УДК 681.31

Студент Рибачек Н.І.

**Національний технічний університет України
«Київський політехнічний інститут»**

АНАЛІЗ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Abstract

Natalia Rybachek, student

Information system protection analysis

This paper concerns the method of systematization and expert knowledge representation about the requirements that are pulled out to the complex systems of the protection of information. Presently estimation of level of object informative protection, his comparison with an objectively necessary level, and in the case of their disparity - the selection of optimum complex of facilities and measures on the increase of informative safety is an intricate scientific problem, that requires the presence of thorough subject knowledge and practical experience. Given approach can be taken for these purposes.

Вступ

Питання безпеки інформації – важлива частина процесу упровадження нових інформаційних технологій у всі сфери життя суспільства. Широкомасштабне використання обчислювальної техніки і телекомунікаційних систем у ІС, перехід на цій основі до безпаперової технології, збільшення об'ємів оброблюваної інформації і розширення кола користувачів призводять до якісно нових можливостей несанкціонованого доступу до ресурсів і даних інформаційної системи, до їх високої уразливості. Саме тому виникає необхідність систематичного проведення аудиту інформаційної безпеки [1].

В даній статі пропонується методика, що дозволяє провести аналіз захищеності інформаційної системи [2].

Постановка задачі

Задача полягає у розробці методики, що дозволить провести повний аналіз і оцінку захищеності інформаційної системи (ІС) та виявити її слабкі місця. Спираючись на отримані дані можна буде сформулювати потребу у засобах захисту ІС.

Методика систематизації та представлення експертних знань про вимоги, що висуваються до комплексних систем захисту інформації (КСЗІ)

Комплексна система захисту інформації (КСЗІ) представляє собою сукупність організаційних та інженерно-технічних засобів спрямованих на забезпечення захисту інформації від розголошування, витоку та несанкціонованого доступу.

Модель КСЗІ представляється у вигляді наступних основних блоків показників: блок показників "Основи", блок показників "Напрями", блок показників "Етапи" [2].

Блок показників "Основи" (O_i)

Основою або складовими частинами практично будь-якої системи, у тому числі системи захисту інформації є: законодавча, нормативно-правова і наукова база; структура і задачі органів (підрозділів), що забезпечують безпеку ІТ; організаційно-технічні і режимні заходи (політика інформаційної безпеки); програмно-технічні засоби [3].

На базі цих частин можна сформулювати наступні показники:

1. О1 – якість нормативно-правової і наукової бази;
2. О2 – повнота структури і задач органів, що забезпечують захист;
3. О3 – якість організаційних заходів і методів захисту інформації (політика безпеки);
4. О4 – якість програмно-технічних засобів захисту.

Блок показників "Напрями" (H_j)

Можна виділити наступні основні напрями створення і оцінки КСЗІ: об’єкти; процеси; канали зв’язку; випромінювання; елементи захисту [3].

У відповідність з цими напрямами виділяють наступні показники:

1. H_1 – рівень захисту об’єктів ІС;
2. H_2 – рівень захисту процесів, процедур и програм обробки інформації;
3. H_3 – рівень захисту каналів зв’язку;
4. H_4 – рівень приглушення електромагнітного випромінювання;
5. H_5 – якість керування системою захисту.

Очевидно, що кожній з показників даного блоку має бути деталізований в залежності від структури ІС.

Блок показників "Етапи" (M_k)

На сьогоднішній день існують різні етапи побудови КСЗІ, всі вони достатньо ефективні і дозволяють вирішувати поставлені задачі. Розглянемо наступні етапи створення КСЗІ, що підлягають оцінці: визначення інформаційних і технічних ресурсів, а також об'єктів ІС, що підлягають захисту; виявлення повної множини потенційно можливих загроз і каналів просочування інформації; проведення оцінки уразливості і ризиків інформації (ресурсів ІС) при наявній множині загроз і каналів витоку; визначення вимог до системи захисту інформації; здійснення вибору засобів захисту інформації і їх характеристик; упровадження і організація використання вибраних заходів і засобів захисту; здійснення контролю цілісності і управління системою захисту [3].

Представимо вказані етапи у вигляді показників:

1. M_1 - повнота визначення інформації, що підлягає захисту;
2. M_2 - повнота виявлення множини потенційно можливих загроз і каналів просочування інформації;
3. M_3 - якість проведення оцінки уразливості і ризиків інформації при наявній множині загроз і каналів витоку;
4. M_4 - якість визначення вимог до системи захисту;
5. M_5 - якість вибору засобів захисту інформації і їх характеристик;
6. M_6 - рівень упровадження і організація використання вибраних заходів і засобів захисту;
7. M_7 - якість контролю цілісності і управління системою захисту.

Етапи можуть бути розбиті на більш детальні пункти (кроки).

Формування моделі КСЗІ

Структура формування моделі оцінки КСЗІ полягає у логічному об’єднанні показників вищеописаних блоків "Основи", "Напрями" і "Етапи" у матрицю знань, що складається з k елементів.

У загальному випадку кількість елементів матриці знань може бути визначено з формули:

$$k = O_i * H_j * M_k,$$

де k – кількість елементів матриці;

O_i – кількість складових блоку "Основи";

H_j – кількість складових блоку "Напрями";

M_k – кількість складових блоку "Етапи".

На основі проведеного вище аналізу в даному варіанті (за умови, що O_i=4, H_j=5, M_k=7) загальна кількість елементів матриці знань складає

$$k = 4*5*7 = 140.$$

Слід звернути увагу на зміст позначення кожного з елементів матриці.

Для прикладу розглянемо зміст елементу матриці № 321, який об'єднує показник № 3 блоки "Етапи", показник № 2 блоки "Напрями" і показник № 1 блоки "Основи".

Елемент із значенням індексів 321 характеризує, наскільки повно відображені в законодавчих, нормативних і методичних документах питання, що визначають порядок проведення оцінки уразливості і ризиків для інформації, що використовується в процесах і програмах конкретної ІС.

В нашому випадку для матриці знань формується 140 питань (по числу її елементів). Зміст кожного з елементів матриці описує взаємозв'язок складових у КСЗІ. Сформулювавши відповіді на всі питання можна скласти повне уявлення про КСЗІ і оцінити рівень захисту, який вона забезпечить.

Крім того, використання матриці дозволяє вирішувати комплекс питань по створенню і оцінці КСЗІ шляхом аналізу різних груп елементів матриці, залежно від вирішуваних задач [2].

Висновки

Запропонована методика дозволяє провести повний аналіз і оцінку захищеності інформаційної системи і виявити потребу у засобах її захисту, що значно прискорить і полегшить процес аналізу захищеності.

У порівнянні з іншими існуючими засобами та методиками, дана методика є більш ефективною, так як вона дозволяє оцінювати не тільки окремі складові КСЗІ, але і їх взаємозв'язок [4].

Література

1. Замятін Д., Прокофьєв М. Алгоритмічні особливості експертних систем, орієнтованих на поблеми захисту інформації // Інтернет ресурс: http://bezpeka.com/
2. Домарев В. В. Безопасность информационных технологий. Системный подход — К.: ООО ТИД Диа Софт, 2004. — 992 с.
3. ГОСТ Р ИСО/МЭК 17799 – «Информационные технологии. Методы безопасности. Руководство по управлению безопасностью информации». Прямое применение международного стандарта с дополнением – ISO/IEC 17799:2005.
4. Снігерьов О.П., Кухарьонок М.А. Визначення можливих загроз інформації в автоматизованих системах // Інтернет ресурс: http://bezpeka.com/