МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Кафедра телекоммуникаций и информационных технологий

ГЕРАСИМЧИК
Тимофей Геннадьевич

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ЦИФРОВЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ В ОПЕРАЦИОННЫХ СИСТЕМАХ

Аннотация к дипломной работе

Научный руководитель – старший преподаватель Е.Е. Попко

Минск, 2022

РЕФЕРАТ

Дипломная работа: 99 с., 141 рис., 22 источника

ШИФРОВАНИЕ, ПОЛНОДИСКОВОЕ ШИФРОВАНИЕ, BITLOKER, LUKS, ЦИФРОВОЙ НОСИТЕЛЬ, EFS, FSCRYPT, DM-CRYPT, SECURE BOOT, SHIM, GRUB, VOLUME MASTER KEY, FULL DISK ENCRYPTION, TPM, ОПЕРАЦИОННЫЕ СИСТЕМЫ, WINDOWS, LINUX.

Целью дипломной работы является разработка программного модуля для изучения механизмов шифрования цифровых носителей информации в операционных системах.

Для достижения цели был проведен анализ существующих решений для полнодискового шифрования, описаны уязвимости и методы защиты от описанных уязвимостей. Были предложены и описаны практические методы усиления защиты полнодискового шифрования в операционных системах Windows и Linux, используя групповые политики безопасности и возможности модуля TPM для ОС Windows, а также механизм безопасной загрузки и сторонние утилиты для ОС Linux. В процессе подготовки практических заданий были исследованы возможности среды виртуализации и эмулируемого аппаратного комплекса.

Подготовленные задания и среда для их выполнения будут использованы в лабораторных работах по курсу «Безопасность информационных систем».

РЭФЕРАТ

Дыпломная работа: 99 с., 141 мал., 22 крыніцы

ШЫФРАВАННЕ, ПОЎНАДЫСКАВАЕ ШЫФРАВАННЕ, BITLOKER, LUKS, ЛІЧБАВЫ НОСЬБІТ, EFS, FSCRYPT, DM-CRYPT, SECURE BOOT, SHIM, GRUB, VOLUME MASTER KEY, FULL DISK ENCRYPTION, TPM, АПЕРАЦЫЙНЫЯ СІСТЭМЫ, WINDOWS, LINUX.

Мэтай дыпломнай працы з'яўляецца распрацоўка праграмнага модуля для вывучэння механізмаў шыфравання лічбавых носьбітаў інфармацыі ў аперацыйных сістэмах.

Для дасягнення мэты быў праведзены аналіз існуючых рашэнняў для паўнадыскавага шыфравання, апісаны ўразлівасці і метады абароны ад апісаных уразлівасцяў. Былі прапанаваны і апісаны практычныя метады ўзмацнення абароны паўнадыскавага шыфравання ў аперацыйных сістэмах Windows і Linux, выкарыстаючы групавыя палітыкі бяспекі і магчымасці модуля TPM для АС Windows, а таксама механізм бяспечнай загрузкі і іншыя ўтыліты для АС Linux. У працэсе падрыхтоўкі практычных заданняў былі даследаваны магчымасці асяроддзя віртуалізацыі і эмуляванага апаратнага комплексу.

Падрыхтаваныя заданні і асяроддзе для іх выканання будуць выкарыстаны ў лабараторных работах па курсе «Бяспечнасць інфармацыйных сістэм».

ABSTRACT

Thesis: 99 p., 141 fig., 22 sources

ENCRYPTION, FULL DISK ENCRYPTION, BITLOKER, LUKS, DIGITAL MEDIA, EFS, FSCRYPT, DM-CRYPT, SECURE BOOT, SHIM, GRUB, VOLUME MASTER KEY, FULL DISK ENCRYPTION, TPM, OPERATING SYSTEMS, WINDOWS, LINUX.

The purpose of the thesis is to develop a software module for studying the mechanisms of encryption of digital media in operating systems.

To achieve the goal, an analysis of existing solutions for full-disk encryption was carried out, vulnerabilities and methods of protection against the described vulnerabilities were described. Practical methods have been proposed and described for strengthening the protection of full-disk encryption in Windows and Linux operating systems, using group security policies and the capabilities of the TPM module for Windows OS, as well as the secure boot mechanism and third-party utilities for Linux OS. In the process of preparing practical tasks, the possibilities of the virtualization environment and the emulated hardware complex were explored.

Prepared tasks and the environment for their implementation will be used in laboratory work on the course «Information Systems Security».