UNIVERSITATEA TEHNICĂ A MOLDOVEI

Securitatea informației cu sisteme bazate pe blocuri

Information security systems based on blocks

Masterand:

Mindrigan Dumitru

Conducător:

Lect. sup Melnic Radu

Chişinău 2016

Ministerul Educa• iei al Republicii Moldova

Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică şi Microelectronică

Catedra Automatică și Tehnologii Informaționale

Admis la sus• inere

Şef de catedră: prof univ, dr. Victor Beșliu

_____

„_____” _____2016

SECURITATEA INFORMAȚIEI CU SISTEME BAZATE PE BLOCURI

Teză de master în Tehnologii Informaționale

Masterand:_____(D.Mindrigan)

Conducător:_____(R. Melnici)

Chişinău 2016

ADNOTARE

Asupra lucrării de master cu tema “Securitatea infoma iei cu sisteme bazate pe blocuri” elaborată de masterandul Mindrigan Dumitru. Securitatea informa iei este un concept mai larg care se referă la asigurarea integrită ii, confiden ialită ii şi disponibilită ii informa iei de aceea dezvoltarea tehnologică a fost acompaniată şi de solu ii de securitate cu sisteme bazate pe blocuri.

Structura logică a lucrării constă din 4 capitole de bază, surse bibliografice, concluzii şi anexe. În capitolul I, No iuni privind securitatea informa iilor se definesc no iuni de securitate a informa iilor. În capitolul II, se descrie politica de securitate informa ională. În capitolul III, sunt reprezentate metode de atac asupra algoritmilor Rivest-Code. În capitolul IV, sunt descrişi algoritmii Rivest-Code.

Argumentarea actualită ii temei constă în analiza şi caracterizarea situa iei curente în domeniul securită ii infoma iei, concret în compartimentul securită ii cu sisteme pe blocuri de tipul Rivest Code cît şi o analiză comparativă a tuturor versiunilor existente şi utilizate în securitate, reieşind din aplicarea rezultatelor preconizate. Rezultatele ob inute sunt în bună corela ie cu scopurile şi con inutul cercetării.

ADDNOTATION

Master's thesis on the topic "Information security systems based on blocks" developed by Master Mindrigan Dumitru. Information security is a broader concept that refers to ensuring the integrity, confidentiality and availability of information that technological development has been accompanied and security solutions based system blocks.

The logical structure of the paper consists of four main chapters, bibliographic sources, conclusions and annexes. In Chapter I, Getting define information security information security concepts. Chapter II describes the Information Security Policy. In Chapter III, are the methods of attack on the algorithms Rivest-Code. In Chapter IV, the algorithms described Rivest-Code. Timeliness argument is to analyze and characterize the theme of the current situation in the field of information security, systems security compartment concrete blocks Rivest Code such as a comparative analysis of all existing versions used in security resulting from the application of the expected results. The results are in good correlation with the aims and content of the research.

Cuprins :