Universitatea Tehnică a Moldovei

# DEZVOLTAREA INSTRUMENTELOR DE PROTECŢIE CRIPTOGRAFICA PENTRU UN SERVER WEB

**Masterand:**

**Mamei Alexandr**

**Conducător:**

**conf. univ., dr. Puşneac Iurie**

**Chişinău-2018**

**Ministerul Educației, Culturii și Cercetării al Republicii Moldova**
**Universitatea Tehnică a Moldovei**

**Facultatea Electronică și Telecomunicații**

**Programul de masterat „Sisteme și comunicații electronice”**

**Admis la susţinere**
**Şef de departament: conf. univ., dr. Şestacov Tatiana**
**„ ” 2018**

# DEZVOLTAREA INSTRUMENTELOR DE PROTECŢIE CRIPTOGRAFICA PENTRU UN SERVER WEB

**Teză de master**

**Masterand:** **Mamei Alexandr**

**Conducător:** **conf. univ., dr. Puşneac Iurie**

**Chişinău-2018**

# А Н Н О Т А Ц И Я

Данный дипломный проект посвящен вопросу разработки средств криптографической защиты для веб-сервера.

В работе приведён анализ средств криптографической защиты криптосистем PKI, RSA, SSL. Разработаны центры сертификации для выпуска SSL сертификатов. Проведена конфигурация для расширения в openssl для включения нескольких DNS-имен в сертификат.

Представлен процесс установления, запуска и конфигурирования локального Web Server на открытой платформе Open Server.

Результатом проделанной работы служит демонстрация защищенного соединения между сервером и клиентом (веб-сайтом).

Дипломная работа содержит 64 страницы, 51 рисунок, 9 литературных источников.

# A D N O T A R E

Aceasta Teza de master este consacrată problemei dezvoltării instrumentelor de protecție criptografică pentru un server web.

În lucrare este dată analiza mijloacelor de protecție criptografică a cripto sistemelor PKI, RSA, SSL. Centrele de certificare au fost dezvoltate pentru emiterea certificatelor SSL. Configurația pentru extensia în openssl a fost efectuată pentru a include mai multe nume DNS în certificat.

Se prezintă procesul de stabilire, pornire și configurare a unui server Web local pe o platformă deschisă de Open Server.

Rezultatul muncii efectuate este demonstrarea unei conexiuni sigure între server și client (site web).

Teza de master conține 64 de pagini, 51 figuri, 9 referințe.

# ANNOTATION

This master thesis is devoted to the development of cryptographic protection tools for a web server.

In the work the analysis of means of cryptographic protection of cryptosystems PKI, RSA, SSL is given. Certification centers have been developed for issuing SSL certificates. The configuration for the extension in openssl was performed to include several DNS names in the certificate.

The process of establishing, starting and configuring a local Web Server on an open platform of Open Server is presented.

The result of the work done is the demonstration of a secure connection between the server and the client (web site).

The master thesis contains 64 pages, 51 figures, 9 references.

# СОДЕРЖАНИЕ

# ВВЕДЕНИЕ

На сегодняшний день потребность в обмене сообщениями, в передаче и хранении информации возникает всё больше, и безопасность передачи данных одна из главных задач. Актуальность данной работы состоит в анализе, выборе и имплементации современных средств защиты данных. Причем речь идет не только о предотвращении утечки информации, а также о снижении объемов трафика и отражении атак на информационные ресурсы и оптимизации работы системы в целом.

Целью работы является разработка средств криптографической защиты для веб-сервера. Для достижения цели необходимо выполнить следующие задачи:

1. Анализ средств криптографической защиты соединения между сервером и клиентом (веб-сайтом).

2. Разработка корневого центра сертификации для выпуска SSL сертификата высшего порядка.

3. Разработка промежуточного центра сертификации для пользовательского SSL сертификата.

4. Установить, запустить и сконфигурировать веб сервер, создать сайт.

5. Произвести установку сертификатов на веб сервере для осуществления работы по протоколу https.

6. Произвести практическую проверку работоспособности системы.

Новизна и практическая ценность данной дипломной работы заключается в использовании криптографических инструментов ранее не использованных в процессе обучения, но имеющих огромный потенциал в современном цифровом мире. Современные области применения криптографических систем это компьютерные сети, internet как в случае данного диплома, а также дипломатия, разведка, военное дело, мобильная связь, радиосвязь, банковские системы, электронная коммерция, электронная почта, электронный документооборот, цифровые деньги, системы электронного голосования, защита персональных данных, защита программного обеспечения, системы управления и это не весь потенциал.

Личным вкладом автора работы является: создание собственных центров сертификации, на основе центров генерация секретных и публичных ключей, создание запросов и изготовление SSL сертификатов, запуск сервера и создание сайта для внедрения выпущенных сертификатов.

# БИБЛИОГРАФИЯ


1. Вильям Столингс. Основы защиты сетей. Приложения и стандарты. 432 стр., 2002.
2. Бехроуз А. Фороузан. Криптография и безопасность сетей 783 стр., 2010
3. https://www.openssl.org/
4. https://blog.regolit.com/
5. https://ospanel.io/
6. https://www.emaro-ssl.ru/blog/convert-ssl-certificate-formats/
7. http://codare-date.cpf.ro/criptare-simetrica.php
8. http://www.danvasilache.info/eGA1.pdf
9. http://www.cs.ubbcluj.ro/~rlupsa/works/retele/retele-cripto.pdf