МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра математического моделирования и анализа данных

ПАВЛОВ КОНСТАНТИН ВЛАДИМИРОВИЧ

ЗАЩИТА XML-ДОКУМЕНТОВ

Аннотация к дипломной работе

Научный руководитель:
Агиевич Сергей Валерьевич,
кандидат физ.-мат. наук

Минск 2016

РЕФЕРАТ

Дипломная работа, 47 с., 3 рис., 1 табл., 18 источников.

XML-защита документов, XML Signature, XML Encryption, XAdES, ЭЦП, форматы ЭЦП.

Объект исследования – XML-защита документов.

Цель работы – изучить технологии XML Signature, XML Encryption и XAdES, провести анализ уязвимости и реализовать данные технологии при помощи отечественных криптографических алгоритмов.

Методы исследования – анализ международных стандартов по XML-защите документов, анализ существующих проектов по реализации данных стандартов, реализация собственного криптопровайдера и внедрение его в проекты по данным технологиям.

Результатом является надстройка над криптографической библиотекой bee2, которая реализует отечественные криптографические алгоритмы, интерфейсами языка Java и внедрение этой обвязки в библиотеку для создания расширенной ЭЦП.

Областью применения является электронный документооборот и любые сферы, где используются технологии по XML-защите документов, описанные в данном документе.

SUMMARY

Graduation assignment, 47 p., 3 pic., 1 t., 18 sources.

XML-document security, XML Signature, XML Encryption, XAdES, electronic signature, electronic signature formats.

Object of study – XML-document security.

Purpose – to research XML Signature technology, XML Encryption and XAdES, an analysis of vulnerability and implement these technologies using national cryptographic algorithms.

Research methods - analysis of the international standards for the protection of XML-documents, analysis of existing projects for the implementation of these standards, the implementation of their own CSP and its implementation in projects to these technologies.

The result is an add-on cryptographic library bee2, which implements the national cryptographic algorithms, with Java language interface and the usage of this add-on to the library to create enhanced electronic signature

The field of application is the electronic document and any areas where the use of technology for XML-document security, described in this document.