

CONTENT

1 Legal information security.

Development problems of regulatory and imethodological bases of information security system.

METHOD FOR TIME DETERMINATION AT CREATION OF INNOVATIVE ENTERPRISES AS A FACTOR OF INFORMATION SECURITY

Liliya Nikiforova, Iurii Iaremchuk, Anatoliy Shiyan..... 11

DEVELOPMENT OF MATHEMATICAL MODEL OF DETECTION TONE UNDER DOMINANT INTERFERENCE

Mikhail Diviziniuk, Yuriy Stolyarchuk, Oleksandr Farrakhov..... 14

THE OPTIMAL TOPOLOGY DATA NETWORK

Vladimir Khoroshko, Julia Hohlachova, Elena Skorobohatko, Nikolai Timchenko..... 20

THE TUPEL MODEL OF BASIC COMPONENTS' SET FORMATION FOR CYBER ATTACKS

Anna Korchenko 29

EVALUATION OF EFFECTIVENESS NOISY SPEECH SIGNAL

Alexander Arkhipov, Katerina Bezymyannaya 37

2 Providing computer security in information systems

ALGORITHM OF ASYMMETRIC ENCRYPTION BASED ON ELLIPTIC CURVES

Anatoly Kochubinsky, Vladimir Sinyavskiy , Alexander Shatalov..... 42

THE UPPER BOUNDS OF THE INTEGER DIFFERENTIALS AVERAGE PROBABILITIES FOR COMPOSITION OF THE MODULAR KEY ADDER, SUBSTITUTION BLOCKS AND THE BLOCK-STRUCTURED LINEAR OPERATOR Lyudmila Kovalchuk, Nataliia Kuchynska, Viktor Bezditnyi	47
RESEARCH OF CUBE ATTACKS WITH LOW DEGREE MAXTERMS Lyudmyla Zavadska, Vitaliy Sergienko	53
ALGORITHM OF ESTABLISHMENT OF GENERAL SECRET VALUE, BASED ON ELLIPTIC CURVES Anatoly Kochubinsky, Vladimir Sinyavskiy , Alexander Shatalov.....	59
THE COMPARISON OF THE COMPONENT-WISE AND MODULAR ADDITION (SUBTRACTION) OF N-DIMENSIONAL VECTOR SPACE OVER A PRIME FINITE FIELD Kovalchuk Ludmila, Lysenko Natalija*, Krasnikov Sergej	65
3 Technical means for protecting information system. Standardization and metrological provision of technical information security. Identification of consistency technical information security means	
DEVELOPMENT OF A SINGLE ELEMENT (STATION) FOR MEASUREMENT OF ATMOSPHERIC AIR PARAMETERS Mikhail Diviziniuk, Valeriia Kovach	72
STABILITY OF INFORMATION PROTECTION RADIO EQUIPMENT AGAINST DESTABILIZING MECHANICAL EFFECTS Juriy Zinkovsky, Boris. Uvarov	76
THE APPLICATION OF METHODS OF FORCED TESTING TO OBTAIN THE DEPENDENCE OF DIAGNOSTIC PARAMETER OF RUN TIMES OF DIGITAL REC Vasil Kuzctvkov, Evgen Redzuk.....	84

THE METHOD OF INCREASING A SPEED OF A CONTROL SYSTEM
OF ACCESS BY IRIS

Yevgeny Podgorny, Lyubov Ryabova, Volodymyr Temnikov..... 88

4 Abstracts..... 93

5 Alphabetic index..... 121