УДК 681.3.067

ВЕБ-СИСТЕМА ТЕСТУВАННЯ ЯКОСТІ ЗНАНЬ НА ОСНОВІ АСИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ ТЕХНОЛОГІЙ, ЩО ВИКОРИСТОВУЮТЬ РЕКУРЕНТНІ ПОСЛІДОВНОСТІ

К. т. н. Ю. Є. Яремчук

Вінницький національний технічний університет
Україна, м. Вінниця
yurevyar@vntu.net

У роботі представлено систему тестування якості знань з використанням крос-платформних рішень та веб-технологій, яка забезпечує надійний захист тестування та має гнучкий доступ кандидатів до системи тестування. При цьому усі необхідні асиметричні криптографічні технології розроблено на основі власних методів, що базуються на єдиному математичному апараті рекурентних V_k-послідовностей. Це дозволило підвищити рівень безпеки та швидкість системи тестування.

Ключові слова: тестування якості знань, веб-система, криптографія, рекурентні послідовності.

Найбільш сучасним методом контролю знань є тестування [1]. Це пов'язано з тим, що поширення систем дистанційного навчання [2, 3] потребує якісного контролю знань. Всі міжнародні компанії та найвідоміші університети давно перейшли до такого виду контролю знань. Це дозволило досить просто, швидко та об'єктивно оцінювати знання, оскільки в тестуванні присутні різноманітні комплексні завдання, які можуть поєднувати в собі як теоретичний, так і практичний матеріал.

Одним із суттєвих недоліків сучасних комп'ютерних систем тестування [4, 5] є прив'язка клієнтського додатку до платформи та операційної системи, під які вона реалізується, що тим самим обмежує клієнтські додатки щодо програмного середовища використання. Окрім цього існує проблема безпеки систем тестування, оскільки кожна операційна система має свої власні вразливості, які можуть впливати на роботу програмного продукту. Забезпечення безпеки системи тестування є дуже актуальним, оскільки під час контролю якості знань здійснюється зберігання і обробка бази з тестами та правильними відповідями, а також результатів тестування кандидатів, тому порушення конфіденційності та цілісності цих баз і результатів може звести нанівець весь процес тестування знань.

Мета роботи – розробка системи тестування якості знань, яка б забезпечувала надійних захист тестування та гнучкий доступ кандидатів до системи тестування без прив'язування до конкретної платформи чи операційної системи.

Для розробки системи тестування пропонується використати крос-платформні рішення, які мають широкі можливості щодо побудови захищених систем з високим рівнем безпеки, що значно підвищує загальну безпеку процесу тестування та унеможливлює виникнення неконтрольованого втручання. Також крос-платформні рішення дозволяють будувати гнучкі системи з можливістю легкого та швидкого перенесення середовища тестування з одного сервера на інший і при цьому не зважати уваги на саму операційну систему (Windows, Linux, Unix), її версію та середовище обробки вебсторінок (IIS, Apatch).

Розробку системи тестування здійснено з використанням веб-технологій у вигляді веб-додатку, що дозволяє використовувати її на будь-якому пристрої, який буде підключений до глобальної мережі Інтернет або локальної мережі з використанням власного веб-серверу. Функціонал веб-системи тестування забезпечує виконання таких дій: реєстрація та авторизація користувачів, ідентифікація робочої станції користувача, створення та модифікація бази даних тестів, тестування та зберігання результатів, захист даних, що передаються та зберігаються.

Модуль, що безпосередньо реалізує систему тестування, та модуль адміністрування розроблено окремо один від одного, оскільки механізм адміністрування в основному є незмінним, в той час як процес тестування може потребувати модифікацій для додавання якихось нових функціональних

особливостей. Досить важливим функціоналом при розробці веб-системи тестування є розподілення прав доступу. Це також потребує окремої, незалежної програмної реалізації, так як даний модуль буде досить часто використовуватись і постійно контролювати всі дії користувачів. Розроблено структурну схему веб-системи тестування з відображенням модулів та взаємодії між ними, та здійснено реалізацію усього необхідного функціоналу та відповідних програмних модулів.

Оскільки такі функціональні дії як авторизація, ідентифікація і захист даних, що передаються та зберігаються, потребує використання криптографічних перетворень, доцільним є створення одного єдиного криптографічного модуля, який буде реалізовувати технології різного криптографічного призначення. При цьому такі модулі як авторизація та ідентифікація робочих станцій реалізовані окремо і пов'язані з криптографічним модулем. Незалежна реалізація цих модулів істотно підвищує загальну безпеку системи, так як успішна атака на модуль авторизації або ідентифікації не дозволяє зловмиснику отримати повноцінний доступ до веб-системи тестування.

Розроблено захищену веб-систему тестування, в якій усі технології криптографічного захисту, як то асиметричне шифрування, розподіл ключів, автентифікація та цифрове підписування є власними і їх реалізовано на єдиному математичному апараті рекурентних V_k-послідовностей. Це надає додаткові переваги реалізації, оскільки використання єдиного апарату значно спрощує процедури вибору параметрів, а також надає можливість використання проміжних результатів обчислення елементів рекурентних послідовностей для криптографічних застосувань різного призначення, що, в свою чергу, дозволяє підвищити швидкість виконання криптографічних перетворень в цих застосуваннях.

Таким чином, запропонована реалізація системи тестування з використанням кросплатформних рішень забезпечує високий рівень безпеки системи тестування, а також реалізацію вебтехнологій, що забезпечує гнучкий доступ кандидатів до системи тестування. Розроблено механізми захисту бази даних та даних, що передаються у системі тестування між клієнтами-користувачами та сервером. Усі необхідні технології криптографічного захисту розроблено на основі власних методів на єдиному математичному апараті рекурентних V_k-послідовностей, що дозволило не лише підвищити рівень безпеки системи тестування, але й підвищити в ній швидкість виконання криптографічних перетворень.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Кабанова Т. А., Новиков В. А. Тестирование в современном образовании. Учебное пособие.— Москва: Высшая школа, 2010.— 384 с.

2. Ибрагимов, И. М. Информационные технологии и средства дистанционного обучения: Учебное пособие для студ. вузов.— Москва: Академия, 2005.— 336 с.

3. Агапонов С. В., Джалиашвили З. О., Кречман Д. Л. и др. Средства дистанционного обучения. Методика, технология, инструментарий.— Санкт-Петербург: БХВ-Петербург, 2003.— 336 с.

4. Батешов Е. А. Основы технологизации компьютерного тестирования. Учебное пособие.— Астана: ТОО «Полиграф-мир», 2011.— 241 с.

5. Калюжный, А. С. Компьютерное тестирование как способ контроля знаний студентов // Высшее образование сегодня.— 2009.— № 7.— С. 67—68.

———————

Iu. E. Iaremchuk

Web-system of knowledge quality testing based on asymmetric cryptographic technologies that use recurrent sequences.

The paper presents the testing system of knowledge quality, using cross-platform solutions and web-technologies, which provides reliable testing protection and has a flexible access system for the candidates, without linking to a particular platform or operating system. We have prepared a structural scheme of the secure web-based testing system and the interrelation between its components. At the same time, all the necessary technologies of asymmetric encryption, key distribution, authentication and digital signature were developed on the basis of our own methods, that are based on a single mathematical apparatus of recurrent V_k- sequences. This allowed us not only to improve the testing system security, but also to increase its speed of cryptographic transformations.

Keywords: *testing the quality of knowledge, web system, asymmetric cryptography, recurrent sequences.*