УДК 004.056

Т.М. Долінський, А.М. Стефанів, І.В. Миколюк, В.М. Бревус
Тернопільський національний технічний університет імені Івана Пулюя, Україна

АУДИТ БЕЗПЕКИ WEB-РУСУРСІВ

T.M. Dolinskii, A.M. Stefaniv, I.V. Mykoliuk, V.M. Brebvus

SECURITY AUDIT WEB-RESOURCES

Інтернет, якщо задуматися, це набагато більше, ніж можливість зайти і щось подивитися-пошукати. Це не тільки середовище, в якому відбувається обмін інформацією, а й простір взаємодії і надання послуг в найширшому сенсі цього слова.

Аудит безпеки - це послуга, призначена для підвищення рівня безпеки веб-сайту та веб-додатків. Кожен власник веб-сайту може звернутися за даною послугою, щоб перевірити власний сайт на наявність вразливостей.

Проблема створення безпечного веб-ресурсу є комплексною і актуальною задачею. Необхідно використовувати потенційні можливості актуальних технологій розробки та надання доступу користувачам під час створення рішення. І дуже важливо розуміти способи використання цих інструментів для боротьби із загрозами.

У 2010 році Міжнародна організація по стандартизації опублікувала стандарт ISO/IEC 27003 «IT Методи і засоби забезпечення безпеки СУІБ - Керівництво по реалізації СУІБ».

Документ розглядає питання успішної розробки і впровадження СУІБ відповідно до вимог ISO/IEC 27001. Стандарт описує процес формування вимог і проектування СУІБ від початку проекту і до підготовки планів впровадження. Описано процес отримання згоди керівництва на впровадження СУІБ, дається деталізація проекту впровадження СУІБ, рекомендації з планування проекту впровадження СУІБ, результатом якого є остаточний план впровадження СУІБ.

В ISO розробляються два стандарти, спрямовані на те, щоб звести до мінімуму «найсерйозніші ризики, що пов'язані з хмарними обчисленнями»: відсутність керівництва (governance) та відсутність управління.

Перший планується опублікувати в кінці 2015 року, нова специфікація спиратиметься на положення інших стандартів сімейства ISO 27000, в тому числі ISO 27018, який стосується приватності в хмарних обчисленнях; ISO 27031, що належить до безперервності бізнесу; ISO 27036-4, регулюючого процеси управління взаємовідносинами.

Другий новий стандарт, ISO 27018, служитиме «зведенням правил щодо захисту персональної інформації в загальнодоступних хмарах, граючих роль обробників такої інформації». Цей документ стане доповненням до ISO 27017, який охоплюватиме ширші аспекти інформаційної безпеки. Проект отримав широку підтримку з боку організацій по стандартизації різних країн, а також Cloud Security Alliance.

Під час розробки рішень рекомендовано звернути увагу на рекомендації відкритих некомерційних організацій, що де-факто долучаються до стандартизації галузі інформаційної безпеки: ISECOM (Institute for Security and Open Methodologies) та OWASP (Open Web Application Security Project).