УДК 681.3.06

І.А.Терейковський

ЗАХИЩЕНІСТЬ WEB-СЕРВЕРІВ APACHE ТА IIS

Стаття присвячена розгляду питань захисту найбільш розповсюджених WEB–серверів Apache та IIS від несанкціонованого доступу та атак на відмову. Визначена інтегральна оцінка захисту означених WEB–серверів від несанкціонованого доступу. Проведено порівняння ефективності захисту Apache та IIS від атак на відмову з санкціонованим використанням HTML–файлів та серверних сценаріїв PHP.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

На сьогодні важливим напрямком підвищення ефективності функціонування багатьох як вітчизняних, так і закордонних автоматизованих інформаційних систем (АІС) є інтеграція з глобальною мережею Інтернету. В багатьох випадках завдяки цієї інтеграції вирішуються дві основні задачі. По-перше, об'єднуються територіально розподілені підсистеми АІС. По-друге, користувачам Інтернету забезпечується доступ до відкритої інформації АІС. Досить часто при вирішенні обох задач використовується WEB–сайт, який, крім того, відіграє представницьку роль АІС в мережі Інтернету. Практичний досвід вказує, що робота Web-сайту значною мірою впливає на ефективність функціонування всієї АІС. Основою WEB–сайту є WEB–сервер, що забезпечує доступ клієнтів із мережі Інтернету до WEB–сторінок сайту.

Останнім часом зафіксовані неподинокі випадки масованих атак порушників на АІС зі сторони Інтернету, причому досить часто об'єктом атак був WEB–сервер. Наприклад, за даними Міністерства Оборони США, у 2002 році було зафіксовано 200 атак, мета яких – отримання контролю над військовими серверами [1]. Як правило, наслідками більшості успішних атак на WEB–сервер ставало унеможливлення санкціонованого доступу, порушення цілісності або створення неконтрольованого поширення інформації АІС. Таким чином у багатьох випадках успішна атака на WEB–сервер може призвести не тільки до загрози функціонування WEB–сайту, але й до значного зменшення ефективності функціонування всієї АІС. Цим визначається актуальність загальної проблеми даної статті – дослідження захищеності WEB–серверу, а також її зв'язок з глобальною науково-практичною задачею забезпечення інформаційної безпеки АІС.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми

Для формалізації задачі оцінювання ефективності системи захисту інформаційної системи в [2] сформований наступний методичний підхід. Пропонується розглядати систему захисту у вигляді багаторівневої ієрархії I_p, де p – кількість рівнів ієрархії. Для інформаційних підсистем на кожному p-му рівні ієрархії вибирається множина об'єктів захисту M_{kp}, де $к$ – номер об'єкта на p-му рівні ієрархії. За допомогою експертного оцінювання для кожного M_{kp} об'єкта формується вектор загроз V_{skp}, де s – номер загрози для $к$-го об'єкта на p-му рівні ієрархії.

Зниження ефективності функціонування ІС на кожному p-му рівні ΔE_p визначається складним впливом реально діючих загроз на об'єкти p-го рівня:

$$\Delta E_p(t)=F\{M_{kp},V_{skp},t\}, \qquad (1)$$

де $F\{*\}$ – функціонал, що описує вплив реально діючих загроз V_{skp} на множину об'єктів M_{kp} в підсистемі p-го рівня; t – часова характеристика.

При цьому вважається, що відновлення ефективності підсистеми *p*-го рівня можливо лише завдяки проведенню адекватного рівню інтегральної загрози комплексу заходів безпеки Z_{jkp}, де *j* – номер заходу безпеки *Z* стосовно *к*-го об'єкта підсистеми *p*-го рівня. Пропонується поставити в залежність кількісну оцінку рівня інтегральної загрози ІС (*U*) від зниження ефективності АІС (ΔE) в цих умовах. Таким чином, враховуючи (1), у формалізованому виді рівень інтегральної загрози АІС на момент *t* можна оцінити функціоналом (2) з урахуванням обмежень (3):

$$U(t)= F\{M_{kp},V_{skp},t\}; \quad (2)$$

$$0 \le U(t) \le 1, \quad (3)$$

де $U(t)=0$ – означає повну відсутність загрози для АІС, а $U(t)=1$ –вивід з ладу АІС (ефективність АІС дорівнює 0).

1. Оцінку рівня загрози деякому *к*-му об'єкту АІС рекомендується здійснювати по сукупності окремих показників U_{kn} для відповідного об'єкта. Кожний *n*-й показник відображає події, пов'язані із зростанням загрози функціонування підсистеми АІС *p*-го рівня, яка розглядається. Розрахунок (2) рекомендується проводити шляхом часткових розрахунків $U(t)$ у фіксовані моменти часу *t* на основі використання методу аналізу ієрархій, а потім по окремих точках встановити функціональну залежність, яку можна використовувати у подальшому для прогнозування зміни рівня інтегральної загрози з плином часу. Також у [2] відзначено, що розв'язання задач керування безпекою інформаційної системи на сьогодні формалізоване недостатньо та досить часто базується на методах експертного оцінювання, проб та помилок, що вносить в розрахунки елементи суб'єктивізму і супроводжується досить великими похибками. Запропонований методичний підхід оцінки ефективності захисту АІС є досить досконалим та універсальним, але потребує уточнення та деталізації, як це відзначається і його авторами при оцінці ефективності захисту конкретної АІС, а в нашому випадку WEB–серверу. Також відомі нормативні вимоги до системи захисту WEB–серверів від несанкціонованого доступу (НСД) [3]. Це дозволяє з урахуванням нормативних вимог на базі методики (1-3) провести оцінку ефективності захисту найбільш розповсюджених WEB–серверів від НСД. Зазначимо, що методики визначення такої оцінки в доступній нам літературі не знайдено.

Крім того, для деталізації ефективності захисту WEB–серверу можливо використати результати [4] в якій проведено дослідження захисту WEB–сайтів корпоративних інформаційних систем від атак на відмову. Між іншим, в цій статті відзначено, що однією з найбільш небезпечних є атака на відмову WEB–сайту з санкціонованим використанням HTML–файлів та серверних сценаріїв PHP. Очікуваним результатом такої атаки є блокування доступу до сторінок сайту в наслідок вичерпання обчислювальних ресурсів сервера сайту. В даному випадку під поняттям обчислювальних ресурсів сервера розуміються ресурси WEB–сервера, операційної системи комп'ютерної мережі, комп'ютера та каналів зв'язку, що обслуговують сайт. Також в [4] показано, що типова атака на відмову корпоративного WEB–сайту проводиться зловмисником в умовах обмеження обчислювальних потужностей та тривалості. Крім цього очікувані умови атаки слід обмежити кваліфікованим адмініструванням сайту та відсутністю помилок в його програмному та апаратному забезпеченні. Зроблено припущення, що пропускна спроможність каналу зв'язку сайту набагато вища, ніж у зловмисника. При виконанні вказаних обмежень основною причиною блокування ресурсів сайту при атаці на відмову може стати тільки вичерпання потужності центрального процесора комп'ютера, що обслуговує сайт. При цьому використання обчислювальних потужностей комп'ютера зловмисника призводить до втрати потужностей комп'ютером, що обслуговує функціонування сайту. За цієї причини пропонується технічну ефективність атаки на відмову поставити у відповідність з кореляцією між цими потужнос-

тями. Витрату обчислювальних потужностей пропонується визначати:

– для зловмисника за допомогою показників навантаженням центрального процесора при реалізації атаки та тривалості виконання атаки для зловмисника;

– для комп'ютера, що обслуговує сайт, за допомогою тривалості роботи з 100% навантаженням центрального процесора. При цьому доступ до сторінок сайту гарантовано блокується.

Це дозволило визначити два показники технічної ефективності атаки на відмову з використанням сценаріїв: ефективну потужність атаки та ефективність блокування. Під потужністю атаки ($П$) пропонується розуміти відношення навантаження центрального процесора атакованого комп'ютера – сервера (K) до навантаження центрального процесора зловмисника при реалізації атаки (Z):

$$П = K/Z \ . \qquad (4)$$

Під ефективністю блокування (B) розуміємо відношення тривалості 100% навантаження процесора комп'ютера, що обслуговує функціонування сайту (β), до тривалості виконання атаки (α):

$$B = \beta/\alpha \ . \qquad (5)$$

Технічну ефективність захисту доцільно поставити в противагу технічній ефективності атаки. Внаслідок цього можливо визначити два показники технічної ефективності захисту: ефективну потужність захисту (Ω) та ефективність захисту від блокування (A), які можна представити у вигляді відношень

$$\Omega = 1/П; \qquad (6)$$

$$A = 1/B. \qquad (7)$$

Важливим результатом наведеної роботи є кількісні та якісні показники ефективності захисту WEB–серверу Apache від атак на відмову. Але для повноти результатів необхідно провести порівняння аналогічних показників ефективності захисту для різних типів WEB–серверів, наприклад для Apache та IIS.

Крім того, проведений аналіз виявив деяку аморфність термінів, що використовуються в науковій літературі, присвяченій захисту інформації в мережі Інтернету. Надалі будемо використовувати терміни, визначені в відповідній вітчизняній нормативній документації [3,5,6].

Виділення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття

- Визначення інтегральної оцінки ефективності захисту від НСД найбільш розповсюджених WEB-серверів відсутнє.
- Порівняння захищеності WEB–серверів Apache та IIS від атак на відмову із санкціонованим використанням HTML–файлів та серверних сценаріїв PHP проведено не в повному обсязі.

Формулювання цілей статті (постановка завдання)

- Проведення інтегральної оцінки ефективності захисту найбільш розповсюджених WEB–серверів від НСД. При цьому слід враховувати вимоги відповідних вітчизняних нормативних документів.
- Порівняння можливостей типових засобів захисту WEB–серверів Apache та IIS від атак на відмову із санкціонованим використанням серверних сценаріїв.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів

Наведемо терміни найбільш важливі для даної статті. WEB–сторінка (WEB–сайт) – це мережевий інформаційний ресурс, наданий користувачеві у вигляді HTML–документа з унікальною адресою у мережі. Сервер (server) – об'єкт комп'ютерної системи (програмний або програмно-апаратний засіб), що надає послуги іншим об'єктам за їх запитами. WEB–сервер обслуговує запити користувачів (клієнтів) згідно з протоколом HTTP (Hyper Text Transfer Protocol), за-

безпечує актуалізацію, збереження інформації WEB–сторінки, зв'язок з іншими серверами.

Використавши методику (1-3), інтегральну оцінку ефективності захисту WEB–серверів ($Z_w(t)$) можна провести наступним чином:

$$Z_w(t)=F\{Z_{wi},V_i,t\}, \quad (8)$$

де V_i – загроза за номером i; Z_{wi} – ефективність заходу безпеки від загрози V_i; t – часова характеристика.

Припустимо, що термін реалізації загроз та відповідних їм заходів безпеки незначний. Це дозволяє знехтувати впливом часових характеристик на ефективність захисту. Таким чином, оцінку ефективності захисту можна розрахувати як

$$Z_w=F\{Z_{wi},V_i\}. \quad (9)$$

Крім того, в першому наближені можна прийняти, що величина Z_{wi} детермінована і може набувати тільки два значення: 0 – захід неефективний та 1 – захід ліквідує загрозу. Розглянемо випадок визначення інтегральної оцінки захисту WEB–серверів від НСД. У цьому випадку відомий перелік нормативних заходів безпеки, що дозволяє переписати функціонал (9) у наступному вигляді:

$$Z_w=\sum_{i=1}^{N} Z_{wi}\ , \quad (10)$$

де i – номер заходу безпеки; N – нормативна кількість заходів безпеки.

Очевидно, що мінімальна величина $Z_w=0$, а максимальна – $Z_w=N$. При $Z_w=0$ захист абсолютно неефективний з точки зору відповідності нормативам. При $Z_w=N$ захист повністю відповідає нормативним заходам безпеки. Крім визначення кількісної оцінки ефективності захисту використання рівняння (10) дозволяє співставити захищеність WEB–серверів різних типів. Відзначимо, що кількість існуючих на сьогодні WEB–серверів досить велика, але найбільш розповсюдженими є Apache та WEB–сервери компанії Microsoft. Так, відповідно до матеріалів [7,8], кількість WEB–сайтів, що забезпечуються Apache становить 55% від загальної кількості. WEB–сервери компанії Microsoft забезпечують біля 25% WEB–сайтів. Розповсюдженість Apache пояснюється в першу чергу його безкоштовністю та відкритістю програмного коду. Останнє означає, що можна настроїти WEB–сервер для конкретних завдань, додати або знищити певні модулі, а також виправити дефекти програми. Ще одною важливою перевагою є мультиплатформеність Apache. Він використовується на серверах Unix–систем, в системах Macintosh, на серверах Windows. Настроювання Apache реалізоване за допомогою конфігураційних файлів, в які вносяться директиви для керування його функціональними можливостями. Великий обсяг можливих директив робить настроювання цього WEB–сервера доволі гнучким та надає адміністратору широкі можливості в сфері керування системою захисту. До загальновідомих недоліків Apache відносять:

– відсутність завершеного та досконалого графічного інтерфейсу, що значно ускладнює роботу адміністратора WEB–сервера;

– відсутність для безкоштовних версій офіційної служби технічної підтримки.

Для WEB–серверів компанії Microsoft вказані недоліки не характерні. Ці WEB–сервери є складовими компонентами таких операційних систем, як Windows NT, Windows 2000, Windows XP [7]. Найбільш популярні сучасні версії WEB–серверу компанії Microsoft входять до складу Internet Information Services (IIS) – набору базових служб Інтернету. Крім WEB–серверу до складу IIS включені FTP–сервер, SMTP–сервер, NNTP–сервер та ряд додаткових служб. Служби IIS об'єднані за допомогою стандартного графічного інтерфейсу адміністрування та спільних методів керування, що є беззаперечною перевагою, а, крім того, вони стандартизовані для Windows-методів керування, що робить процес адміністрування відносно простим.

У загальному випадку WEB–сервер повинен забезпечувати реалізацію вимог із захисту цілісності та доступності розміщеної на WEB–сторінці загальнодоступної інформації, а також

конфіденційності та цілісності технологічної інформації WEB-сторінки. Надалі розглянемо тільки ті вимоги до системи захисту, реалізувати які можна допомогою вдосконалення програмних засобів та методики застосування цих засобів. До методики застосування програмних засобів, крім іншого, слід віднести повноту та досконаліть відповідної документації. З врахуванням цих зауважень на основі [2] проведена структуризація типових вимог до системи захисту WEB–серверу від НСД (рис.1). Відзначимо, що, крім вимог "надійність середовища розробки" та "відкритість програмного коду", інші типові вимоги наведені в вітчизняному державному стандарті [3]. Включення вимог "надійність середовища розробки" та "відкритість програмного коду" в перелік типових здійснене на основі висновків [4]. Назви інших вимог відповідають нормативним. Для деяких вимог на рис. 1 наведені пояснення їх змісту. Принциповим моментом є структуризація вимог відповідно до життєвого циклу WEB–серверу. Проведемо аналіз відповідності систем захисту WEB–серверів Apache та IIS цим вимогам. Відзначимо, що надалі заходи захисту Apache будемо позначати Z^a_{wn}, а IIS – Z^i_{wn} , де n – номер заходу.

1. Програмне забезпечення Apache і IIS побудоване за модульним принципом. Таким чином, $Z^a_{w1} = Z^i_{w1} = 1$.

2. Для відповідності цим вимогам мають бути визначені всі стадії та етапи життєвого циклу WEB–серверу, а для кожної стадії та етапу – перелік та обсяги необхідних робіт і порядок їх виконання. Всі етапи робіт повинні бути задокументовані відповідно до правил встановлених вітчизняними державними стандартами. Відзначимо, що наявність цієї документації є загальноприйнятою вимогою при проектуванні захищених інформаційних систем. Хоча в звичайний супроводжуючий комплект документів Apache та IIS дана документація не входить, але її можна отримати при офіційному зверненні до компаній розробників. Тому, виходячи із фактичного стану речей, вважаємо, що $Z^a_{w2} = Z^i_{w2} = 1$.

3. Хоча форма специфікацій на функціональні послуги безпеки Apache та IIS дещо не відповідає вітчизняним стандартам, але їх досконаліть підтверджена практичним досвідом. Тому $Z^a_{w3}=Z^i_{w3} = 1$.

4. Для відповідності цим вимогам документація на систему захисту повинна містити опис послуг безпеки, що в ній реалізуються, а також настанови для різних категорій користувачів. Для обох WEB–серверів вказана документація, що доступна та досить детальна. Тому $Z^a_{w4} = Z^i_{w4} = 1$.

5. Практичний досвід показує, що система безпеки Apache та IIS пройшла багаторазове та жорстке тестування, хоча програма і методика тестувань не входять до звичайного комплекту супроводжуючої документації цих WEB–серверів, що вимагається [3]. Проте відповідна доукомплектація, на наш погляд, не викликатиме особливих труднощів при офіційному зверненні до компаній розробників. Тому, виходячи із фактичного стану речей, $Z^a_{w5} = Z^i_{w5} = 1$.

6. Надійність середовища розробки означає надійність мови програмування, що була застосована для реалізації WEB–серверу. Apache та IIS реалізовані на досить апробованій та надійній мові програмування C++. Таким чином, $Z^a_{w6} = Z^i_{w6} = 1$.

7. Вимозі відкритості програмного коду відповідає тільки Apache. $Z^a_{w7} = 1$, $Z^i_{w7} = 0$.

8. Як Apache, так і IIS дозволяють здійснювати розмежування прав користувачів на перегляд WEB–сторінок на підставі атрибутів доступу користувача і захищеного об’єкта. Тому $Z^a_{w8} = Z^i_{w8} = 1$.

9. Як Apache так і IIS дозволяють здійснювати розмежування прав користувачів на модифікацію WEB–сторінок на підставі атрибутів доступу користувача і захищеного об’єкта. Тому $Z^a_{w9} = Z^i_{w9} = 1$.

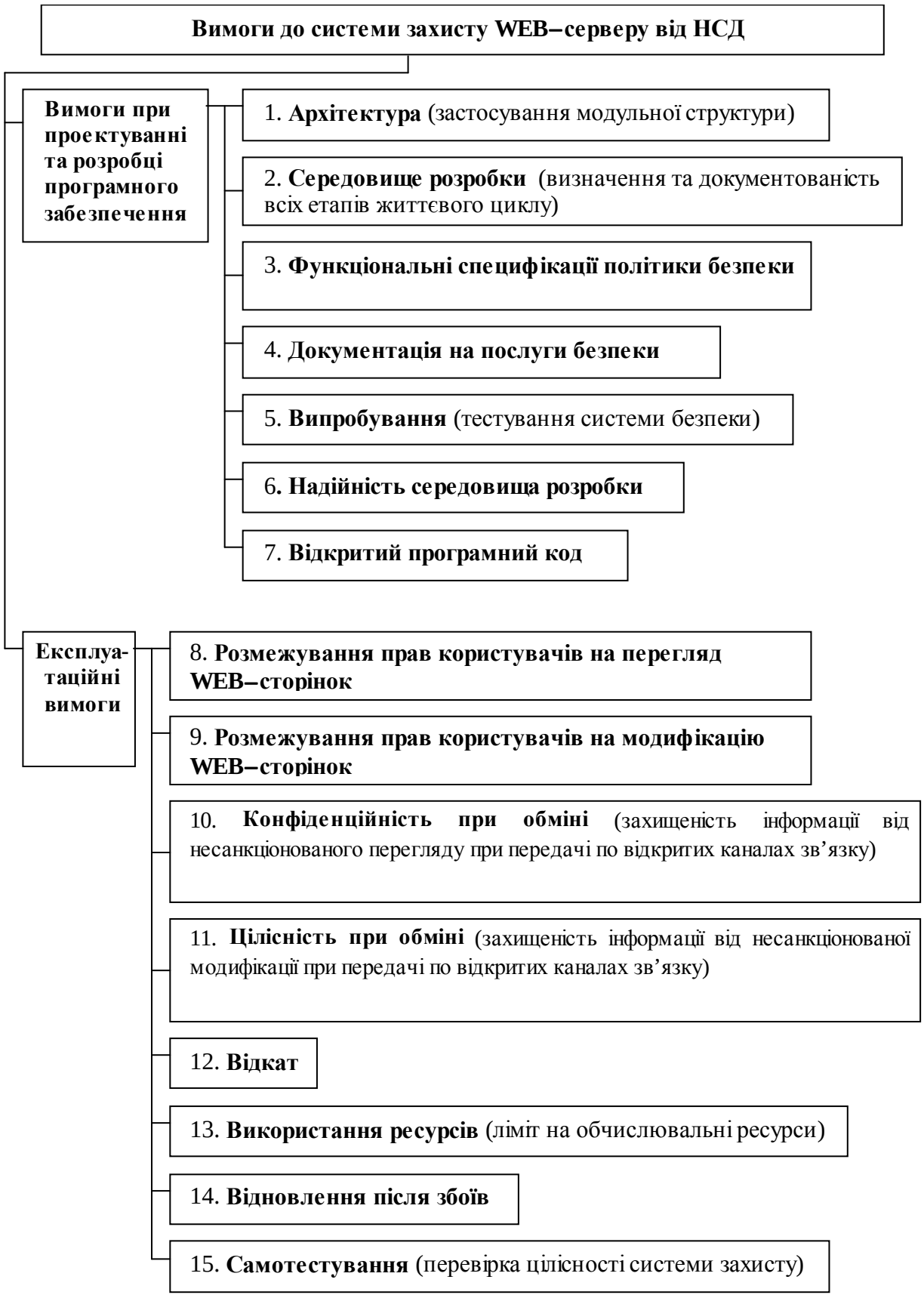

Рис. 1. Структура типових вимог до системи захисту WEB–серверу від НСД

10. Обидва WEB–сервери дозволяють забезпечити захист інформації від несанкціонованого ознайомлення під час їх експорту/імпорту через незахищене середовище. Для цього використовуються комунікаційний протокол SSL, що використовує метод шифрування з відкритим ключем. В Apache протокол SSL реалізований декількома способами, серед яких Apache – SSL та різноманітні комерційні варіанти. Таким чином, $Z^a_{w10} = Z^i_{w10} = 1$.

11. Використання протоколу SSL дозволяє системам захисту Apache і IIS забезпечити надійний контроль за цілісністю інформації в повідомленнях, які передаються, а також здатність виявляти факти їх несанкціонованого видалення або дублювання. Тому $Z^a_{w11} = Z^i_{w11} = 1$.

12. Відкат забезпечує можливість відмінити окрему операцію або послідовність операцій і повернути захищений об'єкт після внесення до нього змін до попереднього наперед визначеного стану. Для забезпечення відкату до складу WEB–серверу повинні входити автоматизовані засоби, які дозволяють адміністратору безпеки відмінити певний набір операцій, виконаних над захищеним об’єктом WEB-сторінки за певний проміжок часу. Факт використання послуги має реєструватись у системному журналі. Програмне забезпечення Apache та IIS дозволяє забезпечити відкат, тому $Z^a_{w12} = Z^i_{w12} = 1$.

13. Визначення ліміту на обчислювальні ресурси означає можливість обмеження щодо використання окремим користувачем та/або процесом обсягів обчислювальних ресурсів серверу. Спроби користувачів перевищити встановлені обмеження на використання ресурсів повинні реєструватися в системному журналі. Обидва WEB–сервери дозволяють визначити кількість обчислювальних потоків, розмір буфера пам’яті, що використовується протоколом TCP/IP, розмір тіла запиту HTTP, розмір черги мережевих з’єднань. Тому $Z^a_{w13} = Z^i_{w13} = 1$.

14. Відповідність вимозі відновлення після збоїв означає визначення множини типів відмов WEB-серверу і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Аналіз документації обох WEB-серверів та практичний досвід показує, що повернення у відомий захищений стан після збоїв відбувається без порушення політики безпеки. Тому $Z^a_{w14} = Z^i_{w14} = 1$.

15. Самотестування повинно дозволяти WEB-серверу перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій захисту. Аналіз документації та функціональних можливостей Apache та IIS показав відсутність в них можливості самотестування. По цій причині $Z^a_{w15} = Z^i_{w15} = 0$.

Підсумовуючи проведений аналіз та використавши (10), розрахуємо інтегральну оцінку системи захисту Apache (Z^a_w) та IIS (Z^i_w). Отже, $Z^a_w = 14$, $Z^i_w = 13$. Відзначимо, що відповідно методиці [2] та вітчизняним стандартам [3], для обох WEB-серверів максимально можлива величина інтегральної оцінки дорівнює 15. Порівняння одержаних реальних величин цієї оцінки з максимально можливою вказує на досить високу захищеність як Apache, так і IIS від НСД. Крім того, результати порівняння вказують на дещо кращу захищеність Apache завдяки наявності відкритого програмного коду, хоча це і не вимагається у вітчизняних стандартах. Відзначимо, що наявність відкритого програмного коду, на наш погляд, є досить важливою вимогою до системи захисту WEB–серверу. Наприклад, тому, що унеможливлює створення різноманітних програмних пасток розробниками WEB–серверу.

Важливим напрямком підвищення рівня захисту від НСД як Apache, так і IIS є введення в них функцій самотестування та відображення в супроводжуючій документації програми і методики тестувань системи безпеки та етапів життєвого циклу.

Для порівняння можливостей типових засобів захисту WEB–серверів Apache та IIS від описаних атак на від-

мову були проведені числові експерименти. Як доведено в [5], найбільш небезпечною є атака з використанням тільки відкриття файлів по протоколу HTTP. Тому для визначення ефективності захисту план експерименту передбачав тільки відкриття HTML- та PHP-файлів. Для здійснення атаки засобами Microsoft VC++.NET було розроблено спеціальну прикладну програму. Ефективність та надійність функціонування програми була забезпечена за допомогою бібліотеки для роботи з Інтернет afxinet. Основними етапами роботи програми є відкриття сесії, багаторазовий доступ до файлу по протоколу HTTP в циклі з визначеною кількістю ітерацій, закриття сесії та обчислення терміну виконання циклу. В якості WEB- серверу використано Apache 1.3 та IIS 5.0, які працювали на комп'ютері Intel Pentium 3 (тактова частота – 600 МГц, обсяг оперативної пам'яті – 256 Мб) під керуванням операційної системи Microsoft Windows 2000 Server. Атака здійснювалась з використанням одного комп'ютера з аналогічними характеристиками під керуванням операційної системи Microsoft Windows 2000 Professional. Експеримент проводився в локальній мережі з топологією "зірка" з пропускною здатністю 100 Мбіт/с. Відзначимо, що WEB-сервер знаходився на комп'ютері сервері домена. Під час проведення експериментів в мережі працювали тільки комп'ютери, які брали участь у експерименті. Реєстрація параметрів використання системних ресурсів комп'ютерів здійснювалась програмно (термін виконання запитів) та за допомогою Windows Task Manager (навантаження процесора). Кожен експеримент повторювався тричі за тих самих вихідних даних. При цьому в різних експериментах величини зареєстрованих параметрів відрізнялись на 3-5%. Крім того, були розраховані середньоарифметичні величини зареєстрованих параметрів. Таким чином, похибка отриманих результатів знаходиться в межах 5%, що вважається прийнятною при інженерних розрахунках. Основні результати експериментів представлені в табл. 1, 2 та показані на рис. 2.

Дані табл. 1 показують, що для обох WEB–серверів для повного блокування сайту достатньо здійснити близько 1000 циклічних процедур відкриття/закриття для HTML-файлів та 100 аналогічних процедур для PHP-файлів.

Аналіз тривалості виконання Web-сервером клієнтських запитів (табл. 2, рис. 1) вказує на різке зростання терміну

Таблиця 1. **Показники навантаження процесора комп'ютера Web – сервера**

Кількість з'єднань	Завантаження процесора			
	Відкриття/закриття HTML-файлу		Відкриття/закриття PHP-файлу	
	Apache	IIS	Apache	IIS
1	2	2	2	2
10	12	6	30	86
100	42	34	100	100
1000	100	100	100	100
10000	100	100	100	100

Таблиця 2. **Термін виконання Web-сервером клієнтських запитів**

Кількість з'єднань	Термін виконання запиту			
	Відкриття/закриття HTML-файлу		Відкриття/закриття PHP-файлу	
	Apache	IIS	Apache	IIS
1	0,09	0,09	0,1	0,1
10	0,12	0,12	1	1
100	1	0,4	6	6
1000	5	2	67	63
10000	41	18	673	638

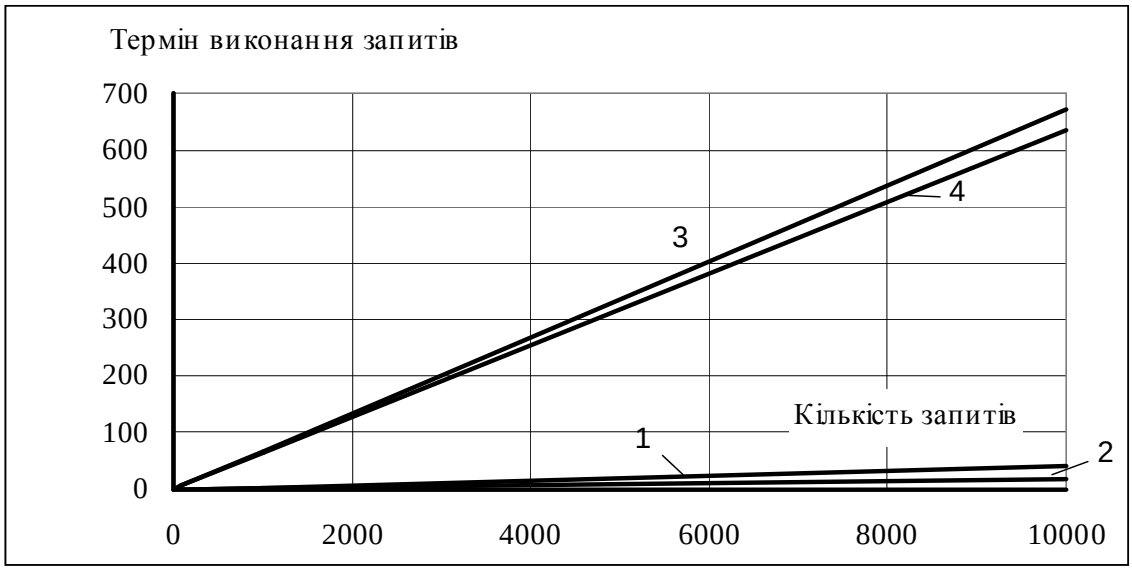

Рис.2. Графіки залежностей термінів виконання WEB–сервером запитів відкриття/закриття HTML- та PHP-файлів від кількості запитів:
1 – HTML-файл WEB–серверу Apache; 2 – HTML-файл WEB–серверу IIS; 3 – PHP-файл WEB–серверу Apache; 4 – PHP-файл WEB–серверу IIS

виконання запиту сервером при зверненні до PHP-файлів відносно HTML-файлів. При здійсненні атаки шляхом відкриття PHP-файлів термін блокування сервера в 19 – 20 разів триваліший, ніж при атаці шляхом відкриття HTML-файлів. Можна відзначити, що для обох WEB–серверів термін виконання запитів до PHP- файлів приблизно однаковий. У той же час термін виконання запитів до HTML-файлів IIS більше, ніж в 2 рази менший ніж в Apache.

Для порівняння захищеності Apache та IIS згідно (4 – 7) було розраховано показники ефективності захисту PHP та HTML-файлів. Результати розрахунків наведеані в табл.3.

Аналіз даних табл.3 показує, що для HTML-файлів ефективна потужність захисту IIS приблизно в 1.2 рази вища, ніж у Apache, а показник ефективності захисту від блокування IIS вищий більш ніж у 2 рази від аналогічного показника Apache. При цьому показники ефективності захисту при атаці на PHP–файли для обох WEB–серверів приблизно однакові.

Відзначимо, що зміна конфігурації та характеристик апаратно-програмного забезпечення комп'ютерної мережі може досить відчутно вплинути на кількісні показники результатів атаки (термін виконання запиту, навантаження процесора). Проте вплив такої зміни на показники ефективності захисту WEB–серверів, що носять відносний характер, не такий відчутний [4]. Тому якісна оцінка ефективності захисту Web-серверів, а також результат порівняння захищеності Apache та IIS відповідає дійсності.

Висновки з даного дослідження і перспективи подальших розвідок у цьому напрямку

- Визначена інтегральна оцінка ефективності захисту від НСД WEB-серверів Apache та IIS із урахуванням

Таблиця 3. **Показники ефективності захисту WEB–серверів**

WEB–сервер	Ефективна потужність захисту – Ω		Ефективність захисту від блокування – A	
	HTML–файлів	PHP – файлів	HTML–файлів	PHP – файлів
Apache	0,1429	0,04	0,0488	0,003
IIS	0,1765	0,04	0,1111	0,0031

відповідної вітчизняної нормативної бази: Apache $Z_{aw}=14$, IIS $Z_{iw}=13$. При цьому максимально допустима величина оцінки $Z_w=15$. Таким чином, ефективність захисту від НСД як Apache, так і IIS досить висока. Важливим напрямком підвищення рівня захисту від НСД для Apache і IIS є введення в них функцій самотестування та доукомплектація супроводжуючої документації відповідно вітчизняних державних стандартів.

- Проведено детальне порівняння захищеності WEB-серверів Apache та IIS від атак на відмову з санкціонованим використанням HTML-сторінок та серверних сценаріїв PHP.
- Доведено, що захищеність IIS від атак на відмову із санкціонованим використанням HTML-сторінок суттєво вища Apache.
- Доведено, що захищеність IIS та Apache від атак на відмову із санкціонованим використанням серверних сценаріїв PHP приблизно однакова.

Перспективи подальших розвідок у даному напрямі полягають в досліджені захищеності WEB–серверів Apache та IIS від атак на відмову із санкціонованим використанням серверних сценаріїв, що створені за допомогою загальнопоширених технологій. До таких слід віднести Java, ActiveX, SSI, ASP, C#. Результатом досліджень може стати універсальна система захисту WEB–серверів від атак на відмову. Крім того, цікавим напрямом дослідження в галузі захисту WEB–серверів від НСД з метою вдосконалення вітчизняної нормативної бази.

1. *Шохін Б.П., Юдін О.М., Мазулевський О.Є.* Вдосконалення контролю за станом захищеності ком'ютерної мережі на основі адаптивного моніторингу // Збірник наукових праць військового інституту телекомунікацій та інформатизації національного технічного університету України "КПІ". – 2004. – Вип. 4,– С.208-217.
2. *Хорошко В.О., Кудінов В.А.* Методичний підхід до формалізації задачі оцінювання ефективності системи захисту інформаційної системи ОВС України // Захист інформації. – 2004. – №4. - С.11-18.
3. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. к.: Держстандарт України. – 2003. – 16 с.
4. *Терейковський І.* Захист Web-сайтів корпоративних інформаційних систем від атак на відмову // Збірник наукових праць військового інституту телекомунікацій та інформатизації національного технічного університету України "КПІ". – 2004. – Вип. 4. – С.201-208.
5. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.– К.: Держстандарт України. – 1997. – 5 с.
6. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни і визначення. – К.: Держстандарт України. – 1998. – 12 с.
7. *Андрееев А.* Microsoft Windows 2000. – СПб.: БХВ–Петербург, 2002.– 960 с.
8. Уэйнпрат Питер. Apache для профессионалов. - М: Изд-во «Лори», 2001. – 473 с.

Отримано 13.12.04

Про автора
Терейковський Ігор Анатолійович
канд. техн. наук.
Місце роботи автора:
Київський національний торговельно–економічний університет, кафедра інформаційних технологій та систем,
Київ, вул. Кіото 19, к 526.
Тел.: (044) 531 4869.
E-mail: terejkowski@rambler.ru