УДК 681.324

# ОЦІНКА ЕФЕКТИВНОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ «ЕКОЛОГІЧНИЙ ПАСПОРТ РЕГІОНІВ УКРАЇНИ»

*Губенко Н.Є., Хімка С.С.*
*Донецький національний технічний університет, Донецьк*

## Аналіз структури системи захисту інформації

"Екологічний паспорт регіонів України" – це АС, метою якої є збір та обробка екологічної інформації щодо стану навколишнього середовища та природних ресурсів регіонів України для підвищення ефективності управління природоохоронною діяльністю на національному рівні.

Функціональні модулі системи розроблені мовою програмування PHP та у базі даних MySQL. Скрипти та база даних зберігаються на віддаленому сервері. Доступ до них здійснюється через протокол http. Авторизація проходить за допомогою логіну та паролю. Для регулювання прав доступу використовується дискреційно-рольова модель політики безпеки. Система має три ролі – адміністратор, модератор та незареєстрований користувач. Адміністратор має можливості додавати користувачів з існуючими ролями та на основі матриці доступу регулювати їх права.

Схема поділення АС «Екологічний паспорт регіонів України» на об'єкти захисту. представлена на рис. 1.

Система захисту інформації АС складається з наступних засобів:

Для об'єкта «Web-сервер»:

- спеціальні настройки обмежень на доступ до контейнерів контенту(каталоги і файли на файловій системі, розділи сайту);
- аудит усіх запитів вбудованими в Apache механізмами логування.


Рисунок 1- Схема поділення АС «Екологічний паспорт регіонів України» на об’єкти захисту

Для об’єкта «Сервер додатків»:
- механізм керування доступом (дискреційно-рольова модель політики безпеки);
- механізм авторизації за допомогою логіну та паролю;
- маски для валідації допустимих значень аргументів.

Для об’єкта «База даних»:
- механізм авторизації;
- фіксація аудітной інформації (ім'я користувача і дати зміни).

Для об’єкта «Користувач»:
- антивірусні програми.

На базі даних про структуру системи захисту інформації та даних про погрози, які виникають, можна розробити модель системи захисту інформації.

**Опис концептуальної моделі СЗІ**

У статті [1] наведені методи і методики, що дозволяють виконувати кількісну оцінку захищеності інформації при використанні СЗІ. Як правило, кількісна захищеність інформації оцінюється певним набором імовірнісних показників, основним з яких є інтегральний показник. Для обґрунтування методики оцінки захищеності інформації розроблена теоретична модель СЗІ від НСД. Її можна представити у вигляді схеми, зображеної на рис. 2.

СЗІ має вигляд мережевої моделі, що складається з набору засобів захисту $S_i$. На вхід засобів захисту надходять потоки запитів НСД $V(t)$ які визначаються моделлю порушника на множині потенційних загроз $\{U_i\}$. Завдання засобу захисту - розпізнати загрозу і заблокувати несанкціонований запит.

В результаті функціонування системи захисту вхідний потік НСД розріджується з імовірністю $p_i(y)$ і утворює вихідний потік $V_i^{'}(t)$. На рис. 3 можна побачити, що для деяких вхідних потоків відсутні засоби захисту, це відображає факт неповного закриття системою захисту всіх можливих каналів прояви загроз.

Кожен засіб (механізм) захисту характеризується ймовірністю пропуску НСД - $q$ і, відповідно, ймовірністю забезпечення захисту (відображення НСД) $p = 1 - q$. Порушник характеризується вектором інтенсивностей $\lambda = \{\lambda_1, \lambda_2, ..., \lambda_{i+m}\}$ спроб реалізації відповідних загроз $U_1, ..., U_{i+m}$.

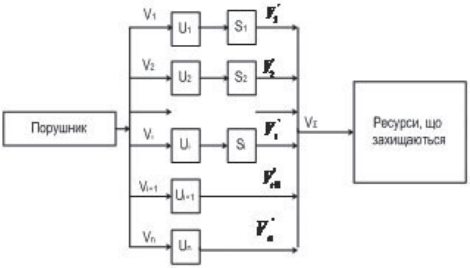


Рисунок 2 - Модель системи захисту інформації для автоматизованої системи «Екологічний паспорт регіонів України» захисту інформації від НСД

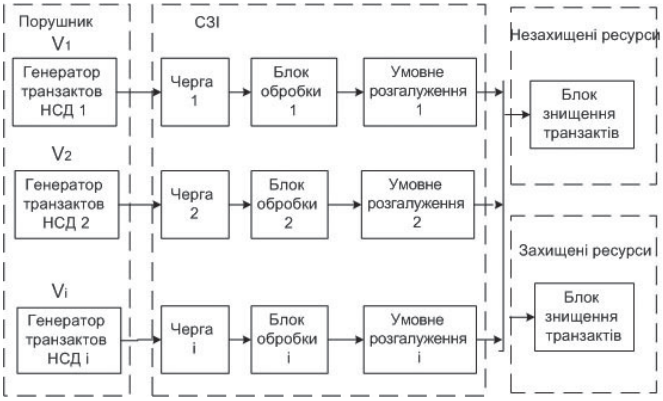


Рисунок 3 - Імітаційна модель СЗІ від НСД

Згідно [2], для того, щоб реалізувати системний підхід до забезпечення інформаційної безпеки необхідно застосовувати методи моделювання систем і процесів захисту інформації. У моделі мають бути відображені істотні властивості об'єкта або процесу, що моделюються, а також математичний або логічний опис його компонентів.

**Розробка імітаційнної моделі СЗІ**

Уявімо математичну модель СЗІ, яка наведена на рисунку 3 у вигляді функціональних блоків, об'єднаних в три групи, що відповідають трьом основним об'єктам моделюється системи: «Порушник», «СЗІ» і «Ресурси, які захищаються». Модель наведена на рис. 3.

Перший блок - «Порушник» - не має вхідного впливу, його завдання - генерація потоку (потоків) запитів НСД (транзактов) із заданою інтенсивністю $\lambda$.

Блок «СЗІ» імітує процес реагування СЗІ на запити НСД. Функціональні елементи цього блоку імітують черги запитів НСД і затримки на обслуговування. Основним же завданням функціонування цього блоку є відсіювання запитів НСД з певною (заданою) ймовірністю. На виході блоку утворюється розріджений потік запитів НСД, що має інтенсивність $\lambda'$.

Останній блок моделі - «Ресурси» - не виконує самостійних функцій і використовується в імітаційної моделі для знищення запитів НСД.

Для оцінки ступеню захищеності автоматизованої системи від НСД використовуються наступні показники: імовірність захисту - $Z(t)$; середній час між пропущеними НСД - $T_n$; інтенсивність потоку пропущених НСД - $H(t)$. [1]

Будемо розглядати вірогідність забезпечення захисту як ймовірність відсутності несанкціонованих запитів до інформації на виході засобів захисту, то її значення можна визначити за формулою:

$$Z(t) = 1 - F(t) \tag{1}$$

де $F(t)$ - функція розподілу випадкової величини $T_n$, Ця величина показує час між двома сусідніми пропусками НСД. $Z(t)$ є інтегральним показником захищеності інформації і показує ймовірність того, що за час $t$ не буде пропущено жодної спроби НСД.

Якщо розглядати сумарний потік НСД як потік, розподілений за законом Пуассона [1], то для обчислень оцінки захищеності можна використовувати формулу:

$$Z(t) = e^{-\sum_{i=1}^{n} \lambda_i q_i t} \tag{2}$$

Тоді, інтенсивність потоку пропущених запитів НСД визначається формулою:

$$H(t) = \sum_{i=1}^{n} \lambda_i q_i t \tag{3}$$

Алгоритм роботи імітаційної моделі має наступний вигляд. Генератор транзактів генерує із заданою інтенсивністю запит НСД. Запит надходить в чергу. Якщо механізм захисту вільний, запит НСД надходить на обслуговування на час $t_{M3}$. Після цього

він відсіюється або пропускається в систему, утворюючи потік пропущених запитів НСД. Відсіювання або пропуск запитів НСД відбувається з заданими ймовірностями

АС представляє собою Web-додаток, тому для аналізу погроз несанкціонованого доступу (НСД) можна використати статистику вразливостей Web додатків за 2008 рік[3]. Було промодельовано загрози, які виникають частіше за все, відповідно до цієї статистики. Приймемо значення середньої інтенсивності потоку запитів рівним 60 секунд. Для загрози «Межсайтингове виконання скриптів» (Cross-Site Scripting) ймовірність розпізнавання запитів дорівнює 0,77, для загрози «Недостатня авторизація» Insufficient Authorization – 0,14, для SQL-ін'єкція (SQL injection) - 0,76. Інші вхідні дані для цих загроз однакові. Вони наведені у табл. 1.

Результати роботи наведені в табл. 2.

Таблиця 1

Вхідні параметри моделі

| Назва | Значення |
|---|---|
| Генератор транзактів | Час між запитами НСД розподіляється за експоненціальним законом |
| Середня інтенсивність потоку запитів, $\lambda$ | 60 с |
| Час обробки запиту | 1 с |
| Час моделювання | 100000 с |

**Висновки**

У ході проведення досліджень розглянуто показники ефективності системи захисту і побудована імітаційна модель системи захисту АС «Екологічний паспорт регіонів України» з використанням мови імітаційного моделювання GPSS.

Зроблено річний розрахунок і побудовані графіки таких показників, як середній інтервал часу між сусідніми пропусками НСД та середньої інтенсивності потоку пропущених НСД. Після

Таблиця 2

Вхідні параметри моделі

| Погроза | Інтенсивність потоку пропущених запитів H,с | Середній час між пропусками запитів $\tau_{нед}$,с |
|---|---|---|
| Межсайтингове виконання скриптів | 13,8 | 260 |
| Недостатня авторизація | 51,6 | 105 |
| SQL-ін'єкція | 14,4 | 254 |

цього проведено експеримент і отримані експериментальні значення цих величин.

Можна зробити висновок, що значення, отримані в ході імітаційного моделювання, підтверджують теоретичні розрахунки. Адекватність імітаційної моделі підтверджується.

Отриманий при моделювання дані мають загальний характер. Для адекватної оцінки ефективності СЗІ необхідні статистичні дані про вразливості для конкретно заданої АС.

**Література**

[1] Карпов В.В. Вероятностная модель оценки защищенности средств вычислительной техники с аппаратно-программным комплексом защиты информации от несанкционированного доступа / В.В. Карпов // «Программные продукты и системы» № 1, 2003 год.

[2] Статистика уязвимостей Web приложений за 2008 год. Эл. ресурс. Режим доступа: http://www.securitylab.ru/analytics/368513.php

[3] Девянин П.Н., Михальский О.О. Теоретические основы компьютерной безопасности. - М.: Радио и связь, 2000.