УДК 004.056

М.В. ЗАХАРОВА

Черкаський державний технологічний університет

МЕТОДИКА ПОБУДОВИ СИСТЕМИ ОЦІНКИ ЗАХИЩЕНОСТІ ІС З УРАХУВАННЯМ ІНТЕНСИВНОСТЕЙ АТАК

Запропонована методика дозволяє вирішити задачу підвищення рівня захищеності інформаційної системи (ІС) та її ресурсів, враховує зміну інтенсивностей потоків атак при застосуванні засобів захисту. Основними етапами оцінки захищеності ІС є аналіз структури та визначення особливостей ІС, визначення множини атак та вразливих ресурсів, імовірнісних характеристик потоку атак та визначення інтенсивності порушення безпеки ІС.

Ключові слова: *інформаційна система, атака, система захисту.*

У сучасній динамічній обстановці виникають проблеми, зв'язані з підвищенням захищеності інформаційних систем (ІС). Очевидно, що без достатнього інформаційного забезпечення неможливо приймати правильні рішення, що безпосередньо впливають на долю підприємства або організації, на його розвиток і життєздатність. Обстановка постійно змінюється, число рішень росте, їхні наслідки усе складніше прогнозувати, а ціна втрат з кожним днем підвищується. Тому саме інформаційні ресурси є незамінним продуктом для вироблення будь-якого рішення, таким же продуктом, який необхідно добути, переробити і поставити до закінчення терміну придатності. Усе це визначає необхідність впровадження складних систем збору, обробки й аналізу різної інформації. Коштовні зведення, що добуваються на превелику силу, повинні вчасно надійти тому, кому вони необхідні, оскільки інформація корисна тільки тоді, коли її можна використовувати для прийняття серйозних рішень. Тому проблема забезпечення безпеки ІС та її ресурсів є однією з найважливіших на сучасному етапі розвитку інформаційних технологій. Можливість використання різних варіантів побудови інформаційних систем приводить до необхідності створення різних систем захисту, що враховують індивідуальні властивості кожної з інформаційних систем.

У деяких публікаціях щодо проектування систем захисту ІС, розробки та використання сучасних засобів захисту ІС є досить повно обґрунтовані об'єктивні часткові задачі по забезпеченню ефективного захисту ІС і представлені раціональні шляхи їхнього вирішення, розглядаються основні методи підвищення захищеності ІС та її ресурсів. Але відсутня єдина концепція захисту ІС, є розходження основних термінів і визначень, класифікації об'єктів захисту, не враховані функціональне призначення та особливості ІС.

Метою даної роботи з розробка методики побудови системи оцінки захищеності ІС з урахуванням інтенсивностей атак. Оцінка захищеності – процес встановлення відповідності між результатом захисту і поставленою метою. Із зростанням складності об'єктів аналізу, складу і характеристик загроз завдання кількісної оцінки захищеності актуальне.

Оцінка ефективності захисту можлива на основі порівняння значення показника захищеності з нормативним значенням і на основі порівняння показників захищеності інформації без вживання і в

умовах вживання ефективних засобів захисту ІС. Тому необхідні методики оцінки захищеності, які б створили передумови для ефективної оцінки загального стану інформаційної системи з погляду рівня захищеності її ресурсів. При побудові відповідних систем захисту визначаються множини ресурсів ІС, що підлягають захисту, множини атак, визначається їх вплив на ІС [1].

Великого значення набуває питання підвищення захищеності ІС за рахунок формування комплексу ефективних засобів захисту ІС з урахуванням інтенсивностей атак, що дозволить всі задачі по забезпеченню захисту ресурсів ІС вирішувати з достатньою повнотою і найбільш раціональним образом.

Проведення оцінки захищеності ІС повинно виконуватись згідно етапам: аналіз структури та особливостей ІС, аналіз впливу загроз на ІС, вибір засобів захисту, визначення ймовірностей та інтенсивностей порушення безпеки.

Першим етапом оцінки захищеності є вибір об‘єктів захисту. В якості об‘єкта захисту розглядається ІС. Під ІС можна розуміти систему, призначену для організації, збереження, поповнення, підтримки і надання користувачам інформації відповідно до їх запитів [2]. Іншими словами – це система, що складається з множини зосереджених підсистем, і безлічі засобів, що забезпечують з'єднання і взаємодію цих підсистем з метою надання користувачам широкого набору послуг зі сфери інформаційного обслуговування. Метою будь-якої системи, незалежно від області її застосування, програмного й апаратного забезпечення, є надання повної, достовірної і своєчасної інформації. ІС має складну децентралізовану структуру, що побудована в загальному випадку на основі інформаційно-обчислювальної мережі (ІОМ) і включає наступні взаємозалежні компоненти:

– технічні засоби обробки і передачі даних (засобів обчислювальної техніки і зв'язку);

– методи й алгоритми обробки у виді відповідного програмного забезпечення;

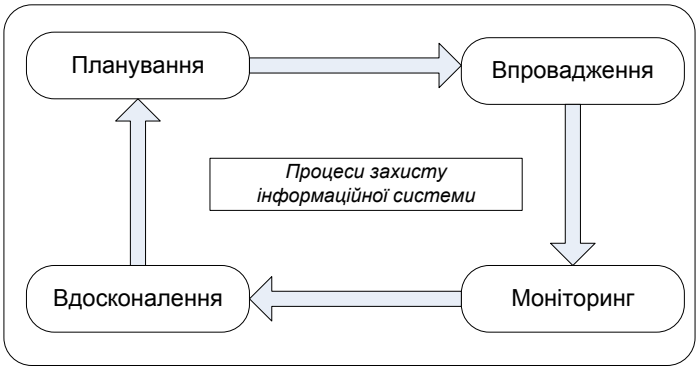
– інформацію (масиви, набори, бази даних) на різних носіях;

– персонал і користувачів системи, об'єднаних по організаційно-структурній, тематичній, технологічній або іншій ознаках для виконання автоматизованої обробки інформації з метою задоволення інформаційних потреб суб'єктів інформаційних відносин.

Сучасні ІС володіють наступними основними особливостями: територіальна рознесенність компонентів системи і наявність інтенсивного обміну інформацією між ними; широкий спектр використовуваних способів представлення, збереження і передачі інформації; інтеграція даних різного призначення, що належать різним суб'єктам, у рамках єдиних баз даних і, навпаки, розміщення необхідних деяким суб'єктам даних у різних віддалених вузлах мережі; абстрагування власників даних від фізичних структур і місця розміщення даних; використання режимів розподіленої обробки даних; участь у процесі автоматизованої обробки інформації великої кількості користувачів і персоналу різних категорій; безпосередній і одночасний доступ до ресурсів (у тому числі й інформаційних) великого числа користувачів (суб'єктів) різних категорій; високий ступінь різнорідності використовуваних засобів обчислювальної техніки і зв'язку, а також їхнього програмного забезпечення; використання імпортної обчислювальної техніки для побудови ІОМ; підключення ІОМ ІС до загальнодоступних систем зв'язку; специфічний характер збереженої, оброблюваної і переданої інформації, що володіє всім спектром

ступенів таємності; обов'язкова державна сертифікація механізмів захисту інформації; що зберігається, оброблюється і передається в ІС; використання в ІС неадаптованого до рішення спеціальних задач програмного й апаратного забезпечення. Таким чином, при розгляді ІС як об‘єкта захисту слід звернути увагу на ступінь деталізації моделі ІС. Очевидно, що чим вище детальність розгляду об'єктів ІС, тим точніше оцінка потенційного збитку. Однак розміри інфраструктури ІС можуть не дозволити провести детальний аналіз всіх об'єктів системи. У цьому випадку варто зупинитися на найбільш важливих сервісах, з огляду на наближеність результатів, що будуть отримані.

Крім того, на даному етапі, при проведенні оцінки рівня захищеності необхідно враховувати всі стадії проектування ІС та процеси її захисту. Представлення процесів захисту ІС засновано на процесах безперервного поліпшення якості – цикл Демінга [3] (рис. 1). Першим процесом є планування, метою якого є виявлення, аналіз, визначення і опис станів ІС. При створенні цього процесу слід розробити методику категоризації ресурсів ІС та оцінки захищеності на основі інформації про актуальні для даної ІС загрози та вразливості. Далі відбувається процес впровадження спланованих методів захисту, що описує процедуру запуску нового процесу забезпечення інформаційної безпеки, або модернізації того, що існує. Наступні процеси – моніторинг функціонуючих процесів забезпечення захисту ресурсів ІС та вдосконалення процесів забезпечення конфіденційності, цілісності і доступності ІС відповідно до результатів моніторингу, який робить можливою реалізацію корегуючих дій.



Схематичне відображення процесів захисту ІС

Після детального аналізу ІС, на другому етапі необхідно проведення аналізу впливу атак на ІС. Визначення, аналіз і класифікація найбільш небезпечних атак є одним з найважливіших етапів оцінки захищеності ІС та її ресурсів. Аналіз впливу атак на ІС – це задача досить складна і трудомістка, яка включає складання повного переліку потенційних атак і дослідження можливості їх впливу на систему. Основні труднощі при цьому виникають при визначенні законів розподілу ймовірностей таких подій, як реалізація атак [2].

Тому, на даному етпі, необхідно сформувати перелік найбільш важливих ресурсів ІС, розташувати всі ресурси у ряд з наскрізною нумерацією. Множину ресурсів можна записати $X = X_1, X_2, ..., X_M$, де M – кількість ресурсів. Таким чином, потрібно визначити глибину деталізації і скласти перелік вразливих ресурсів ІС.

Оцінку впливу атак на ІС можна здійснити за допомогою методів статистичних випробувань, теорії масового обслуговування, математичної статистики, теорії нечітких множин. Наприклад, при проведенні аналізу ІС з метою виявлення вразливих ресурсів проводиться їх ранжирування за рівнем вразливості та ранжирування атак за ступенем небезпеки за допомогою використання нечіткої логіки. Якщо припустити, що множина атак є кінцевою і нараховує N компонент $R = R_1, R_2, ..., R_N$, то при визначенні впливу атак розглядається можливість дії кожної атаки з множини $R = R_1, R_2, ..., R_N$ на кожен ресурс ІС. В результаті одержуємо інтенсивності потоку n-ої атаки на m-й ресурс – $I_{nm}(t)$.

На наступному етапі для забезпечення безпеки ІС на необхідному рівні застосовуються засоби захисту, які поєднуються в єдину систему захисту ІС. Вибір засобів і методів захисту конкретного ресурсу можна проводити виходячи тільки з функціонального призначення, властивостей незахищеного ресурсу, аналізу атак, що впливають на цей ресурс [2].

Якщо об‘єктом захисту виступає ІС, то захист X_m від атаки R_n може бути з застосуванням декількох засобів захисту з множини $Z = \{Z_1, ..., Z_k, ..., Z_K\}$, де K – кількість засобів захисту [1]. Припустимо, що Z_{nm} – засоби захисту ІС X_m від атак R_n , P_{nm} - імовірність атаки R_n на ресурс ІС X_m; $P*_m$ – імовірність порушення захисту ресурса X_m атакою R_n., тоді від кожної потенційної атаки існує захист при умові, що контур перешкоди замкнутий.

Модель системи захисту, де для кожного ресурса ІС існує захист від будь-якої атаки, називається моделлю захисту з повним перекриттям.

Система, побудована на основі цієї моделі, повинна мати засіб захисту на кожен ресурс ІС, що захищається, від кожної можливої атаки.

Система захисту ІС та будь-якого її ресурса X_m від атаки R_n повинна бути багаторівневою та здійснюватися з застосуванням багатьох засобів захисту.

У такому випадку ефективність засобу Z_{nm} буде дорівнює $P_{Z_{nm}} = 1 - \prod (1 - P_{Z_{nmi}})$,

де $P_{Z_{nmi}}$ – ефективність і-го засобу захисту ІС, що застосовується для побудови захисту X_m від R_n.

На наступних етапах визначаються імовірності та інтенсивності порушення безпеки ІС. Ймовірність порушення безпеки ресурсу X_m від атаки R_n за Δt може бути визначено співвідношенням:

$$\overline{P}_{nm}(t, t+\Delta t) = P_{nm}(t, t+\Delta t)(1 - P_{Znm}(t, t+\Delta t)), \quad (1)$$

де $P_{nm}(t, t+\Delta t)$ – імовірність хоча б однієї атаки на X_m за Δt .

Для пуассонівського потоку подій доведено, що при $\Delta t \to 0$ з точністю до нескінченно малих величин вищих порядків імовірність виникнення однієї події з інтенсивністю $\overline{I}_{nm}(t)$ дорівнює $\overline{P}_{nm}(t, t+\Delta t) \approx I_{nm}(t)\Delta t$.

Тоді інтенсивність порушення захисту ІС X_m від атаки R_n можна визначити:

$$\bar{I}_{nm}(t) = \frac{\overline{P}_{nm}(t, t+\Delta t)}{\Delta t} = \frac{P_{nm}(t, t+\Delta t)(1 - P_{Znm}(t, t+\Delta t))}{\Delta t}, \quad (2)$$

де $\overline{P}_{nm}(t, t+\Delta t)$ – імовірність хоча б однієї атаки на X_m за Δt [4].

В результаті аналізу стану ІС при впливі атак мають бути визначені функціональні залежності, що відбивають зміни станів системи. При впливі атак на ІС із відносно повної множини *R*, для кожної пари $X_m, m = \overline{1, M}$ та $R_n, n = \overline{1, N}$ замість інтенсивності потоку $I_{nm}(t)$ будуть інтенсивності порушення безпеки ІС $\bar{I}_{nm}(t)$, тобто зміна інтенсивностей атак на ресурси ІС[2]. Таким чином, при проведені оцінки рівня захищеності ІС враховується зміна інтенсивностей потоків атак, що впливають на ІС при застосуванні засобів захисту $\Delta I_{nm}(t) = I_{nm}(t) - \bar{I}_{nm}(t)$. Використовуючи зміни інтенсивностей потоків атак можна провести оцінку рівня захищеності ІС. Знаючи нечіткі значення і функції належності коефіцієнтів небезпеки загроз, можна із врахуванням імовірності реалізації загроз за правилами теорії нечіткої множини розрахувати нечіткі значення ступеня захищеності ІС від множини загроз.

Висновки

Запропонована методика оцінки захищеності ІС дозволяє вирішити задачу підвищення рівня захищеності ІС та її ресурсів, враховує зміну інтенсивностей потоків атак при застосуванні засобів захисту. Основними етапами побудови системи оцінки захищеності ІС є аналіз структури та визначення особливостей ІС, визначення множини атак та найбільш вразливих ресурсів, визначення інтенсивностей, імовірнісних характеристик потоку атак та визначення інтенсивності порушення безпеки ІС. Методика дозволяє прискорити вибір оптимального варіанту захисту від атак та підвищити ефективність проектування систем захисту ІС.

Список використаної літератури

1. Паціра Є.В., Захарова М.В., Корченко А.О. Дослідження процесів впливу та поводження інформаційних ресурсів під дією кібератак // Науково-технічний журнал «Захист інформації». – К.: НАУ, 2010. – С. 26 – 30.

2. Стасюк О.І., Корченко О.Г., Захарова М.В Побудова ефективних моделей систем захисту інформаці // Защита информации: Сборник научних трудов. – К.: НАУ, 2007. – С.186 – 190.

3. Деминг У.Э. Выход из кризиса. Тверь: Альба, 1994. – 498 с.

4. Вентцель Е.С., Овчаров Л.А. Теория случайных процессов и ее инженерные приложения. – М.: Наука, 1991. – 241 с.

Стаття надійшла до редакції 27.04.2013

Методика оценки защищенности информационных систем с учетом интенсивностей атак

Захарова М.В.
Черкасский государственный технологический университет

Предложенная методика позволяет решить задачу повышения уровня защищенности ИС и ее ресурсов, учитывает изменение интенсивностей потоков атак при использовании средств защиты. Основными этапами оценки защищенности ИС является анализ структуры и определение особенностей ИС, определение множества атак и наиболее уязвимых ресурсов, вероятностных характеристик потока атак и определения интенсивности нарушения безопасности ИС.

Ключевые слова: информационная система, атака, система защиты.

Methodology to evaluate the security of information systems, taking into account the intensity of attacks

M. Zaharova
Cherkasy State Technological University

The proposed method can solve the problem of raising the level of security of information systems (IS) and its resources, taking into account the change in flux attacks in the application of remedies. The main stages of IS security evaluation is to analyze the structure and defining features of IP, the definition of the set of attacks and vulnerable resources probabilistic flow characteristics determine the intensity of attacks and security breaches IS

Keywords: information system, attack, security system.