покера, тест на подпоследовательности одинаковых бит, тест на длинные подпоследовательности одинаковых бит. Данная система была выбрана для исследования ГСЧ.

Для реализации тестов стандарта FIPS 140-2 была использована среда программирования JavaScript. JavaScript – язык программирования высокого уровня, позволяющий получить собственный программный продукт тестирования с возможностью размещения программы на Web-серверах.

В докладе приводятся результаты тестирования ГСЧ по системе FIPS 140-2, полученные с использованием языка программирования JavaScript. Полученные результаты могут быть успешно использованы при формировании носителей ключевой информации, которые выполнены с применением языка JavaScript.

Литература

1. Federal Information Processing Standards Publication 140-2. Security Requirements for Cryptographic Modules //NIST [Electronic resource]. – 2001. – Mode of access: http://mayor.fri.utc.sk/v731/04/fips140-2.pdf. – Date of access: 24.03.2015.

THE PARTICULARS OF ELECTRONIC SHOP PROGRAM APPLICATION

V.A. Vishnyakov, M. Forootan

The report presents the results of electronic shop development. It was designed and worked out the program application for E-commerce, which the following requirements are corresponded:

− flexibility and university – the program application is maximum connected to management system of site, on the base of which the electronic shop was created;

− correctness – the user and administrator have possibilities for changing the program application by simple correction of настроек;

− functionality – the program application supports all users, who will bay products in this E-shop;

− standardization – the accordance to the common conception of standard services using in the management system of site.

The distinction features and positive particulars the created program application are: to easy integration with others applications like 1C ERP system; unique platform is used to create own information management and support its with small spending; the realizing features of multy currency and multy languages allow to use the program application in other counters; the realizing additional marketing tool allow to see new goods and goods which are the lieder of sales.

ANALYSIS OF INFORMATION SECURITY IN E-COMMERCE

V.A.Vishnyakov, M. Forootan

The report presents the results of analysis of the information security in electronic commerce (EC). It is identified the following areas: threats and technologies for their prevention, action to protect in EC, protection services for the EC, two encryption technologies (symmetric and asymmetric), the use of firewalls, digital signature technology, secure protocols: Secure HTTP (S-HTTP), Secure Sockets Layer (SSL), Secure Electronic Transaction (SET).

The threat of information in EC: data intentionally intercept, read or write; users identify themselves no correctly (with fraudulent goals); user gains unauthorized access from one network to another. Actions to protect are the following: data encryption that prevents their reading or distortion; authentication of the sender and the recipient is carried out with digital signature technology (DST); filtering traffic entering the network or the server is protected by a firewall. Cryptographic technology provides three basic types of services for e-commerce: authentication (which includes identification), inability to refrain from executing and secrecy.

Technology DST includes: the using of hash-function for obtained Digest (uniquely condensed version of the original text); the digest is encrypted using the sender private key and becomes the digital signature; last is sent along with the original text (encrypted by symmetric algorithm) to

receiver. On the second side the receiver decrypts the digest, compares it with the decrypted text, in case of mismatch, there has been a security breach. Some data protection standards for EC include secure protocols: S-HTTP (secure HTTP), SSL (an integral part of all known browsers and Web servers.), SET (used for operations with credit cards.).