МАТЕМАТИЧНА МОДЕЛЬ ОЦІНЮВАННЯ ЗАХИСТУ WEB-САЙТІВ

Ткаченко В.П., *зав. кафедри МСТ ХНУРЕ*
Огірко І.В., *професор, кафедра ОМТ УАД*
Огірко О.І., *ст. викладач, ЛДУВС*

На сьогоднішній день користувачі інтернет-ресурсів звертають особливу увагу на захист веб-сервісів [1-3]. Актуальними є якість захисту сайтів, зручність у користуванні, інформативність, дизайн тощо. Сервіс вебометричних досліджень наукових сайтів призначений для аналізу сайтів наукових організацій та інших наукових сайтів. Для розрахунку вебометричного рангу використовується наступна формула [1]:

$$WR = 5RankV + 2RankS + 1RankR + 1RankSc\,. \qquad (1)$$

Рейтинг сайтів надає найбільш повні актуальні відомості про стан їх сайтів з точки зору кіберметрія. Для цього проводиться щотижневе оновлення рейтингу і збереження історії змін індикаторів [1,2]. Методика розрахунку рейтингу аналогічна.WEB-сторінка установи може бути розміщена на власному сервері або на сервері, що є власністю оператора. У випадку користування послугами оператора щодо розміщення, експлуатації та адміністрування WEB-сторінки власник інформації укладає з оператором договір, яким визначаються права і обов'язки сторін, умови підключення, розміщення інформації та забезпечення доступу до неї, інші питання, що вимагають урегулювання між власником інформації WEB-сторінки та оператором, виходячи з вимог законодавства у сфері захисту інформації.

До складу АС, яка забезпечує функціонування WEB-сторінки, входять:

– ОС;

– фізичне середовище, в якому вона знаходиться і функціонує;

– середовище користувачів;

– оброблювана інформація, у тому числі й технологія її оброблення.

Під час забезпечення захисту інформації мають бути враховані всі характеристики зазначених складових частин, які впливають на реалізацію політики безпеки WEB-сторінки. У випадку, якщо WEB-сторінка містить посилання на інформаційні ресурси іншої WEB-сторінки, умови функціонування останньої не повинні порушувати встановлену для даної WEB-сторінки політику безпеки [1-3].

Технологічна інформація призначена для використання тільки уповноваженими користувачами з числа співробітників СЗІ та персоналу, що забезпечує функціонування АС. Способи і методи обробки інформації WEB-сторінки визначають технології оброблення інформації. Технологічні особливості роботи користувачів із загальнодоступною інформацією WEB-сторінки визначаються особливостями системного та функціонального ПЗ, зокрема браузерів, які ними використовуються. Технологічні особливості

роботи користувачів інших категорій визначаються, крім того, архітектурою, способами оброблення та передавання інформації між компонентами і способами здійснення доступу до неї [1-3].

Можливі наступні способи здійснення доступу до технологічної інформації та передавання даних для актуалізації загальнодоступної інформації:

– з робочої станції, розміщеної на тій самій території, що і WEB-сервер або з терміналу WEB-сервера;

– з робочої станції, яка розміщена на території установи-власника WEB-сторінки, до WEB-сервера, що розміщений на території оператора, з використанням мереж передачі даних.

Технологія оброблення інформації повинна бути здатною реалізовувати можливість виявлення спроб несанкціонованого доступу до інформації WEB-сторінки та процесів, які з цією інформацією пов'язані, а також забезпечити реєстрацію в системному журналі визначених політикою відповідної послуги безпеки подій. Технологічними процесами повинна бути реалізована можливість створення резервних копій інформації WEB-сторінки та процедури їх відновлення з використанням резервних копій. Технологія оброблення інформації повинна передбачати можливість аналізу використання користувачами і процесами обчислювальних ресурсів і забезпечувати керування ресурсами [1-3].

Підсистема обробки інформації забезпечує створення, зберігання, актуалізацію інформації WEB-сторінки і складається із засобів обробки інформації, системного та функціонального ПЗ.

До засобів обробки інформації належать WEB-сервер та необхідна кількість робочих станцій для забезпечення всіх функцій щодо супроводження WEB-сторінки та захисту інформації. Програмно-апаратні засоби захисту повинні мати належним чином оформлені документи, які засвідчують відповідність цих засобів вимогам нормативних документів.

За рівнем повноважень щодо доступу до інформації, характером та складом робіт, які виконуються в процесі функціонування, користувачі поділяються на такі категорії [1-3]:

а) користувачі, яким надано право доступу тільки до загальнодоступної інформації WEB-сторінки;

б) користувачі, яким надано повноваження супроводжувати (адміністратор безпеки, користувачі з функціональними обов'язками WEB-майстрів, адміністраторів сервісів, адміністраторів мережевого обладнання, адміністраторів ресурсів, якщо передбачається їх взаємодія з WEB-сторінкою, тощо);

в) технічний обслуговуючий персонал, що забезпечує належні умови функціонування АС, повсякденну підтримку життєдіяльності фізичного середовища;

г) розробники ПЗ, які здійснюють розробку та впровадження нових функціональних процесів, а також супроводження вже діючого функціонального ПЗ сервера, розробники та проектанти фізичної структури АС;

д) постачальники обладнання і технічних засобів та фахівці, що здійснюють його монтаж, поточне гарантійне й післягарантійне обслуговування.

Доступ до інформації WEB-сторінки повинен надаватися користувачам у відповідності до положень політики безпеки інформації, визначеної для АС, що забезпечує функціонування WEB-сторінки. Обов'язковою є реєстрація користувачів, що належать до категорії, чим забезпечується можливість однозначного їх ідентифікування, а також їхніх дій щодо інформації WEB-сторінки. Для встановлення правил та регламентації доступу цих користувачів до інформації WEB-сторінки розробляються та впроваджуються нормативні та розпорядчі документи, передбачені планом захисту інформації. Користувачі загальнодоступної інформації одержують доступ до WEB-сторінки у відповідності до діючих у мережі Інтернет правил та регламенту[1-3].

Політика безпеки інформації повинна поширюватися на об'єкти комп'ютерної системи, які безпосередньо чи опосередковано впливають на безпеку інформації [1-3].

До таких об'єктів належать:

– адміністратор безпеки;

– користувачі, яким надано повноваження забезпечувати управління;

– користувачі, яким надано право доступу до загальнодоступної інформації;

– інформаційні об'єкти, що містять загальнодоступну інформацію;

– засоби адміністрування і управління обчислювальною системою та технологічна інформація, яка при цьому використовується;

– обчислювальні ресурси, наприклад, дисковий простір, тривалість сеансу роботи користувача із засобами АС, час використання центрального процесора та ін.

За власником WEB-сторінки залишається право реалізації, у разі необхідності, окремих послуг безпеки інформації зазначених профілів з більш високим рівнем, доповнення цих профілів іншими послугами, а також реалізація послуг безпеки з більш високим рівнем гарантій.

Політика мінімальної адміністративної цілісності стосується:

– користувачів усіх категорій;

– загальнодоступної інформації WEB-сторінки;

– файлової системи та функціонального ПЗ, що використовується для актуалізації, захисту загальнодоступної інформації та супроводження WEB-сторінки.

Користувачам, які мають доступ тільки до загальнодоступної інформації WEB-сторінки, забороняється модифікувати будь-які захищені об'єкти.

Адміністратору безпеки надається право модифікувати функціональне ПЗ, що використовується для захисту загальнодоступної інформації, та технологічну інформацію КСЗІ.

Користувачам, що мають повноваження щодо управління АС, надається відповідно до функціональних обов'язків, право модифікувати технологічну інформацію та функціональне ПЗ, що використовується для актуалізації загальнодоступної інформації та супроводження WEB-сторінки.

Права доступу до захищених об'єктів WEB-сторінки повинні встановлюватися в момент їх створення або ініціалізації. Обмеження щодо використання окремим користувачем та/або процесом обсягів обчислювальних ресурсів або кількості об'єктів встановлюються адміністратором безпеки або користувачами, яким надано повноваження щодо управління.

Реєстрація всіх подій, що мають безпосереднє відношення до безпеки, здійснюється в журналі реєстрації, який повинен містити інформацію стосовно дати, часу, місця, типу і наслідків зареєстрованої події, ім'я (IP-адресу) та/або ідентифікатор причетного до цієї події користувача. Реєстраційна інформація повинна бути достатньою для однозначної ідентифікації користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.

Автентифікація користувачів, що мають виключне право доступу тільки до публічної інформації, не здійснюється. Адміністратору безпеки дозволяється доступ до всієї інформації WEB-сторінки. Повноваження всіх інших користувачів щодо доступу до інформації надаються їм адміністратором безпеки. Політика самотестування поширюється на адміністратора безпеки, компоненти системного та функціонального програмного забезпечення, засоби захисту інформації. Склад послуг безпеки, а також механізмів захисту, що реалізують кожну з послуг, визначається політикою безпеки інформації і повинен відповідати її вимогам. Використання таких засобів можливе за умови вилучення цих функцій або гарантування неможливості їх активізації.

Список літератури

1. Пелещишин, А.М. Позиціонування сайтів у глобальному інформаційному середовищі / А.М. Пелещишин. – Львів: Видавництво Львівської політехніки, 2007. – 260 с.

2. Паславська, І. Інформаційна система оцінки якості електронних видань / І. Паславська, І. Огірко, О. Пілат // Моделювання економіки: проблеми, тенденції, досвід. – 2013. – С. 92-94.

3. Огірко, І. Інформаційні технології безпекометрії в поліграфії / І. Огірко, О. Огірко // ІІІ Міжнародна науково-технічної конференції «Захист інформації і безпека інформаційних систем»; 05 – 06 червня. – Львів, 2014. –С. 46-51.