультів управління;

M_i - множина маршрутизаторів;

Km_i - множина комутаторів.

Множина t_{ri} може бути описана у вигляді:

$$t_{ri} = \{Kн_i, md_i, \text{int}_i, K_{Ti}\}$$

де $Kн_i$ -множина каналів зв'язку;
md - множина модемів;
int_i - множина інтерфейсів;
K_{Ti} - множина концентраторів.

Множина D_i може бути описана у виді

$$D_i = \{d_i, bnf_i, op_i\}$$

де d_i - множина довгочасно запам'ятовуючих пристроїв;
op_i - множина оперативно запам'ятовуючих пристроїв;
bnf_i - множина буферних накопичувачів.

При необхідності деталізація запропонованих структур може бути продовжена. Множина програмних засобів *i*-ого ТС може бути описана у вигляді

$$P_i = \{I_i^p, \{F_i, S_i, N_i\}\}$$

де I_i^p - множина інформації, яка описує програмні засоби і-ого ТС як цілісної системи;
F_I - множина функціональних програм;
S_I -системне програмне забезпечення;
N_I - мережне програмне забезпечення.

Множина F_i може бути описана у вигляді

$$F_i = \{F_i^i, F_i^o, F_i^p, F_i^g, F_i^3\}$$

де F_i^i - множина функціональних програм які виконують інформаційні функції;
F_i^0 - множина функціональних програм , які можуть виконувати функції обробки інформації;
F_i^P - множина функціональних програм , які можуть виконувати функції представлення інформації;
F_i^g - множина функціональних програм , які можуть обробляти графічну інформацію;
F_i^3 - множина функціональних програм , які можуть обробляти звукову інформацію.

Множина S_i може бути описана у вигляді

$$S_i = \{S_i^{on}, S_i^c, S_i^d, S_i^t\}$$

де S_i^{on} -операційні системи АРМ;
S_i^c — множина СУБД і-ого ТС;
S_i^d - множина програмних засобів захисту інформації;
S_i^t - множина програмних засобів сервісного обслуговування і тестування.

Множина N_i може бути описана у вигляді:

$$N_i = \{C_i^l, M_i^p, B_i^p, dp_i, N_i^E, N_i^d\}$$

де C_i^1 - Множина протоколів управління лінією передачі даних;
M_i^p - множина протоколів маршрутизації;
B_i^p — множина протоколів буферизації;
Dp_i — множина протоколів диспетчерського управління (управління режимами функціонування мережі);
N_i^E - МНожина протоколів міжмережевої взаємодії, (протоколи взаємодії через шлюзи у зв'язку з несумісністю довільних мереж);
N_i^d - міжмережеві протоколи захисту інформації.

Подальша деталізація складових програмного забезпечення можлива тільки у вигляді обширних каталогів.

Графова модель буде мати вигляд: (рис 1).

Користувацьке середовище — сукупність організацій та фізичних осіб, діяльність яких повязана з функціонуванням інформаційного середовища.

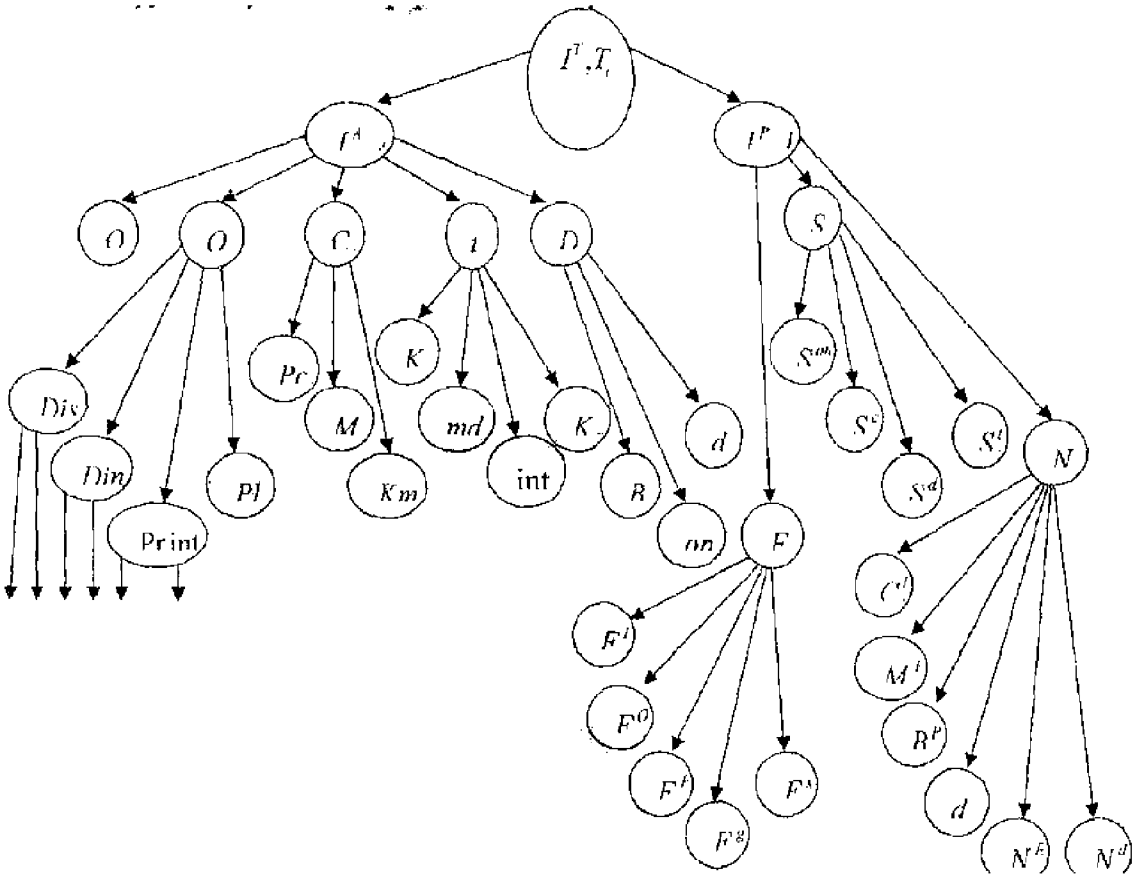

Рис.1. Графова модель

Аналогічним чином можуть бути структуровані інформаційне, користувацька та робоче середовище.

Інформаційне середовище — сукупність розміщених на різних носіях інформаційних ресурсів, які обробляються за допомогою відповідних засобів технологічного середовища.

Складові інформаційного середовища: В і - бази даних, К і - каталоги, Ф і - файли і-го рівня ієрархії.

З наведених міркувань можна зробити висновок, що спеціалізована структурна модель інформаційної системи може бути описана в наступному вигляді:

$$S = \{IC, TC, KC, PC\} = \{B, K, \Phi, O, P_r, C, t_r, D, F, S, N, B_T, B_H, T_P, K_{TP}\} =$$

$$= \{B, K, \Phi, O, D_{is}, D_{in}, P_{r\,\mathrm{int}}, P_l, P_c, M, K_m, K_н md, \mathbf{int}, K_T, d, bnf, op, F^i, F^o, F^p, F^g, F^3, S^{on}$$

$$S^c, S^d, S^t, C^l, M^p, B^p, dp, N^E, N^d, T, A, O_n, C_{on}, П, E, P, B_3, O_i, T_p, T_{TP}, П_M, K_n\} \quad (3)$$

Висновки

Дана структуризація не є єдиною. У зв'язку зі складністю задачі важливо мати декілька типових моделей структуризації при чому кожна може використовуватися неодноразово при різних вихідних даних.

Можна, наприклад, розглядати ІС для оцінки впливу загроз на інформаційні ресурси в наступних розрізах:

1. ІС як цілісна система — на цьому рівні розглядаються загрози, пов'язані з недостатньою надійністю архітектури ІС, або з не відповідністю її стандартам і вимогам по створенню і експлуатації ІС;

2. ІС як множина функціональних підсистем - на цьому рівні можуть розглядатися загрози, які пов'язані з невиконанням вимог до окремих підсистем, наприклад, вимоги використовувати тільки сертифіковані засоби криптографічного захисту для підсистем криптографічного захисту;

3. ІС як множина територіально-розподілених локальних середовищ, де під локальним середовищем розуміється локально в фізичному (географічному) смислі розташована частина функціонально взаємопов'язаних програмно-апаратних засобів ІС. На цьому рівні можуть розглядатися загрози, які пов'язані з недостатньою захищеністю будівель (від пожарів, від проникнення сторонніх і т.д.), де розташовані відповідні локальні середовища, або з недостатньою захищеністю телекомунікацій, які зв'язують локальні середовища між собою;

4. ІС як множина локальних інформаційних засобів, які використовуються в ній. На цьому рівні можуть розглядатися загрози, які пов'язані з неповною відповідністю того чи іншого програмно-апаратного засобу вимогам типових профілів захисту для відповідного класу інформаційних засобів, визначених в таких документах як[8,9].

5. ІС як множина виконуваних нею або з використанням її інформаційних засобів, функцій - на цьому рівні можуть бути виявлені такі загрози як наявність можливостей нерегламентованого використання функцій інформаційної системи;

6. ІС як множина складових її інформаційних об'єктів, де під інформаційним об'єктом розуміється люба частина інформаційних ресурсів, які входять до аналізуємої інформаційної системи. На цьому рівні можуть розглядатися загрози, які пов'язані з можливістю неявної компрометації інформаційних об'єктів типу криптографічних ключів.

Список літератури

1. Антонюк А.А. - Аналіз складу профілів захищеності інформації / Антонюк А.А., Берестов Д.С., Пустовіт С.М. // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. - 2005, №10. - С. 46-51.

2. Кудин А.М. - Количественные оценкикачества функционирования системы защиты информации / Кудин А.М., Корольков В.Н. // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. - 2005, №11. - С. 35-37.

3. Антонюк А.А. - Моделювання доступу та каналів витоку в інформаційних системах / Антонюк А.А., Жора В.М. // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. - 2001, №3. - С. 156-160.

4. Герасименко В.А. - защита информации в автоматизированых системах обработки данных / Герасименко В,А, - М.: Энергоатомиздат, 1994. - т.т. 1,2.

5. Бєлошапкін В.К. - Побудова спеціалізованої структурної моделі інформаційної системи з метою синтезу комплексної системи захисту інформації / Бєлошапкін В.К., Пустовіт С.М., Степанов В.Д. // Захист інформації. - 2005, №3. - С. 78-83.

6. Критерії оцінки захищеності інформації в компютерних системах від несанкціонованого доступу. НД ТЗІ 2.5 - 004 - 99.

7. Загальні положення щодо захисту інформації в компютерних системах від несанкціонованого доступу. НД ТЗІ 1.1 - 002 - 99.

8. Класифікація авттоматизованих систем і стандартні функціональні профілі захищеності обробленої інформації від несанкціонованого доступу. НД ТЗІ 2.5 - 003 - 99.

9. Ленков С.В. - Методы и средства защиты информации / Ленков С.В, Перегудов Д.А., Хорошко В.А. - К.: Арий, 2008. -т.т. 1,2.

У даній роботі побудовано спеціалізовану структурну модель інформаційної системи для вирішення задачі синтезу комплексної системи захисту інформації.

Ключові слова: структурна модель, інформаційна система.

В работе построена специализированная структурная модель информационной системы для решения задачи синтеза комплексной системы защиты информации.

Ключевые слова: структурная модель, информационная система.

The specialized structural model of information system for the solution of synthesis task of complex data security system has been built in the paper.

Key words: structural model, information system.

Надійшла 29.11.2009