БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра дискретной математики и алгоритмики

Аннотация к магистерской диссертации

ДРЕВОВИДНЫЕ СТРУКТУРЫ ДАННЫХ В КРИПТОГРАФИИ

Павлов Константин Владимирович

Научный руководитель — кандидат физико-математических наук
С. В. Агиевич

2017

РЕФЕРАТ

Магистерская диссертация, 43 с., 5 рис., 13 источников.

XML-защита документов, XML Signature, XAdES, одноразовая ЭЦП, деревья Меркля.

Объект исследования: древовидные структуры данных в криптографии.

Цель работы: изучить технологии XML Signature и XAdES, провести анализ уязвимостей, реализовать криптопровайдер bee2j, изучить деревья Меркля, связанные с ними технологии и провести анализ уязвимостей этих технологий.

Результат: проведен аналитический обзор публикаций по деревьям Меркля; подготовлены материалы по технологии XAdES для разрабатываемого государственного стандарта; разработан криптопровайдер bee2j, который реализует отечественные криптографические алгоритмы в среде Java.

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

РЭФЕРАТ

Магістарская дысертацыя, 43 с., 5 мал., 13 крыніц.

XML-ахова дакументаў, XML Signature, XAdES, аднаразавы ЭЛП, дрэвы Меркля.

Аб'ект даследавання: дрэвападобныя структуры даных у крыптаграфіі.

Мэта работы: вывучыць тэхналогіі XML Signature і XAdES, правесці аналіз слабасцей, рэалізаваць крыптаправайдар bee2j, вывучыць дрэвы Меркля, звязаныя з імі тэхналогіі і правесці аналіз слабасцей гэтых тэхналогій.

Вынік: праведзены аналітычны агляд публікацый па дрэвах Меркля; падрыхтаваны матэрыялы па тэхналогіі XAdES для распрацоўванага дзяржаўнага стандарту; распрацаван крыптаправайдэр bee2, які рэалізуе айчынныя крыптаграфічныя алгарытмы ў Java.

Вобласць ўжывання: электронны дакументаабарот і любыя сферы, дзе выкарыстоўваюцца тэхналогіі па XML-ахове дакументаў, апісаныя ў дадзеным дакуменце.

ABSTRACT

The master's thesis, 43 pages, 5 figures, 13 literature references.

XML-document protection, XML Signature, XAdES, one-time EDS, Merkle trees.

Object of research: tree-like data structures in cryptography.

Objective: to learn XML Signature and XAdES technologies, to carry out vulnerability analysis, to implement bee2j crypto provider, to learn Merkle trees, related technologies and to analyze vulnerabilities of these technologies.

Result: an analytical review of publications on the trees of Merkle; materials on XAdES technology for the state standard being developed; an add-on has been developed cryptographic provider bee2j, which implements Belarussian cryptographic algorithms in Java.

The scope: electronic workflow and any areas where XML document security technologies described in this document are used.