УДК 681.324

# Розробка імітаційної моделі захисту інформації для автоматизованої системи «Екологічний паспорт регіонів України»

Губенко Н.Є., Хімка С.С.
Донецький національний технічний університет,
gubenko@cs.dgtu.donetsk.ua, s.s.himka@gmail.com

***Abstract***

***Khimka S. " Development of a simulation model of information security for the automated system "Environmental Passport of Regions of Ukraine"*** *Analysis of existing methods to evaluate the effectiveness of information security. Study of the protection system for the automated information system "The ecological passport of regions of Ukraine". Study of the probabilistic approach to evaluate the characteristics of effective information security systems. On the basis of this approach, the simulation model.*

**Key words***: simulation model, assessment of efficiency, vulnerability.*

## *Вступ*

Про важливість впровадження в інформаційні системи засобів захисту написано чимало робіт. Але дотепер не можна виділити універсального методу, який дозволяв би створити оптимальну систему захисту інформації. Це викликано тим, що будь-яка інформаційна система має свої особливості в архітектурі, способах обробки даних, ступенях критичності інформації та багато в чому іншому. До того ж кожна сфера має свої критерії оптимальності. Тому розробка оптимальної системи захисту інформації для певного типу інформаційних систем є на сьогоднішній день актуальною проблемою.

Згідно до нормативних документів [1, 2], ефективність захисту інформації визначається класом захищеності автоматизованої системи (АС). Клас захищеності, у свою чергу, визначає набір механізмів захисту (МЗ), які мають бути реалізовані в АС. Такий підхід не дозволяє враховувати ні якість самих МЗ, констатуючи лише факт їхньої наявності або відсутності, ні зміни умов функціонування системи захисту інформації (СЗІ).

В останній час науковцями постійно розглядаються альтернативні підходи щодо оцінки ефективності захисту інформації.

Провідним дослідником у цій сфері є Домарев В.В. Його дослідження присвячені проблемам створення комплексних систем захисту інформації. У своїх роботах [3,4] він пропонує системний підхід до рішення зазначеної проблеми. Їм розроблена трьохвимірна матриця, яка описує елементи захисту та зв'язок між ними. Щоб провести оцінку захищеності СЗІ треба мати експертну оцінку за усіма 140 елементами матриці. Такий підхід є дуже складним у використанні.

Ще один підхід ґрунтується на економічних аспектах. Провідними дослідниками цього питання є Петренко С.А. та Сімонов С.В. В роботах [5, 6] описується методика оцінки СЗІ на основі сукупної вартості володіння. Ця методика базується на визначенні вартості інформаційних ресурсів. Але цей показник дуже складно визначити для некомерційних установ.

У роботі [7] розглянута ймовірнісна модель оцінки ефективності СЗІ, яка ґрунтується на припущенні, що потенційно можливі прояви загроз і розміри потенційно можливих збитків є випадковими подіями, тому вони можуть бути охарактеризовані законами розподілу та типовими характеристиками [8].

Метою даної роботи є аналіз існуючих алгоритмів і методів захисту інформації АС «Екологічний паспорт регіонів України» та створення імітаційної моделі оцінки ефективності СЗІ для удосконалення механізмів та методів захисту зазначеної системи.

## *Аналіз системи захисту інформації*

«Екологічний паспорт регіонів України» – це АС, призначенням 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. Тому захисту цієї інформації від погроз порушення конфіденційності та цілісності повинна приділятися певна увага.

Програмний комплекс «Екологічний паспорт регіонів України» може працювати в

двох режимах: у режимі центрального серверу та у режимі локального серверу. Ми будемо розглядати режим центрального серверу. Доступ до центрального серверу здійснюється через мережу Інтернет за адресою http://ukrecopass.org.ua.

Структура системи «Екологічний паспорт регіонів України» наведена на рисунку 1.

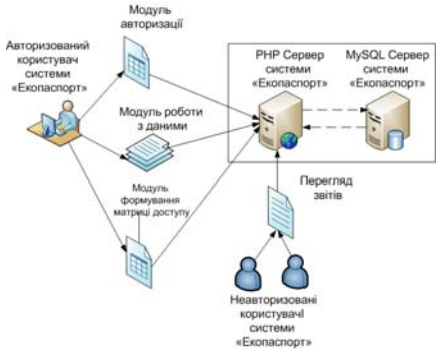


Рисунок 1. – Структура АС «Екологічний паспорт регіонів України»

Функціональні модулі системи розроблено за допомогою мови програмування PHP та бази даних MySQL. Скрипти та база даних зберігаються на віддаленому сервері. Доступ до них здійснюється через протокол *http*. Захист від погрози порушення конфіденційності здійснюється за допомогою традиційної авторизації (введення логіну та паролю). Для регулювання прав доступу використовується дискреційно-рольова модель політики безпеки. Система має три ролі – адміністратор, модератор та незареєстрований користувач. Адміністратор має можливість додавати користувачів з існуючими ролями та за допомогою матриці доступу регулювати їхні права.

Схему поділення АС «Екологічний паспорт регіонів України» на об'єкти захисту наведено на рисунку 2.


Рисунок 2. – Схема поділення АС «Екологічний паспорт регіонів України» на об'єкти захисту

Аналіз існуючої системи захисту інформації АС «Екологічний паспорт регіонів України» показав, що вона складається з наступних засобів.

Для об'єкту «Web-сервер» - це спеціальні настройки обмежень на доступ до контейнерів контенту (каталоги і файли на файловій системі, розділи сайту).

Для об'єкту «Сервер додатків» - це механізм управління доступом (дискреційно-рольова модель політики безпеки) та механізм авторизації за допомогою логіну та паролю.

Для об'єкту «База даних» - це механізм авторизації.

Для об'єкту «Користувач» - це антивірусні програми.

Наведений перелік засобів захисту, які використовуються у АС «Екологічний паспорт регіонів України», та досвід її експлуатації показав недосконаліть цих засобів.

На основі даних про структуру системи захисту інформації та даних про погрози, які виникають, було розроблено концептуальну модель, яка дозволяє удосконалити існуючу систему захисту інформації.

### *Опис концептуальної моделі системи захисту інформації*

У статті [8] наведено методи і методики, які 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. Традиційно для обґрунтування методики оцінки захищеності інформації розробляється теоретична модель СЗІ від погроз несанкціонованого доступу (НСД). Таку модель можна представити у вигляді схеми, зображеної на рисунку 3.

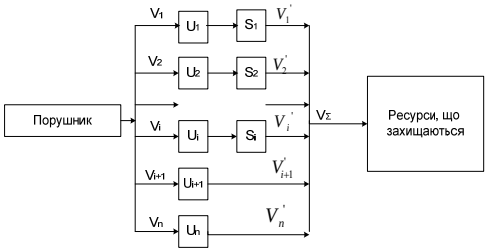


Рисунок 3. – Модель системи захисту інформації від НСД

СЗІ має вигляд мережевої моделі, яка 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.

При функціонуванні системи захисту вхідний потік НСД розріджується з імовірністю

$p_i(y)$ і утворює вихідний потік $V_i(t)$. На рисунку 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 $\lambda = \{\lambda_1, \lambda_2, \dots \lambda_{i+m}\}$ спроб реалізації відповідних загроз $U_1 \dots U_{i+m}$.

Згідно з [3], 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.

В роботі [8] описано ймовірну модель системи захисту інформації з використанням теорії масового обслуговування. Отже доцільно використовувати при побудові імітаційної моделі засоби моделювання систем масового обслуговування. До таких засобів можна віднести досить поширену мову імітаційного моделювання GPSS.

### *Розробка імітаційної моделі системи захисту інформації*

Уявімо математичну модель СЗІ, яка наведена на рисунку 3 у вигляді функціональних блоків, які об'єднані в три групи, що відповідають трьом основним об'єктам системи, яка моделюється: «Порушник», «СЗІ» і «Ресурси, які захищаються». Модель СЗІ у вигляді функціональних блоків наведено на рисунку 4.

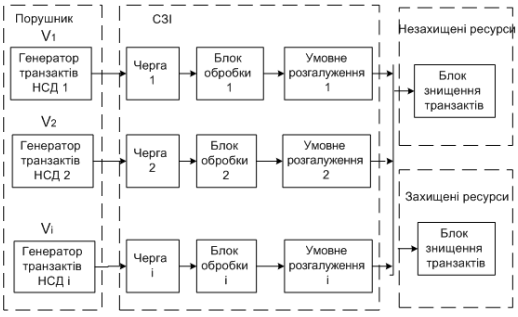


Рисунок 4 – Імітаційна модель СЗІ від НСД

Перший блок - «Порушник» - не має вхідного впливу, його завдання - генерація потоку (потоків) запитів НСД (транзактів) 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 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 ступеня захищеності автоматизованої системи від НСД використовуються наступні показники: імовірність захисту - $\mathcal{Z}(t)$; середній час між пропущеними НСД - $\tau_n$; інтенсивність потоку пропущених НСД - $H(t)$. [8]

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

$$\mathcal{Z}(t) = 1 - F(t), \qquad (1)$$

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

Якщо розглядати сумарний потік НСД як потік, який розподілено за законом Пуассона [8], тоді для обчислень оцінки захищеності можна використовувати формулу:

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

Виходячи з цього, інтенсивність потоку пропущених запитів НСД визначається за формулою:

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

Алгоритм роботи імітаційної моделі має наступний вигляд. Генератор транзактів генерує з заданою інтенсивністю запит НСД. Запит надходить до черги. Якщо механізм захисту вільний, тоді запит НСД надходить до обслуговування на час $t_{M3}$. Після цього він відсіюється або пропускається в систему з заданими ймовірностями, утворюючи потік запитів НСД, які було пропущено .

АС уявляє собою Web-додаток, тому для аналізу погроз НСД можна використовувати статистику вразливостей Web додатків за 2008 рік, яку було зібрано Дмитром Євтєєвим [9]. Під час роботи були промодельовані загрози, які, відповідно до цієї статистики, виникають частіше за все. Значення середньої інтенсивності потоку запитів було прийнято таким, що дорівнює 60 секундам. Для загрози «Межсайтінгове 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 таблиці 1.

Таблиця 1. – Вхідні параметри моделі

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

За допомогою розробленої імітаційної моделі проведено три експерименти. Результати роботи наведено в таблиці 2:

Таблиця 2. – Результати моделювання роботи СЗІ АС «Екопаспорт регіонів України»

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

На рисунку 5 відображена гістограма щільності розподілення $\tau_{НСД}$ для загрози Insufficient Authorization. Для інших загроз гістограми цільності мають аналогічний вигляд.

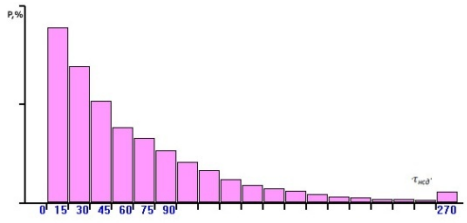


Рисунок 5. – Гістограма щільності розподілення $\tau_{НСД}$ для загрози «Недостатня авторизація»

Аналіз отриманих гістограм показує недосконаліть існуючої системи захисту з точки зору її уразливості через відсутність посилених механізмів захисту від НСД.

Нами запропоновано удосконалити засоби захисту АС «Екологічний паспорт регіонів України» за допомогою уведення в кожен об'єкт додаткових функцій інформаційної безпеки.

Для об'єкту «Web-сервер» - це аудит усіх запитів вбудованими в Apache механізмами логування та використання захищеного каналу зв'язку. Для об'єкту «Сервер додатків» - маски для валідації допустимих значень аргументів. Для об'єкту «База даних» - фіксація аудітної інформації (ім'я користувача та дати зміни).

### *Висновки*

При проведенні досліджень розглянуто структуру, методи та показники ефективності системи захисту АС «Екологічний паспорт регіонів України» і побудована її імітаційна модель з використанням системи GPSS.

Проведено експеримент і отримані експериментальні значення середнього інтервалу часу між сусідніми пропусками запитів НСД та середньої інтенсивності потоку пропущених запитів НСД. Це дало змогу запропонувати низку додаткових заходів для об'єктів захисту системи, яка розглядається.

На наступному етапі для вдосконалення захисту системи передбачається продовжити збір статистичної інформації щодо атак на окремі об'єкти АС «Екологічний паспорт регіонів України». Також планується розробка алгоритму визначення інтенсивності потоку запитів у залежності від імовірності прояви тієї чи іншої загрози.

### *Література*


1. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності інформації від несанкціонованого доступу.
2. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
3. Домарев В.В. Безопасность информационных технологий. Системный поход / В.В. Домарев – К.: ТИД ДС, 2004. – 992 с.
4. Домарев В.В. Моделирование процессов создания и оценки эффективности систем защиты информации / В.В. Домарев http://www.citforum.ru/security/articles/model_proc (29.09.2009).
5. Петренко С.А. Симонов С.В Информационная безопасность: экономические аспекты. / С.А. Петренко // Jet Info – 2003. – №10 (125) . С. 3-24.
6. R. Witty, J. Dubiel, J. Girard, J. Graff, A. Hallawell, B. Hildreth, The Price of Information Security. Gartner Research, // Strategic Analysis Report, June 2001. С. 2-15.
7. Герасименко В.А., Малюк А.А. Основы защиты информации / В.А. Герасименко - М.: Известия, 1997.
8. Карпов В.В. Вероятностная модель оценки защищенности средств вычислительной техники / В.В. Карпов // «Программные продукты и системы» – 2003 – № 1. С. 31-36.
9. Д. Євтєєв Статистика уязвимостей Web приложений за 2008 год. http://www.Securitylab.ru/analytics/368513.php (29.09.2009).