

**НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ  
„ВАСИЛ ЛЕВСКИ“**

---

Подделение 52520-Шумер

№ x 026-28-2862/26.11.2016

от 6 листа 0 Не

**РЕЦЕНЗИЯ**

от професор д.т.н. Атанас Иванов Начев,

**ОТНОСНО:** Научните и приложни трудове на доцент д.н. Жанета Николова Савова-Ташева, представени за участие в обявения в ДВ, бр. 59/29.07.2016 г. конкурс за заемане на академична длъжност „професор“ в Националния военен университет „Васил Левски“

**Шумен  
2016**

## ОБЩИ СВЕДЕНИЯ ПО КОНКУРСА

Конкурсът е за заемане на академична длъжност „професор“, обявен е със обявени със заповед на началника на НВУ „Васил Левски“ № РД-02-732/06.07.2016 г. и в Държавен вестник, бр. 59 от 29.07.2016 г. и е за нуждите на факултет „Артилерия, ПВО и КИС“ на Националния военен университет „Васил Левски“. От областта е на висшето образование 5. Технически науки, професионално направление 5.3. Комуникационна и компютърна техника, научна специалност „Автоматизирани системи за обработка на информация и управление“.

По темата на конкурса е подала документи доцент д.н. Жанета Николова Савова-Ташева.

### КРАТКИ БИОГРАФИЧНИ ДАННИ ЗА КАНДИДАТА

Доцент д.н. Жанета Николова Савова-Ташева е завършила през 1989 г. Техническият университет в гр. Варна, специалност „Изчислителна техника“.

През 2002 г. защитава дисертационен труд и въз основа на решение на Висшата атестационна комисия и е присъдена образователната и научна степен „Доктор“ по научната специалност 02.07.20 „Комуникационни мрежи и системи“.

През 2015 г. защитава дисертационен труд и е присъдена научната степен „доктор на науките“ по научната специалност „Комуникационни мрежи и системи“, област на висшето образование 5. Технически науки, професионално направление 5.3. Комуникационна и компютърна техника.

От 2006 г., с решение на Висшата атестационна комисия, притежава научното звание „Доцент“. Длъжност „Доцент“ заема в Националния военен университет „Васил Левски“, факултет „Артилерия, ПВО и КИС“ - гр. Шумен и в Шуменския университет „Епископ Константин Преславски“.

Доцент д.н. Жанета Николова Савова-Ташева има богат опит като научен работник и преподавател във ВУЗ.

### ОБЩО ОПИСАНИЕ НА ПРЕДСТАВЕНИТЕ МАТЕРИАЛИ

Като член на научното жури са ми предоставени следните материали:

1. Заявление за допускане до участие в конкурс.
2. Автобиография.
3. Творческа автобиография.
4. Диплома за научна и образователна степен „Доктор“ (ксерокопие).
5. Диплома за научно звание „Доцент“ (ксерокопие).
6. Списък с научните трудове и публикации.

7. Списък на разработки на изделия и рационализации, внедрени в производството.

8. Справка с основните резултати и приноси в трудовете.

9. Наукометрични данни за научната продукция.

10. Списък на международни редкологии и публикувани рецензии в международни научни издания.

11. Списък на успешно защитилите докторанти.

12. Справка за цитирания.

Представените ми материали, по обем и съдържание, са достатъчни, за да се оцени научния облик на доцент д.н. Жанета Николова Савова-Ташева.

За нуждите на конкурса доцент д.н. Жанета Николова Савова-Ташева е представила 47 заглавия, не рецензирани при получаване на научното звание „Доцент“. Те са разпределени както следва:

- Монографии – 1 бр. - 205 стр.;
- Учебно методични трудове – 5 бр. - общо 515 стр.;
- Статии в научни списания и публикации в годишници – 20 бр. – общо 138 стр.;
- Научни статии и доклади в сборници на международни симпозиуми и конференции – 6 бр - общо 34 стр.;
- Научни доклади в сборници от научни конференции – 15 бр., общо 1020 стр.

Монографията е в съавторство.

Не рецензирам програмните продукти, внедрени в производството, поради техния чисто приложен характер.

При формиране на общата оценка по конкурса за „професор“ за научната дейност на доцент д.н. Жанета Николова Савова-Ташева вземам под внимание цялата и научна и педагогическа дейност.

### **ОПРЕДЕЛЯНЕ И АНАЛИЗ НА ПРИНОСИТЕ В РЕЦЕНЗИРАНИТЕ НАУЧНИ ТРУДОВЕ**

Научните трудовете на доцент д.н. Жанета Николова Савова-Ташева са от областта на конкурса за заемане на академична длъжност „професор“ и касаят проблемите, свързани с автоматизирана обработка на информацията в компютърни системи, управление на комуникационни и информационни системи, кодиране и защита на информацията в компютърни и комуникационни системи.

Приносните моменти в тези трудове могат да се групират по следния направления:

- Систематизиране и обобщаване на знанията в проблемната област;

- Развитие на криптографски методи и средства;
- Развитие на стеганографски методи и средства;
- Методи за обработка на информация в среда на компютърни системи и мрежи;

Научните и научноприложните приноси в обхвата на тези направления могат да се дефинират като:

1. Обогаляване на теорията на поточните шифри с предлагането на нови методи за генериране на  $p$ -чен ключов поток, където  $p$  е просто число (IV.1.1, IV.3.7, IV.3.14, IV.5.1).
2. Развитие на теорията на поточните шифри чрез предлагането на нови методи за синтез на генератори на двоичен ключов поток, подходящи за хардуерна и софтуерна реализация на поточни шифри. (IV.1.1, IV.3.7, IV.3.14, 5.14).
3. Разработени са математически модели, описващи основните характеристики на нелинейния ключов поток, произведен от предложените генератори (IV.1.1, IV.3.4, IV.4.3, IV.5.15).
4. Извършено е систематизиране в обхвата на теорията на поточните шифри (IV.1.1) чрез:
  - анализ на перфектната сигурност на еднократния шифър на Вернам и сигурността на поточните шифри;
  - развитие на подходите за проектиране на поточни шифри;
  - дефиниране на основните характеристики на синхронните и асинхронни поточни шифри и формулиране на изискванията към генераторите на ключов поток;
  - анализ на архитектурите на основните градивни елементи на поточните шифри и характеристиките на техните изходни последователности;
  - систематизиране на основните свойства на поточните шифри и формулиране на основните критерии за анализ, които предоставят оценка по отношение на трудността на разбиване на даден поточен шифър.
5. Систематизиране на основните принципи и алгоритми за обработка на информацията в системите за информационна сигурност (трилогия IV.2.4, IV.2.1, IV.2.2).
6. Предложена е методика за тестване на основните характеристики на нелинейния ключов поток, произведен от предложените генератори, и

потвърждаване на верността на доказаните математически изрази в 1.3 (IV.1.1, IV.3.6, IV.3.6).

7. Разработени са ускорени алгоритми и програмни средства за генериране изчисления в разширено поле на Галоа (IV.3.3, IV.4.1).

8. Предложен е метод за оценка на изчислителната сложност на алгоритмите за генериране на големи прости числа (IV.5.10).

9. Дефинирани са и са оценени проблемите, отнасящи се за сигурността и предизвикателства към нейното усъвършенстване в системите за обработка на информация (IV.1.1, IV.3.1, IV.3.2, IV.3.8, IV.3.10, IV.3.15, IV.3.19, IV.3.20, IV.5.3, IV.5.7, IV.5.13).

10. Разработени са методи за синтез на средства за тестване и анализ на уязвимостите в сигурността на системите за обработка на информация (IV.4.4, IV.5.4).

11. Предложен е метод за синтез на софтуерна система за скриване на конфиденциална информация чрез комбинирано използване на криптографски и стеганографски методи. (IV.3.9, IV.5.6).

12. Предложена е софтуерна система за скриване на конфиденциална информация чрез LSB стеганографски метод. Изследвано е влиянието на скриване на информация в различни цветови канали или в тяхна комбинация, както и скриване на информация в различен брой най-младши битове. (IV.4.2).

13. Разработен е метод за синтез на свършени двумерни масиви на основата на два свършени едномерни масива. (IV.3.17, IV.3.18).

14. Предложен е метод за синтез на семейство взаимно ортогонални комплементарни кодове и алгоритъм за синтез на двойка взаимно ортогонални комплементарни кодове (IV.4.5, IV.4.6).

15. Разработен е метод за синтез на фазово-манипулирани комплементарни сигнали, приложими в космически-базирани радари (IV.3.16).

16. Предложена е методика за анализ на сигурността в комуникационни мрежи и системи (IV.1.1, IV.3.11, IV.5.5).

17. Предложени са методи за разработване на алгоритми и програмни средства за генериране на  $p$ -ични кодове на Рийд-Соломон, където  $p$  е произволно просто число (IV.5.2).

18. Разработени са методи за анализ и оценка на комуникационни мрежи и системи (IV.3.12, IV.3.13, IV.5.6, IV.5.9, IV.5.11, IV.5.12).

### **КРИТИЧНИ БЕЛЕЖКИ**

Определена слабост е наличието на известна разпиляност в насоките на изследователската дейност на автора. Това на моменти създава впечатление за незавършеност на научното търсене и непълнота на изложението.

Казаното по никакъв начин не поставя под съмнение верността на получените резултати, тяхната интерпретация и значение.

### **ЛИЧНИ ВПЕЧАТЛЕНИЯ**

Познавам кандидата. Прави впечатление неговата задълбоченост при дефиниране на научните проблеми и търсенето на решения за тях. Добре съчетава научноизследователската с преподавателската си дейност. Творчески прилага в педагогическата си практика резултати от научното си творчество.

### **ЗАКЛЮЧЕНИЕ**

Като вземам предвид казаното в пълния обем на настоящата рецензия и това, че приносните моменти в трудовете на кандидата са в съответствие с изискванията на Закона за развитие на академичния състав в Република България и на Правилника за неговото прилагане, ще гласувам положително за избирането на доцент д.н. Жанета Николова Савова-Ташева за заемане на академична длъжност „Професор” във факултета по Артилерия, ПВО и КИС на Националния военен университет „Васил Левски“.

  
ПРОФЕСОР, АТАНАС НАЧЕВ,

ДОКТОР НА ТЕХНИЧЕСКИТЕ НАУКИ