НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ „ВАСИЛ ЛЕВСКИ”
ФАКУЛТЕТ „АРТИЛЕРИЯ, ПВО И КИС”
9700 гр. Шумен, ул. „Карел Шкорпил” №1
телефон: (054)801 040; тел.факс:(054)877 463; email: decanat@aadcf.nvu.bg

С Т А Н О В И Щ Е

от доц. д-р инж. Росен Атанасов Богданов
доцент в Национален Военен Университет „Васил Левски“
на дисертационния труд на Радостин Стефанов Димов
на тема „Изследване на сигурността на когнитивни комуникационни системи”,
представен за придобиване на образователната и научна степен „доктор” в област
на висшето образование 5. „Технически науки“, професионално направление 5.3.
„Комуникационна и компютърна техника“, по докторска програма
„Киберсигурност”.

1. Актуалност и значимост на разработвания научен проблем

Динамичното развитие на съвременните когнитивни комуникационни системи неминуемо е свързано с необходимостта от извършване на изследвания относно условията и средствата за осигуряване на надеждното им функциониране. Успоредно с подобряване на функционалните способности и техническите параметри на когнитивните мрежи се увеличават и заплахите от страна на хора и организации. Това налага разработването на специализирани инструменти за откриване на заплахите, идентификация на уязвимостите, изграждане на процедури за реакция при инциденти и натрениране на потребителите. Посредством симулиране на различни сценарии и заплахи се разработват и внедряват нови технологии за киберсигурност. Подготовката на специалисти в областта на киберсигурността, способни да подържат оборудването и да реагират своевременно на възникналите заплахи, е задължително изискване за всяка комуникационна мрежа.

Основна характеристика на комуникационните когнитивни системи е повишаването на ефективността на използване на честотните ресурси. В този аспект, с цел осигуряване на надеждното им функциониране, е необходим анализ и синтез на нови модели за сигурност на тези системи. Този анализ изисква изграждане на специфична симулационна среда, в която да бъдат проверени различни хипотези, да се формулират процедури за добра координация на участващите екипи, провеждане на стрес тестове и оценка на реакцията при инцидентите.

Считам, че разглежданата тематика е навременна, актуална и напълно отговаря на техническото равнище и предизвикателствата пред комуникационните системи.

Съдържанието на представения дисертационен труд напълно съответства на поставения в заглавието проблем.

2. Оценка на научните резултати и приносите на дисертационния труд

В резултат от работата по дисертационния труд са изведени следните научно-приложни приноси:

Предложени са нови математико-приложни модели:

- модел на когнитивна комуникационна мрежа;
- модел на разузнаване за киберзаплахи в публични бази данни;
- модел на противник.

Предложените модели са полезни за научни и технически екипи, които се занимават с анализ на атаки, разработване и внедряване на защитни процедури и архитектури за сигурност.

Изграден е специализиран киберполигон, реализиран е симулационен сценарий на експериментална среда, с цел изследване на сигурността на когнитивна мрежа.

Изградената виртуална среда успешно емулира работата на когнитивна мрежа за радиодостъп и потребителското оборудване.

Киберполигонът дава възможност за идентифициране на уязвимости в когнитивната мрежа и трениране на екипите при реакция на кибератаки.

Разработеният модел дава възможност за формулиране на разнообразни сценарии и дефиниране на задачите за изпълнение.

Предложена е и е изследвана система за киберсигурност на когнитивни мрежи, която осигурява значително повишаване на агрегираната ефективност на системата.

Разработеният модел и направените изследвания имат значителна практическата приложимост за автоматизирано изграждане на симулационни среди в специализиран киберполигон.

Получените по време на работата резултати са апробирани в специализираната научна литературa и са представени на научната общност в три публикации, като една от тях е индексирана в SCOPUS.

Представеният автореферат към дисертацията отразява в пълен обем всички получени резултати.

Приемам без забележки авторовите формулировки и претенции за приноси в областта на сигурността на когнитивните комуникационни системи.

3. Критични бележки

При разработването на дисертацията е акцентирано върху принципите на работа, заплахите и уязвимостите на гражданска клетъчна комуникационна система от пето поколения, която е типична когнитивна мрежа. Не са изследвани когнитивните мрежи, които са проектирани и намират приложение в системата на сигурността и отбраната. Считам, че разработеният модел и полигон за киберсигурност може да бъде разширен и адаптиран към специфичните изисквания на мрежите от системата на сигурността и отбраната. Подобно развитие на модела ще доведе до идентификация на заплахите и уязвимостите, а също така ще бъде полезно за подобряване на натренираността на екипите за киберсигурност.

4. Заключение

Представеният дисертационен труд е на актуална тема от областта на комуникациите и киберсигурността. Авторът, инж. Радостин Димов, е представил оригинална разработка и е получил резултати, които ще позволят да се поддържа и подобрява нивото на сигурността на когнитивните комуникационни системи. Дисертацията и представените заедно с нея автореферат и публикации по темата отговарят на изискванията на Закона за развитие на академичния състав в Република България, Правилника за неговото прилагане и на Правилника за

обучение и придобиване на научни степени в Националия военен университет „Васил Левски“.

5. Оценка на дисертационния труд

Давам положителна оценка на дисертационния труд и предлагам на капитан инж. Радостин Стефанов Димов да бъде присъдена образователната и научна степен „Доктор“ по докторска програма „Киберсигурност“, област на висшето образование 5 „Технически науки“, професионално направление 5.3 „Комуникационна и компютърна техника“.

07.01.2026 г. Член на журито:

гр. Шумен /доц. д-р Росен Богданов/

OPINION

by Assoc. Prof. Eng. Rosen Atanasov Bogdanov, PhD
Associate Professor at the National Military University "Vasil Levski"
on the PhD thesis of thesis of master engineer Radoslav Stefanov Dimov
on the topic "Investigation on the Security of Cognitive Communication Systems,"
submitted for the educational and scientific degree of "Doctor" in the field of higher education 5. "Technical Sciences," professional direction 5.3. "Communication and Computer Engineering," in the doctoral program "Cybersecurity."

1. Relevance and significance of the scientific problem

The dynamic development of modern cognitive communication systems is inevitably linked to the need for research into the conditions and means of ensuring their reliable functioning. Along with the improvement of the functional capabilities and technical parameters of cognitive networks, threats from individuals and organizations are also increasing. This necessitates the development of specialized tools for detecting threats, identifying vulnerabilities, establishing incident response procedures, and training users. New cybersecurity technologies are developed and implemented by simulating various scenarios and threats. The training of cybersecurity specialists capable of maintaining equipment and responding promptly to emerging threats is a mandatory requirement for any communication network.

A key feature of communication cognitive systems is the increased efficiency of frequency resource utilization. In this regard, in order to ensure their reliable operation, it is necessary to analyze and synthesize new security models for these systems. This analysis requires the creation of a specific simulation environment in which various hypotheses can be tested, procedures for good coordination of the participating teams can be formulated, stress tests can be conducted, and incident response can be evaluated.

I believe that the topic under consideration is timely, relevant, and fully corresponds to the technical level and challenges facing communication systems.

The content of the presented dissertation fully corresponds to the problem stated in the title.

2. Evaluation of the scientific results and contributions of the dissertation work.

The following scientific and applied contributions have been identified as a result of the work on the dissertation:

New mathematical and applied models have been proposed:

- a cognitive communication network model,
- a model for cyber threat intelligence in public databases,
- an adversary model.

The proposed models are useful for scientific and technical teams involved in attack analysis, development, and implementation of defensive procedures and security architectures.

A specialized cyber range has been built and a simulation scenario of an experimental environment has been implemented to study the security of a cognitive network.

The virtual environment successfully emulates the operation of a cognitive radio access network and user equipment.

The cyber range enables the identification of vulnerabilities in the cognitive network and the training of teams in responding to cyber attacks.

The developed model allows for the formulation of various scenarios and the definition of tasks to be performed.

A cybersecurity system for cognitive networks has been proposed and studied, which provides a significant increase in the aggregate efficiency of the system.

The developed model and the research conducted have significant practical applicability for the automated construction of simulation environments in a specialized cyber range.

The results obtained during the work have been verified in specialized scientific literature and presented to the scientific community in three publications.

The abstract of the dissertation reflects all the results obtained in full.

I accept completely the author's formulations and claims for contributions in the field of cognitive communication system security.

3. Critical notes

The dissertation focuses on the operating principles, threats, and vulnerabilities of a fifth-generation civilian cellular communication system, which is a typical cognitive network. Cognitive networks that are designed and used in security and defense systems have not been studied. I believe that the developed model and cybersecurity testing ground can be expanded and adapted to the specific requirements of security and defense system networks. Such a development of the model will lead to the identification of

threats and vulnerabilities and will also be useful for improving the training of cybersecurity teams.

4. Conclusion

The presented dissertation deals with a topical issue in the field of communications and cybersecurity. The author, Radoslav Dimov, has presented an original study and obtained results that will enable the security level of cognitive communication systems to be maintained and improved. The dissertation and the accompanying abstract and publications on the topic meet the requirements of the Law on the Development of Academic Staff in the Republic of Bulgaria, the Regulations for its implementation, and the Regulations for Training and Acquiring Academic Degrees at the Vasil Levski National Military University.

5. Evaluation of the dissertation work

I give a positive assessment of the dissertation and propose that Captain Eng. Radoslav Stefanov Dimov be awarded the educational and scientific degree of "Doctor" in the scientific specialty "Cybersecurity," field of higher education 5 "Technical Sciences," professional direction 5.3. "Communication and Computer Engineering."

07.01.2026 Member of the jury:
Shumen /Assoc. Prof. Rosen Bogdanov, PhD/