НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ "ВАСИЛ ЛЕВСКИ"

ФАКУЛТЕТ „АРТИЛЕРИЯ, ПВО И КИС"

9713 гр. Шумен, ул. „Карел Шкорпил" №1

телефон: (054)801 040; тел.факс:(054)877 463; e-mail:www.aadcf.nvu.bg

С Т А Н О В И Щ Е

от

доцент д-р инж. Дилян Иванов Димитров,

доцент в катедра ПВО на факултет „А, ПВО и КИС" на НВУ „В. Левски",

гр. Шумен, ул."К. Шкорпил" 1

на дисертационен труд на капитан инженер Станимир Христов Първанов на тема: **„Изследване на възможностите за съвместно приложение на шумоустойчивото кодиране и шифриране в комуникационните системи"** представен за придобиване на образователната и научна степен „доктор" по докторска програма „**Комуникационни мрежи и системи"** в област на висшето образование 5. Технически науки, професионално направление 5.3. Комуникационна и компютърна техника

1. АКТУАЛНОСТ НА РАЗРАБОТВАНИЯ В ДИСЕРТАЦИОННИЯ ТРУД ПРОБЛЕМ

Кодирането и шифриране на информацията са важни елементи от процеса на създаването и функционирането на комуникационните мрежи. Кодирането е процес на преобразуване на данни в нов формат, като се използва публично достъпна и стандартна схема, като минимизира грешките при предаване на

цифрови данни. Това осигурява ниво на достоверност на приетите битове информация чрез добавяне на контролни битове за проверка.

От друга страна, шифрирането е процес на преобразуване на данни в нечетим вид (скрит текст), като се използва сложен математически алгоритъм и секретен ключ. Това осигурява най-ефективната защита срещу кибератаки и компрометирането на личните данни. Прилагането както на кодиране така и на шифриране усложнява процеса на предаване и обработка на информация и намалява скоростта на нейното предаване.

Актуалността на представения дисертационният труд с автор инж. Станимир Първанов произлиза от предложените нови подходи за съвместно използване на шумоустойчиво кодиране и шифриране. Това предлага едновременно висока криптографска устойчивост, шумозащитеност и необходимата скорост на предаване на информацията чрез оптимално използване на възможностите на хардуерните и софтуерните компоненти на комуникационните системи.

2. КРАТКА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Дисертационният труд е структуриран както следва: увод, четири глави и заключение, библиография, декларация за оригиналност на резултатите и приложения. Списъкът на авторските публикации са показани в дисертационния труд. Всяка глава представлява обособен етап от решавания проблем, съответства на дадена задача (задачи) и завършва с изводи, които акцентират върху получените приноси. Логическата свързаност между отделните глави е осигурена и позволява да се добие цялостна представа за научното изследване.

В уводната част е обоснована актуалността на разглеждания проблем и са дефинирани целта и задачите на дисертационния труд. Поставените задачи са решени в отделните глави на дисертационния труд.

В първа глава е направен анализ на принципите на построение на комуникационните системи. Показана е значимостта на тяхната

шумоустойчивост. Анализирани са също и известните технологии за съвместно използване на шумоустойчиво кодиране и шифриране.

Глава втора систематизирано описва основните етапи на обработка на данните при шумоустойчиво кодиране. Направен е анализ на симетричните и асиметрични алгоритми за шифриране на съобщенията, предавани по незащитен канал. Направена е обща характеристика на конволюционните и турбо кодове, както и на алгоритмите за шифриране.

В трета глава е синтезиран модел за обработка на информацията в комуникационна система, осигуряващ съвместно шумоустойчиво кодиране и шифриране на информацията. Разработен е симулационен модел на канала с добавяне на разбъркващи устройства преди кодиращото устройство и подреждащи устройства след декодиращото устройство. Подробно е описан всеки един от елементите на комуникационния канал.

В четвърта глава е обоснована практическата приложимост на синтезирания модел като са приведени получените резултати от изследванията на предложения комуникационен канал.

Обобщени са постигнатите резултати и са представени приносите на дисертацията.

3. ОЦЕНКА НА НАУЧНИТЕ РЕЗУЛТАТИ И ПРИНОСИТЕ НА ДИСЕРТАЦИОННИЯ ТРУД

Дисертационният труд е написан в научно-издържан стил без излишна информация. Научната терминология е използвана правилно. Използваният математически апарат е правилен и разбираем. Предложените реални архитектури на елементите от синтезирания комуникационен канал са правилни и точни. Най-добри резултати са постигнати с две успоредно свързани разбъркващи устройства към комуникационния модел.

Научно приложните приноси са формулирани коректно, точно и ясно и съответстват на показаното в дисертационния труд.

Представени са и чисто приложни приноса, което показва че представените модели са реализирани и са безспорен труд на докторанта.

Показаният подход на комбинирано изпилване на RSA и AES алгоритми за шифриране е използван подход и този принос го определям като научно-приложен, защото комбинираното шифриране се използва в много сфери, като Военна и правителствена сателитна комуникация (MILCOM), Комуникация в дълбокия космос на NASA, Банкови трансакции през сателитни терминали (VSAT) и други. Използването му за конкретния синтез на комуникационния канал го прави научно-приложен.

Цитираните информационни източници са представителни, основната част са от чужди автори и са от последните години. Почти всички имат отношение към темата на дисертационния труд.

От показаните 3 публикации на докторанта две са в съавторство и една самостоятелна. Едната е индексирана в SCOPUS. Всичките са свързани с темата на дисертацията.

4. КРИТИЧНИ БЕЛЕЖКИ И ПРЕПОРЪКИ

Към дисертационния труд могат да се направят следните по-съществени забележки и препоръки:

- на места липсва цитиране на литературните източници, които са използвани, най-вече в първа и втора глава;

- не е показано конкретно предложение за приложение на синтезирания комуникационен канал в сферата на сигурността и отбраната. Тази забележка следва да се отчита като препоръка за бъдеща работа.

5. ЗАКЛЮЧЕНИЕ

Посочените слабости в дисертационния труд не намаляват цялостното положително впечатление за предложения дисертационен труд.

Предложените анализи, изчислителни алгоритми и архитектури на синтезирани модели са обосновани, полезни и допълват научните постижения в дадената област.

В заключение цялостната ми оценка е, че дисертационния труд се характеризира със задълбочени научно-приложни и приложни резултати.

Предвид на изложеното имам основанието да предложа на уважаемото жури да присъди на докторанта капитан инженер Станимир Христов Първанов образователната и научна степен "Доктор" в област на висшето образование 5. Технически науки, професионално направление 5.3 „Комуникационна и компютърна техника", докторска програма по докторска програма „Комуникационни мрежи и системи".

24.08.2026 г.

Гр. Шумен

Член на научното жури:

доц. д-р инж. Диляна Димитров

"VASIL LEVSKI" NATIONAL MILITARY UNIVERSITY

ARTILLERY, AIR DEFENSE AND CIS FACULTY

9713 Shumen, 1 Karel Shkorpil Street

phone: (054)801 040; tel. fax: (054) 877 463; e-mail: www.aadcf.nvu.bg

OPINION

by Associate Professor Eng. Dilyan Ivanov Dimitrov PhD,

Air Defense Department, Air Defense and CIS Faculty,

Vasil Levski National Military University,

Shumen

of the dissertation work of Captain Engineer Stanimir Hristov Parvanov on the topic: **"Investigation of the possibilities for joint application of noise-resistant coding and encryption in communication systems"** presented for acquisition on educational and scientific degree "Philosophy Doctor" in doctoral program **"Communication Networks and Systems"** in the field of higher education 5. Technical Sciences, professional field 5.3. Communication and Computer Engineering

1. RELEVANCE AND SIGNIFICANCE OF THE SCIENTIFIC PROBLEM

Information encoding and encryption are important elements of the process of creating and operating communication networks. Encoding is the process of converting data into a new format using a publicly available and standard scheme, minimizing errors in the transmission of digital data. This provides a level on credibility on accepted bits of information by adding check bits for verification.

On the other hand, encryption is the process of converting data into an unreadable form (hidden text) using a complex mathematical algorithm and a secret key. This

provides the most effective protection against cyberattacks and the compromise of personal data. The application of both encoding and encryption complicates the process of transmitting and processing information and reduces the speed of its transmission.

The relevance of the presented dissertation stems from the proposed new approaches for the joint use of noise-resistant coding and encryption. This offers simultaneously high cryptographic stability and noise protection of information transmission through optimal use of the capabilities of the hardware and software components of communication systems.

2. GENERAL CHARACTERISTICS AND STRUCTURE OF THE DISSERTATION

The dissertation is structured as follows: introduction, four chapters, heads and conclusion, bibliography, declaration of originality of the results and applications. The list of the author 's publications is shown in the dissertation. Each chapter represents a separate stage of the problem being solved, corresponds to a given tasks and ends with conclusions that emphasize the contributions received. The logical connection between the individual chapters is ensured and allows one to obtain a comprehensive picture of the scientific research.

The introductory part justifies the relevance of the problem under consideration and defines the goal and objectives of the dissertation. The tasks set are solved in the individual chapters of the dissertation.

In first chapter is made analysis of the principles of construction of communication systems. The importance of their noise immunity is shown. The known technologies for the joint use of noise-resistant coding and encryption are also analyzed.

Chapter The second systematically describes the main stages of data processing in noise - resistant coding. An analysis of the symmetric and asymmetric algorithms for encrypting messages transmitted over an unprotected channel is made. A general characteristic on convolutional and turbo codes, as well as the algorithms for encryption.

In the third chapter, a model for information processing in a communication system is synthesized, providing joint noise-resistant encoding and encryption of information. A simulation model of the channel is developed with the addition of scramblers before the encoding device and arrangers after the decoding device. Each of the elements of the communication channel is described in detail.

In The fourth chapter justifies the practical applicability of the synthesized model by presenting the results obtained from the research of the proposed communication channel.

The results and the contributions of the dissertation are presented.

3. CHARACTERISTICS OF THE SCIENTIFIC RESULTS

The dissertation is written in a scientifically style without unnecessary information. The scientific terminology is used correctly. The mathematical apparatus used is correct and understandable. The proposed real architectures of the elements of the synthesized communication channel are correct and accurate. The best results are achieved with two parallel-connected mixing devices to the communication model.

The scientific and applied contributions are formulated correctly, accurately and clearly and correspond to what is shown in the dissertation.

Purely applied contributions are also presented, which shows that the presented models have been implemented and are the undisputed work of the doctoral student.

The presented approach of combined use of RSA and AES encryption algorithms is a used approach and I define this contribution as scientifically applied because combined encryption is used in many areas, such as Military and Government Satellite Communication (MILCOM), NASA Deep Space Communication, Banking transactions via satellite terminals (VSAT) etc. Its use for the specific synthesis of the communication channel makes it scientifically applied.

The cited information sources are representative, the majority are from foreign authors and are from recent years. Almost all of them are relevant to the topic of the dissertation.

Of the 3 publications shown by the doctoral student, two are co-authored and one is independent. One is indexed in SCOPUS. All are related to the topic of the dissertation.

4. CRITICAL NOTES AND RECOMMENDATIONS

The following more significant remarks and recommendations can be made regarding the dissertation:

- in places there is a lack of citation of the literary sources that were used, especially in the first and second chapters;

- no specific proposal for the application of the synthesized communication channel in the field of security and defense is shown. This remark should be considered as a recommendation for future work.

5. CONCLUSION

The indicated weaknesses in the dissertation do not diminish the overall positive impression of the proposed dissertation.

The proposed analyses, computational algorithms, and architectures of synthesized models are justified, useful, and complement scientific achievements in the given field.

In conclusion, my overall assessment is that the dissertation work is characterized by in-depth scientific and applied results.

In view of the above, I have reason to propose to the esteemed jury to award Captain Engineer Stanimir Hristov Parvanov the educational and scientific degree "PhD" in the field of higher education 5. Technical Sciences, the doctoral program "Communication Networks and Systems".

24/08/2026

Shumen

Member of the scientific jury:

Assoc. Prof. Dilyan Dimitrov PhD