відповідної РОМ та сукупність потрібних засобів захисту від інформаційних об'єктів від можливих загроз із середовища РОМ.

1. *Василенко В.С.* Класифікація та моделювання загроз в розподілених мережах. // К.: Моделювання та інформаційні технології. Збірка наукових праць ІПМЕ ім. Г.Є. Пухова НАН України. - К.: ІПМЕ, 2007. – Вип.. 39 – С. 98– 103.
2. *Василенко В.С.* Оцінка та моделювання загроз в розподілених мережах. Загрози селекції та модифікації інформації. // К.: Моделювання та інформаційні технології. Збірка наукових праць ІПМЕ ім. Г.Є. Пухова НАН України. - К.: ІПМЕ, 2007. – Вип.. 40 – С. 142 – 146.
3. *Василенко В.С.* Оцінка та моделювання загроз в розподілених мережах. Типові атаки в розподілених мережах. // К.: Моделювання та інформаційні технології. Збірка наукових праць ІПМЕ ім. Г.Є. Пухова НАН України. - К.: ІПМЕ, 2007. – Вип.. 40 – С. 108 – 115.
4. TCP під прицілом (http://www.hackzone. ru/articles/tcp.html);
5. Деякі проблеми FTP (http://www. hackzone.ru /articles/ftp.html);
6. Атака на DNS або нічний кошмар мережного адміністратора (http://www.hackzone.ru/articles/dn s−poison.html);
7. *Медведовский И.Д. Семьянов П.В. Леонов Д.Г.* "Атака на Інтернет" М.: Видавництво ДВК 1999;
8. *Соболев К.И.* Дослідження системи безпеки з Windows NT 4.0 HackZone: Територія злому. № 1−2, 1998.
9. Переповнення буфера в WIN32 (http://www.void.ru/stat/9907/20.html).
10. Теорія й практика атак FORMAT STRING http://www.void.ru/stat/0102/27.html+http://www.void. ru/stat/0102/28.html);
11. Перехоплення пакетів TCP: Захист від флуда (http://www.void. ru/stat/9907/19.html).

Поступила 25.02.2010р.

УДК 681

С. М. Головань, А.М. Давиденко, Л.М. Щербак

КОНЦЕПЦІЯ ЕКСПЕРТИЗИ У СФЕРІ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

It is shown in work, that conception of examination of defence of information with the limited access is based on the results of analysis of examination on the objects of informative activity, it is suggested to examine in the sphere of information with the limited access in three stages.

Вступ

Захист інформації з обмеженим доступом в інформаційних системах, мережах, приміщеннях, інженерно-технічних спорудах є невід'ємною

складовою частиною конкретного об’єкта інформаційної діяльності, що поєднує організаційні та інженерні заходи, програмні й технічні засоби, призначені для попередження навмисних дій блокування інформації, забезпечення таких критеріїв безпеки інформаційних технологій як: конфіденційність, цілісність, доступність, обліковість, достовірність та надійність [1-2]. Збільшення кількості процедур, методів, інструментальних засобів, що застосовуються з метою оцінки захищеності інформації, обумовлено використанням сучасних інформаційних технологій. У даній роботі розглянуті питання аналізу задач та побудови моделі експертизи у сфері технічного захисту інформації з обмеженим доступом. Це дає можливість проведення експертизи, забезпечує оцінку ефективності заходів технічного захисту інформації з обмеженим доступом та підготовки обґрунтованих висновків для прийняття відповідних рішень.

Аналіз задач експертизи у сфері технічного захисту інформації з обмеженим доступом на об’єктах інформаційної діяльності

Відсутність формалізованих моделей і методів роблять процедуру експертизи трудомісткою та затратною, внаслідок чого стримується широке її впровадження у оцінку ефективності заходів технічного захисту інформації з обмеженим доступом на об’єктах інформаційної діяльності. У ряді випадків така експертиза проводиться іноді не в повному обсязі і без належного обґрунтування отриманих результатів. Таке положення викликано відсутністю науково обґрунтованих методик розв’язання всього комплексу задач, пов’язаних з експертизою.

Вибір засобів захисту відповідно до проблем та загроз безпеці можна використовувати таким чином.

Перший крок – визначити вимоги та оцінити забезпечення таких критеріїв безпеки інформаційних технологій як: конфіденційність, цілісність, доступність, обліковість, достовірність та надійність. Кількість вибраних засобів захисту має відповідати оціненим проблемам безпеки.

Другий – для кожної проблеми визначаються типові загрози і для кожної загрози пропонуються засоби захисту.

Значимість проблем безпеки може бути оцінена залежно від того, чи порушення безпеки спричинює серйозні ушкодження ділової діяльності, або ж тільки завдає малої шкоди, чи не впливає зовсім.

Якщо інформація, оброблена системою, є різнотипною, різні її типи можуть вимагати окремого розгляду. Захист, що надається об’єкту інформаційної діяльності, має бути достатнім для всіх типів оброблюваної інформації. Таким чином, якщо інформація потребує високого рівня безпеки, весь об’єкт треба захищати належним чином. У випадку, якщо кількість інформації з великими потребами безпеки незначна, є сенс розглянути перенесення цієї інформації на інший об’єкт, якщо це не заважає діловим процесам.

Згідно з визначеннями нормативних документів системи технічного захисту інформації в Україні експертиза – це процедура оцінки захищеності

інформації з обмеженим доступом, яка обробляється або циркулює на об'єктах інформаційної діяльності, а проведення призначені для експериментального визначення кількісних та якісних характеристик для підготовки обґрунтованих висновків та прийняття відповідних рішень [3]. Однак вимоги до експертизи носять суб'єктивний характер, оскільки вони формуються замовником та виконавцем який є ліцензіатом, регламентуються відповідно до положень укладеного між ними договором, а їх висновки можуть призвести до того, що один й той самий висновок різними суб'єктами може трактуватися по різному, декілька висновків можуть бути необґрунтовано об'єднані в один (об'єднання висновків) тощо. Тому експертиза, яка базується на таких вимогах зазнає впливу суб'єктивних факторів, а це може призвести до некоректних висновків щодо її результатів, які можуть бути як підтверджені, так і спростовані, або не визнані якоюсь із сторін.

Пропонується проводити експертизу у сфері технічного захисту інформації з обмеженим доступом на базі формалізованої моделі, яка будується разом з замовником експертизи на основі формалізованих методів. При цьому виникає ряд задач, вирішення яких потребує теоретичних досліджень та розробку методів їх практичного розв'язання. Основними із цих задач є:

– формалізація та розробка методів побудови моделі експертизи, яка б була обґрунтованою і конструктивною;

– створення працездатної методики експертизи;

– трудомісткість робіт пов'язаних із виданням "Експертного висновку" або "Атестата відповідності".

За результатами проведених робіт організатор складає "Експертний висновок" щодо відповідності об'єкта експертизи нормативних документів системи технічного захисту інформації з обмеженим доступом, підписує його і подає до Департаменту де він розглядається Експертною радою і в разі затвердження результатів експертизи реєструється та видається замовнику.

На підставі позитивного рішення щодо експертизи комплексної системи захисту інформації з обмеженим доступом замовнику видається зареєстрований "Атестат відповідності", який підписується керівником (заступником керівника) Департаменту.

Для проведення експертизи у сфері технічного захисту інформації з обмеженим доступом пропонується технологічна схема процедури експертизи у сфері технічного захисту інформації з обмеженим доступом на об'єкті інформаційної діяльності, яка має вигляд, наведений на рисунку 1.

Побудови моделі експертизи у сфері технічного захисту інформації з обмеженим доступом на об'єкті інформаційної діяльності

Концепція побудови моделі експертизи визначає систему відображень для переходу від моделі вимог до моделі експертизи і складається з наступних етапів:

– ґрунтуючись на вимогах до експертизи у сфері технічного захисту інформації з обмеженим доступом будуємо нормативну модель вимог шляхом об'єднання функціональних і не функціональних вимог та обмежень. Нормативна модель вимог, у першу чергу, залежить від набору вимог замовника щодо проведення експертизи;

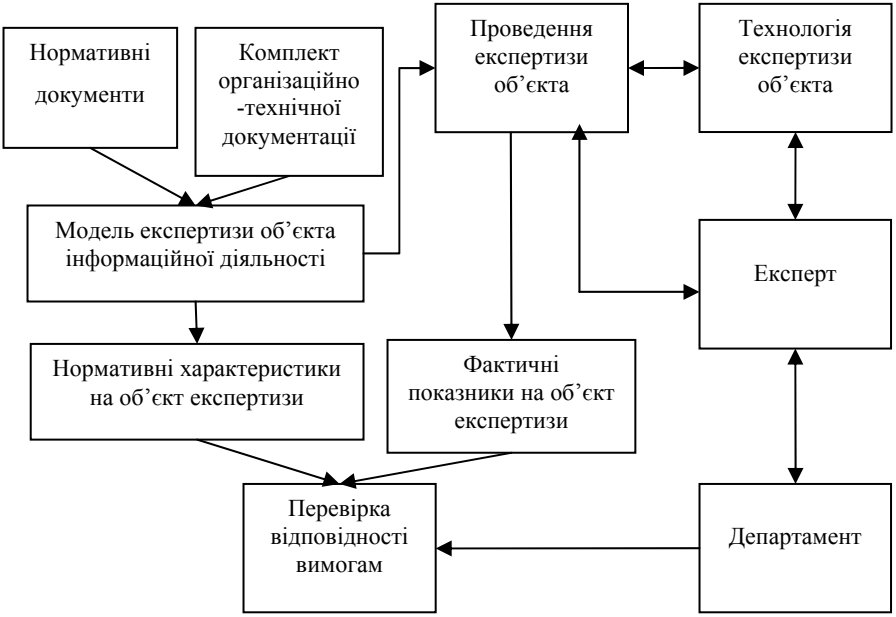

Рис. 1. Технологічна схема процедури експертизи у сфері технічного захисту інформації з обмеженим доступом на об'єкті інформаційної діяльності

– на основі аналізу нормативних документів системи технічного захисту інформації з обмеженим доступом вибираємо найбільш повну оцінку захищеності інформації з обмеженим доступом, яка обробляється або циркулює на об'єктах інформаційної діяльності, з поділом характеристик на критичні та другорядні;

– здійснюємо відображення нормативної моделі вимог на загальну модель експертизи з вибіркою характеристик оцінки захищеності інформації з обмеженим доступом, яка обробляється або циркулює на об'єктах інформаційної діяльності. Сукупність вибраних елементів загальної і нормативної моделей складе модель експертизи, у якій відповідність атрибутів вимогам залежить від задоволення обмежень.

На першому етапі будуємо нормативну модель, виходячи з вимог замовника експертизи та нормативних документів системи технічного захисту інформації з обмеженим доступом:

$$V = \left\{ \left\{ x_i, y_j, B_{x_k}, u_a \right\}, i \in I_1 \cup J_1, j \in I_2, k \in I_3 \cup J_2, a \in J_3 \right\}, \quad (1)$$

де V – множина вимог, які містять функціональні вимоги $x_i, x_i \in X, i \in I_1 \cup J_1$, не функціональні вимоги $y_j, y_j \in Y, j \in I_2$, обмеження на функціональні вимоги $B_{x_k}, B_{x_k} \in B, k \in I_3 \cup J_2$ та нормативні документи на виконання операцій $u_a, u_a \in U, a \in J_3$ (множина індексів I відповідають вимогам замовника, а множина J – вимогам предметного середовища).

На другому етапі концепція передбачає побудову загальної моделі експертизи відповідно до нормативних документів технічного захисту інформації з обмеженим доступом. Але з метою спрощення моделі, пропонується, по-перше, ввести в модель тільки критичні характеристики (конфіденційність, цілісність, доступність, обліковість, достовірність та надійність і відображення необхідних вимог замовника та нормативних документів системи технічного захисту інформації з обмеженим доступом), а, по-друге – необхідні другорядні характеристики.

Загальна модель експертизи у сфері технічного захисту інформації з обмеженим доступом відповідно до нормативних документів можна записати у такому вигляді:

$$Q_G = \left\{ C_i \left\{ S_{ij} \left\{ A_{ijk} \left\{ E_{ijkl}, M_{ijkl}, W_{ijkl} \right\}_{l=1}^{L_{ijk}} \right\}_{k=1}^{K_{ij}} \right\}_{j=1}^{J_i} \right\}_{i=1}^{I}, \quad (2)$$

де C_i – i -та характеристика;

S_{ij} – j -та під характеристика i -ї характеристики;

A_{ijk} – k -й атрибут j -ї під характеристики i -ї характеристики захищеності.

Для того щоб модель (2) була завершеною, необхідно вибрати метрики M_{ijkl} вимірювання елементів атрибутів під характеристик E_{ijkl}, та вагомі коефіцієнти W_{ijkl}. Атрибути і елементи атрибутів пропонується виділяти з нормативних документів системи технічного захисту інформації з обмеженим доступом [4].

Третій етап полягає у відображенні моделі (1) на модель (2) із класифікацією вимог і сполучення атрибутів. Класифікаціям вимог проводиться відображення сформульованої вимоги V_i з моделі (1) у адекватну їй характеристики з моделі (2).

Висновки

В роботі показано, що концепція експертизи захисту інформації з обмеженим доступом базується на результатах аналізу експертизи на об'єктах інформаційної діяльності, запропоновано проводити експертизу в сфері інформації з обмеженим доступом у три етапи:

– на першому етапі створюється нормативна модель;

– на другому – загальна модель;

– на третьому –відображення нормативної моделі на загальну модель з класифікацією вимог і сполучення атрибутів.

1. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1-002-99. – Офіц. вид. – К. : НікС : Департамент спеціальних телекомунікаційних систем та захисту інфор-мації Служби безпеки України, 1999. – III. 15 с. (Нормативний документ системи технічного захисту інформації).
2. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 2.5-004-99. – Офіц. вид. – К. : НікС : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. – IV. 53 с. (Нормативний документ системи технічного захисту інформації).
3. Положення про державну експертизу у сфері технічного захисту інформації. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 29 грудня 1999 року № 62. Зареєстровано в міністерстві юстиції України 24 січня 2000 р. за № 40/4261.
4. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій : ДСТУ ISO/IEC TR 13335-3:2003. – [Чинний від 2004 – 10 – 01]. – К. : Держспоживстандарт України, 2005. – V. 42 с. – (Національний стандарт України).

Поступила 8.02.2010р.

УДК 004.021:334.722.1(045)

С.В. Карпенко, О. П.Ткалич, П. А. Андрухович

СЕРВИС-ОРИЕНТИРОВАННАЯ АРХИТЕКТУРА И АРХИТЕКТУРА, УПРАВЛЯЕМАЯ МОДЕЛЯМИ

In the article the service-oriented architecture (SOA) manageable with the help of the models is described. The main concepts of SOA are discussed. The main aspects and advantages of implementation of SOA in organizations of different types are shown. In comparison the Model-driven architecture concepts of creation of organization model are described.

Необходимость интеграции и взаимодействия приложений в рамках совокупности большого количества информационных систем (ИС) предприятия (или нескольких предприятий), оказывают существенное влияние на используемые программные архитектуры. Прежде всего, это сервисная модель взаимодействия между приложениями общей системы в рамках так называемой сервис-ориентированной архитектуры (Service-

