



VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

FUNDAMENTINIŲ MOKSLŲ FAKULTETAS

INFORMACINIŲ SISTEMŲ KATEDRA

Dainius Čeponis

**WINDOWS API FUNKCIJŲ PANAUDOJIMAS REALIOJO LAIKO
NUSKAITYMO SISTEMOSE**

**WINDOWS API FUNCTIONS USAGE IN A REAL-TIME SCANNING
SYSTEMS**

Baigiamasis magistro darbas

Inžinerinės informatikos studijų programa, valstybinis kodas 62409P11

Informacinių sistemų specializacija

Informatikos mokslo kryptis

Vilnius, 2010

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
FUNDAMENTINIŲ MOKSLŲ FAKULTETAS
INFORMACINIŲ SISTEMŲ KATEDRA

TVIRTINU

Katedros vedėjas

(Parašas)

(Vardas, pavardė)

(Data)

Dainius Čeponis

**WINDOWS API FUNKCIJŲ PANAUDOJIMAS REALIOJO LAIKO
NUSKAITYMO SISTEMOSE**

**WINDOWS API FUNCTIONS USAGE IN A REAL-TIME SCANNING
SYSTEMS**

Baigiamasis magistro darbas

Inžinerinės informatikos studijų programa, valstybinis kodas 62409P11

Informacinių sistemų specializacija

Informatikos mokslo kryptis

Vadovas _____
(Moksl. laipsnis, vardas, pavardė) (Parašas) (Data)

Konsultantas doc. dr. Angelė Kaulakienė _____
(Moksl. laipsnis, vardas, pavardė) (Parašas) (Data)

Konsultantas _____
(Moksl. laipsnis, vardas, pavardė) (Parašas) (Data)

Vilnius, 2010

Vilniaus Gedimino technikos universitetas

Fundamentinių mokslų fakultetas

Informacinių sistemų katedra

ISBN

ISSN

Egz. sk.

Data-....-....

Inžinerinės informatikos studijų programos baigiamasis magistro darbas

Pavadinimas **Windows API funkcijų panaudojimas realiojo laiko nuskaitymo sistemose**

Autorius **Dainius Čėponis**

Vadovas doc. dr. **Antanas Čenys**

Kalba

☒ **X**

lietuvių

☐

užsienio

Anotacija

Darbe aptariamos virusų aptikimo metodikos, jų raida. Pristatomi nauji virusų aptikimo metodai ir genetinių algoritmų pritaikymas juose. Pirmoje praktinėje dalyje atliktas Windows API funkcijų perėmimo bibliotekų palyginimas.

Antroje praktinėje dalyje parašyta realiojo laiko nuskaitymo programa. Programa veikia naudodama nemokamas ClamAV virusų parašų duomenų bazes. Atliktas programos palyginimas su kitomis nemokamomis antivirusinėmis programomis.

Darbą sudaro 4 dalys: įvadas, teorinis pagrindimas, sistemos realizacija, išvados ir siūlymai, literatūros sąrašas.

Darbo apimtis – 47 p. teksto be priedų, 25 iliustr., 2 lent., 40 bibliografinių šaltinių.

Atskirai pridedami darbo priedai.

Prasminiai žodžiai: ClamAV, Detours, EasyHook, funkcijų perėmimas, programinis kenkimo kodas, realiojo laiko nuskaitymas, Windows API.

Vilnius Gediminas Technical University

Fundamental science faculty

Information systems department

ISBN

ISSN

Copies No.

Date-....-....

Engineering informatics study programme master thesis.

Title: **Windows API functions usage in real-time scanning systems**

Author **Dainius Čeponis**

Academic supervisor **Antanas Čenys**

Thesis language

☒ Lithuanian

☐ Foreign (English)

Annotation

There described virus scanning techniques in the work, they historical appearance. New scanning techniques presented, including genetic algorithms usage. In first practical part presented Windows API hooking libraries, they tests.

There created real-time system scanning program in second practical part. ClamAV free databases are used for files checking. Program tested with others free antivirus solutions.

Structure: introduction, analytical part, system implementation, conclusions and suggestions, references.

Thesis consist of: 47p. text without appendixes, 25 pictures, 2 tables, 40 bibliographical entries.

Appendixes included.

Keywords: ClamAV, Detours, EasyHook, hooking, real-time scanning, virus, Windows API.