Списък
на научните трудове и техните резюмета

на доц. д.н. инж. Жанета Николова Савова-Ташева
за придобиване на академична длъжност „професор“

№	Наименование на трудовете	Харак-тер	Обем (стр.)	Съавто-ри	Резюмета
1	**2**	**3**	**4**	**5**	**6**
IV. Научни трудове и публикации за академична длъжност „професор“					
1. Монография (1 бр., 205 стр.)					
1.	Поточни шифри. Технически Университет – София, 2016, ISBN: 978-619-167-240-0, с 205.	Моногра-фия	205	А. Т. Ташева	Целта на това научно издание е да представи в систематизиран вид теоретичните и практически въпроси, свързани с избора на подходящи поточни шифри за криптиране на информация. Обект на настоящото научно изследване са поточните шифри, и по-специално методите за конструиране на генератори на ключов поток, осигуряващи нелинейност в тяхната изходна последователност. Монографията е предназначена за широк кръг читатели, специалисти по информационна сигурност в комуникационните и компютърни мрежи и системи. Тя е полезна и за студенти, докторанти, инженери и потребители, които се стремят към по-добро разбиране на информационните технологии за поточно шифриране, инженери и архитекти, работещи по проектиране и изграждане на техническите възможности за сигурност на информацията, както и за специалисти, разработващи ръководства за използване на технологиите за информационна сигурност.
2. Учебно-методически трудове (5 бр., 515 стр.)					
1.	Информационни технологии за сигурност. Издателски комплекс	Електронен учебник	174	-	Целта на този учебник е да се даде описание на математическите основи на информационните технологии за сигурност и

1	2	3	4	5	6
	на Национален военен университет „Васил Левски“, 2014, ISBN 978-954-753-190-1. с 174.				криптографските алгоритми, които са в основата на предоставяните услуги за информационна сигурност. Учебникът е предназначен основно за студенти магистри в дистанционна форма на обучение по специалността „Информационна сигурност“.
2.	Хардуерни и софтуерни средства за информационна сигурност. Издателски комплекс на Национален военен университет „Васил Левски“, 2014, ISBN 978-954-753-187-1. с 136.	Електронен учебник	136	-	Целта на този учебник е да се даде описание на техническите модели и средства, които са в основата на сигурността на информационните технологии. В сбита форма са представени моделите, които трябва да бъдат взети предвид при проектирането и разработването на техническите възможности за сигурност. Тези модели обхващат извлечените поуки, добри практики, както и конкретни технически съображения, представени в съвременните препоръки на Националния институт по стандартизация и технологии NIST (National Institute of Standards and Technology) на САЩ и Интернационалния съюз по телекомуникации ITU (International Telecommunication Union). Учебникът е предназначен основно за студенти магистри в дистанционна форма на обучение по специалността „Информационна сигурност“.
3.	Представяне и обработка на информацията в микропроцесорната техника. Издателски комплекс на ШУ „Еп. К. Преславски“, 2014, ISBN 978-954-577-846-9, с 86.	Електронен учебник	86	-	Разгледани са бройните системи за представяне на информацията – двоична, осмична и шестнайсетична, както и форматите за представяне на целочислени, реални, символни и логически данни. Дефинирани са основните аритметични и логически операции за обработката на информацията в микропроцесорната техника. Подробно са анализирани архитектурите на комбинационните и натрупващи суматори, както и основните алгоритми за умножение и деление на целочислени и реални данни, извършвани в аритметично-логическото устройство на микропроцесора. Всяка от петте теми е илюстрирана с множество конкретни примери и задачи за самостоятелна работа, които да спомогнат за по-доброто самостоятелно възприемане на представената тематика, както и за успешното разработване на курсовите задачи в края на обучението. Учебникът е предназначен за дистанционно обучение на студенти от специалността „Комуникационни и информационни системи”. Той е разработен по учебната програма за дисциплината “ Микропроцесорна техника” от учебните планове за обучение в ОКС “бакалавър” в

1	2	3	4	5	6
					професионално направление "Комуникационна и компютърна техника".
4.	Технологични решения за информационна сигурност. Издателски комплекс на Национален военен университет „Васил Левски", 2013, ISBN 978-954-753-130-7. с 110.	Електронен учебник	110	Р. А. Богданов	Учебникът е посветен на основните технологични решения за осигуряване на целите на информационната сигурност: конфиденциалност, цялостност, наличност, автентификация, недопускане на отхвърляне, както и управление на достъпа. Разгледани са въпроси свързани с архитектурата на сигурността в еталонния модел за взаимодействие между отворени системи и дефинираните в нея услуги и технологии за информационна сигурност, както и връзките между тях. Подробно са описани принципите на работа на широко използваните технологични решения за криптиране на информация, управление на достъпа и осигуряване целостта на предаваната информация. В заключение са предложени варианти за избор на технологични решения за сигурност на информацията в зависимост от предоставяните услуги за сигурност. Учебникът е предназначен основно за студенти магистри в дистанционна форма на обучение по специалността „Информационна сигурност".
5.	Успешна научна публикация. Занятия на декана на Факултет „Артилерия, ПВО и КИС", 13-14.03.2014	Научноме-тодически доклад	9	-	В научнометодическата разработка са пояснени основните термини, описващи видовете научни публикации, представени са насоки за изграждане на подходяща структура на успешна научна статия и са представени някои етични проблеми при подготовката на научната статия за публикуване.
3. Статии в научни списания и публикации в годишници (20 бр., 138 стр.)					
1.	Криптирането – стратегическа част на системите за сигурност. *CIO*, бр. 7. 2016, стр. 66-67. http://cio.bg/8073_kriptiraneto__strategicheska_chast_na_sistemite_za_sigurnost	Научно-популярен	2	Д. Дойчинов	Предвид на нараствалата потребност от защита на чувствителната информация е обоснована необходимостта от въвеждане на ново регулиране на защитата на данните в ЕС. За целта всяка организация трябва да използва криптиране на данните като основен инструмент за тяхната защита. Криптирането трябва да се прилага за всички данни, независимо дали те се съхраняват, предават или използват в момента. Криптирането, като стратегическа част от системата за сигурност, трябва да работи заедно с допълващи се технологии, които включват контрол на достъпа и интелигентни системи за сигурност.
2.	Следващо поколение	Научно-	3	-	В статията накратко се представя съвременното състояние на

1	2	3	4	5	6
	киберсигурност - предвиждане на заплахите. *CIO*, бр. 7. 2015, стр. 51-53. http://cio.bg/7296_sledvashto_pokolenie_kibersigurnost__predvizhdane_na_zaplahite	популярен			киберсигурността и на тази основа е изведена необходимостта от въвеждане на фундаментално нов подход в следващото поколение киберсигурност, който не само да реагира на осъществени заплахи, а да предвижда тяхното възникване.
3.	Algorithms for Extended Galois Field Generation and Calculation. *Mathematical and Software Engineering*. Vol 1, No 1, 2015, pp. 18-24. ISSN: 2367-7449 http://www.varepsilon.com/index.php/mse/article/view/7	Научно-приложен	7	A. T. Tasheva	*The paper aims to suggest algorithms for Extended Galois Field generation and calculation. The algorithm analysis shows that the proposed algorithm for finding primitive polynomial is faster than traditional polynomial search and when table operations in GF(p^m) are used the algorithms are faster than traditional polynomial addition and subtraction.* Статията има за цел да предложи алгоритми за генериране и изчисления в разширено поле на Галоа $GF(p^m)$. Анализът на алгоритъма показва, че предложеният алгоритъм за намиране на примитивен полином е по-бърз от традиционните алгоритми за претърсване на всички полиноми, и използването на таблични операции в $GF(p^m)$ повишава бързодействието на алгоритмите за събиране и изваждане в сравнение с традиционните.
4.	On Linear Complexity of Generalized Shrinking-Multiplexing Generator. *Journal of Basic and Applied Research International*, *4*(1), 2015. International Knowledge Press. pp. 8-17. ISSN: 2395-3438 (Print), 2395-3446 (Online). http://www.ikpress.org/abstract.php?iid=489&id=42&aid=3673#.VcsyQ_mqpHw	Научен	10	-	*The linear complexity of the Generalized Shrinking-Multiplexing Generator (GSMG), based on Linear Shift Feedback Registers (LFSRs), is investigated in this paper. The lower and upper bounds of linear complexity of its output binary Pseudo Random Sequences are established. It is proved that the linear complexity increases exponentially with the length of the control p-ary LFSR and the prime p used. Some linear complexity analysis is given. It is shown that the linear complexity of the GSMG based on LFSRs is greater than the linear complexity of the Shrinking Generator.* В статията е изследвана линейната сложност на Обобщения Свиващ-Мултиплексиращ генератор (*GSMG*), базиран на преместващи регистри с линейни обратни връзки (*LFSRs*). Математически са доказани долната и горна граници на линейната сложност на изходните *GSMG* двоични псевдослучайни последователности. Доказано е, че линейната сложност се увеличава експоненциално с увеличаване на дължината на управляващия *p*-ичен *LFSR* и използваното просто число *p*. Анализирани са резултатите от практически изследваната линейна сложност на генерираните последователности. Показано е, че линейната сложността на *GSMG*, основан на *LFSRs*, е по-голяма от линейната сложност на свиващия генератор (*SG*).
5.	Briefly about the basic properties of	Научен	9	A. T.	*In this paper a brief review of p-ary m-sequences properties is made. The balance property, run property, two level autocorrelation and ideal k-tuple distribution properties with*

1	2	3	4	5	6
	p-ary *m*-sequences. *International Journal Science Education Innovation, Volume 4*, 2015, ISSN 1314-9784, pp. 5-13 http://www.associationsar.com/wp-content/uploads/2015/09/vol-4-innovation.pdf			Tasheva	*examples in Galois Field GF(3^n) are discussed. These properties allow us to consider p-ary m-sequences as random process with uniform distribution.* В статията е направен кратък преглед на основните свойства на *p*-ичните *m*-последователности. Дискутирани са свойствата балансираност, разпределение на сериите, автокорелационна функция с две нива и идеално разпределение на *k*-торките, като са приведени примери в поле на Галоа GF(3^n). Доказано е, че тези свойства позволяват *p*-ичните *m*-последователности да се разглеждат като случаен процес с равномерно *p*-ично разпределение.
6.	Randomness Testing of Sequences Produced by *p*-ary Generalized Self-Shrinking Generator Using Approximate Entropy. *Journal scientific and applied research, vol. 5*, 2014. ISSN 1314-6289, pp. 76-84. http://web.b.ebscohost.com/abstract?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=13146289&AN=99641218&h=NtwWNxhhS4mm%2b6RDsejEpIdvhSHvRYZ84Pst1RTZsIs8a%2b%2b9hFwIaUkKgEvzLk2X9QTOMn9by2yWHgo61ORAdQ%3d%3d&crl=c&resultNs=AdminWebAuth&resultLocal=ErrCrlNotAuth&crlhashurl=login.aspx%3fdirect%3dtrue%26profile%3dehost%26scope%3dsite%26authtype%3dcrawler%26jrnl%3d13146289%26AN%3d99641218	Научно-приложен	9	A. T. Tasheva	*In this paper a supervene testing for sequences generated by p-ary Generalized Self-Shrinking Generator (pGSSG) is made. Thanks to the Approximate Entropy (ApEn) approach certain randomness properties are proved to be possessed by them. In order to test the applicability of the generator the pGSSG sequence minimum length in excess of which it can be considered that the sequence behaves as truly random is detected.* В статията са тествани случайните свойства на последователностите, генерирани от *p*-ичния Обобщен Самосвиващ Генератор (*pGSSG*). Благодарение на приложения подход, базиран на приблизителната ентропия (*ApEn*) е доказано, че изходните *pGSSG* последователности притежават случайни свойства. Математически е определена минималната дължина на *pGSSG* последователността, при надвишаването на която генераторът да се счита, че се държи като истински случаен.
7.	Software Stream Cipher based on pGSSG Generator. *International Journal of Cyber-Security and Digital Forensics (IJCSDF) - Hong Kong*, *3*(2), 2014, pp. 111-121. http://sdiwc.net/digital-	Научно-приложен	11	Tasheva, A., Nakov, O.	*Secrecy of a software stream cipher based on p-ary Generalized Self-Shrinking Generator (pGSSG) is examined in this paper. Background information for the generator's algorithm is provided. The software architecture and key management for the cipher initialization are explained. Galois Field GF(257^{32}) and feedback polynomials are chosen for initialization of the generator. In order to examine the secrecy mathematical model of the software system is made. It is proved that the cipher is not perfect but the empirical tests result in less than 0,0125% deviation of the encrypted files' entropy from the perfect secrecy. At last the*

1	2	3	4	5	6
	library/software-stream-cipher-based-on-pgssg-generator.html				*proposed cipher is compared to four eSTREAM finalists by key length and period.* В статията е изследвана сигурността на софтуерен поточен шифър, базиран на *p*-ичен Обобщен Самосвиващ Генератор (*pGSSG*). Представена е основна информация за алгоритъма на работа на генератора. Пояснени са софтуерната архитектура на генератора и управлението на секретните ключове при нейната инициализация. Избрани са подходящи за инициализацията на генератора поле на Галоа $GF(257^{32})$ и полиноми за обратна връзка. С цел да се изследва сигурността на генератора е предложен математически модел на софтуерната система. Доказано е, че шифърът не е съвършен, но емпиричните тестове показват по-малко от 0,0125% отклонение на ентропията на криптираните файлове от перфектната сигурност. В заключение, предложеният шифър е сравнен с четири eSTREAM финалисти по дължина на използвания ключ и период на генерираната псевдослучайна последователност.
8.	Предизвикателства към сигурността на съвременните информационни системи. *CIO*, бр. 7. 2014, стр. 55-58 http://cio.bg/6511_predizvikatelstva_kam_sigurnostta_na_savremennite_informacionni_sistemi	Научно-популярен	4	-	Статията разглежда проблемите на традиционния модел за информационна сигурност, анализира основните 5 тенденции в развитието на зловредния софтуер през 2014 година и на тази основа определя основните характеристики на платформа за сигурност, от която се нуждаят държавните агенции.
9.	Combining cryptography and steganography in software system for hiding confidential information. *Journal Science Education Innovation, Volume 1*, 2013. Association Scientific and Applied Research International Journal, pp. 84-92.	Научно-приложен	9	A. T. Tasheva	*The basic idea of combined use of both cryptographic and steganographic methods is first to do data encryption with AES block cipher and then hiding encrypted data in an image that does not attract any attention. As a consequence, the reliability of hiding information increases which have been evidenced by a comparative analysis of stego-images quality at different levels of protection.* Основната идея на комбинирана употреба на криптографските и стеганографски методи е първоначално криптиране на данните с *AES* блоков шифър и след това скриване на шифрованите данни в изображение, което не привлича вниманието. В резултат на това, надеждността на скриване на информацията се увеличава, което се потвърждава от направения анализ на качеството на стего-изображенията при различни нива на защита.
10.	Предизвикателства пред сигурността на облачните	Научно-популярен	3	-	В статията е представена основната визия за развитие на облачните технологии за отбраната, като са посочени четири стъпки, които ще

1	2	3	4	5	6
	технологии. *CIO*, бр. 7. 2013, стр. 57-59. http://cio.bg/5600_sigurnostta_na_oblachnite_tehnologii__predizvikatelstvo_pred_it_prilozheniyata_za_otbranata				позволят поетапна реализация на корпоративната облачна среда за отбраната. Пояснени са основните модели и характеристики на облачните технологии и на тази основа са определени ключовите предизвикателства пред сигурността на облачните технологии за отбраната.
11.	Някои въпроси относно сигурността на радио комуникациите на бойното поле. *CIO*, бр. 7, 2012, с. 65-66. http://cio.bg/4761_nyakoi_vaprosi_otnosno_sigurnostta_na_radio_komunikaciite_na_bojnoto_pole	Научно-популярен	2	Р. А. Богданов	В статията са разгледани компоненти на информационната сигурност в светлината на предизвикателствата, стоящи пред военни технологични лидери. Дадени са основните определения, касаещи сигурността на съвременните радиокомуникации. Разгледани са подходите са осигуряване на сигурността и са дадени примери за технологични решения. Показани са тенденциите и предизвикателствата при използва не на *FPGA* като основен градивен елемент на съвременните системи за сигурност.
12.	Безжичните 4G системи – изисквания и характеристики. *CIO*, бр. 7, 2011, с. 56-57. http://cio.bg/3970_bezzhichnite_4g_sistemi__iziskvaniya_i_harakteristiki	Научно-популярен	2	-	В статията са разгледани основните характеристики на напълно функциониращите и широко разпространени *IMT-Advanced* системи, които ще се превърнат в напълно обичайни през следващите десет години. Подробно са разгледани изискванията на *IMT-Advanced*, както и основните характеристики на двете кандидат-технологии, които се борят за 4G статус. Обсъждат се техните различни подходи при спазване на изискванията за *IMT-Advanced*.
13.	Еволюция на мобилните мрежи към 4G поколение. *CIO*, бр. 7, 2010,с. 48-50. http://cio.bg/3276_evolyuciya_na_mobilnite_mrezhi_kam_pokolenie_4g	Научно-популярен	3	Р. А. Богданов	В статията е разгледана еволюцията на мобилните комуникационни устройства към следващия етап от тяхното развитие и са анализирани тенденциите в разработването на системите от поколение 4G. Разгледани са основните услуги, които ще се предлагат от 4G системите, както и техническите характеристики, които трябва да бъдат осигурявани, за да се реализират тези услуги. Изведени са общите тенденции в техническо отношение, валидни за всички формати и варианти на устройства, имащи претенции да удовлетворяват изискванията на спецификации *IMT-Advanced* на международната организация *ITU-R*. Направен е анализ на предложенията на основните разработчици на 4G устройства.
14.	Generalization of the Self Shrinking Generator in the Galois Field GF(p^n). *Journal of Information Technology*	Научен	9	Al. Milev	*Wireless WLAN and WMAN technologies are gained the most popularity because of their benefits such as portability and flexibility, increased productivity and lower installation costs. The main problem in these networks is security related not only to the information but*

1	2	3	4	5	6
	and Communication Security, Bucharest, Romania, 2009, pp.53-62, ISBN 978-606-505-283-3				*for authentication as well. The strength of the encryption algorithm is as better as the non-linearity of generated encrypted data is much increased. The architecture of the non-binary Generalized Self-Shrinking Generator (GSSG) is proposed in this paper. It is shown that generated sequence has non-linear and it is hard to be recognized by attackers. A method for transformation of non-binary self-shrunken sequence into balanced binary sequence is given. The properties of generated sequence are analyzed. The GSSG applications ensure confidentiality of the transmitted data in wireless networks and it can increase the security level by using a second additional encryption level with GSSG in networks.* Безжичните WLAN и WMAN технологии са спечелили голяма популярност поради своите предимства като преносимост и гъвкавост, повишена производителност и по-ниски разходи за монтаж. Основният проблем в тези мрежи е сигурността, свързана не само с информацията, но и с механизмите за автентификация. Алгоритъмът за криптиране е толкова по-добър, колкото по-голяма е нелинейността на генерираните ключови потоци. В статията се предлага архитектура на недвоичен Обобщен Самосвиващ Генератор (*GSSG*). Показано е, че генерираната изходна *GSSG* последователност е нелинейна и е трудно да бъде разпозната от атакуващите. Предложен е метод за преобразуване на изходната *GSSG* недвоичната самосвита последователност в балансирана двоична последователност. Анализирани са свойства на генерираната *GSSG* последователност. Доказано е, че приложенията за *GSSG* гарантират поверителността на предаваните данни в безжични мрежи, както и това, че може да се повиши нивото на сигурността чрез използване на второ допълнително ниво на криптиране с *GSSG* генератора в тези мрежи.
15.	WLAN and WMAN Security Problems. *Journal of Information Technology and Communication Security*, Bucharest, Romania, 2009, pp.195-204, ISBN 978-606-505-283-3	Научно-приложен	9	T. Tashev, Al. Milev	*Nowadays, the* W*ireless WLAN and WMAN technologies are gained the most popularity because of their benefits such as portability and flexibility, increased productivity and lower installation costs. The mesh networks using WiMAX is a backhaul function and the local WiFi hotspots to provide the wireless broadcast are the feature to mobile citywide access. Their success will depend on the level of security being offered. The aim of this paper is to make a survey of the security problems in most used WLAN and WMAN technologies. The paper is organized as follows. Firs, the tree basic security services in WiFi technologies are described. Then the particular security weaknesses and the know attacks in WLANs are investigated and analyzed. Second, the same security problems in WiMAX technologies are shown. Finally, the WLAN and WMAN security services are compared.* В днешно време, безжичните *WLAN* и *WMAN* технологии имат голяма популярност поради своите предимства като преносимост и гъвкавост, повишена производителност и по-ниски разходи за монтаж. Меш

1	2	3	4	5	6
					мрежите, използващи *WiMAX* и *WiFi* технологиите, са основните елементи на безжичните градски мрежи. Успехът на тези технологии основно зависи от нивото на сигурност, което се предлага на потребителя. Целта на тази статия е да се направи проучване на проблемите на сигурността в най-използваните *WLAN* и *WMAN* технологии. Статията е организирана по следния начин. Първо са описани трите основни услуги на сигурността в *WiFi* технологиите. След това са изследвани и анализирани конкретните слабости в сигурността и възможните атаки в *WLAN* мрежите. На второ място са показани проблемите със сигурността в *WiMAX* технологиите. Накрая са сравнени услугите на сигурността в *WLAN* и *WMAN* мрежите.
16.	A Method of Phase-Manipulated Complementary Signals Applying in Spacecraft-based Radars. *Aerospace Research in Bulgaria*, No 21, 2007, pp. 105-114	Научно-приложен	10	Bedzhev B. Y., Bogdanov R. A.	*Radar imagery, realized by means of Synthetic Aperture Radars (SARs) is very important in exploring planet, satellite and comet surfaces. The most valuable feature of the autocorrelation function (ACF) of the SAR signals is the level of their side lobs, because they determine the dynamic range of the image and the possibility to discover small objects. With regard to this, our paper suggests a method for applying in spacecraft-based SARs the so named generalized complementary signals whose ACF does not have any side-lobs. It uses the polarization features of electromagnetic waves.* Радарните образи, получени с помощта на радари със синтезирана апертура (*SAR*), са много важни за проучване на повърхностите на планети, сателити и комети. Най-важната характеристика на автокорелационната функцията (*ACF*) на *SAR* сигналите е нивото на техните странични листи, защото то определя динамичния диапазон на изображението, както и възможността да се откриват малки обекти. Във връзка с това, статията предлага метод за прилагане на така наречените обобщени комплементарни сигнали, чиито *ACF* няма никакви странични листи, в космически базирани *SAR*. Той използва поляризационните характеристики на електромагнитни вълни.
17.	Метод синтеза совершенных двумерных массивов. *Международный научно-технический журнал „Проблемы управление и информатики”*, № 5, сентябрь – октябрь, 2006, стр. 131-137, ISSN 0572-2691	Научно-приложен	7	Б. Й. Беджев, Б. П. Стоянов	*Уровень боковых лепестков авто-корреляционной функции представляет очень важный параметр сигналов, используемых в коммуникациях, так как он существенно влияет на основные характеристики систем. Ввиду этого большие усилия были затрачены на разработку методов синтеза сигналов, чья авто-корреляционная функция „идеальна”, т.е. подобна дельта импульсу. Независимо от того, список известных сегодня классов сигналов с такими авто-корреляционными функциями нельзя считать достаточно полным. По этой причине в нашей статье мы представляем математический метод синтеза одного класса сигналов, названые „совершенные двумерные массивы”, чья двумерная авто-корреляционная функция*

1	2	3	4	5	6
					свободна от боковых лепестков и кратко исследуем их практическое применение. Нивото на страничните листи на автокорелационната функция е много важен параметър на сигналите, използвани в комуникациите. С оглед на това, учените полагат големи усилия за разработването на методи за синтез на сигнали, чиято автокорелационна функция е „идеална“, т.е. тя е подобна на делта импулс. Независимо от това, списъкът на известните до сега класове сигнали с такава автокорелационна функция не може да се счита за достатъчно пълен. Поради тази причина, в статията е предложен математически метод за синтез на клас сигнали, наречени „перфектни двумерни масиви“, чиято двумерна автокорелационна функция е без странични листи и накратко е изследвано неговото практическо приложение.
18.	The Method for Synthesis of Perfect Two-Dimensional Arrays. *Journal of Automation and Information Sciences*, Vol. 38 Number 10, 2006, pp. 56-62, ISSN 1064-2315 **Impact factor: 0.024** **5-Year Impact Factor: 0.056** **SJR: 0,312**	Научен	7	Bedzhev B. Y. Stoyanov B. P.	*The method for synthesis of perfect two-dimensional arrays (PTA) on the basis of a Kronecker product of two perfect one-dimensional arrays is proposed. Two algorithms for PTA synthesis are considered. It is shown that the PTA synthesis method can be generalized and used for synthesis of perfect r-dimensional arrays.* В статията се предлага метод за синтез на перфектни двумерни масиви (*PTA*) въз основа на произведение на Кронекер на два перфектни едномерни масива. Обсъждат се два алгоритъма за *PTA* синтез. Показано е, че методът на *PTA* синтез може да бъде обобщен и да се използва за синтез на перфектни *r*-мерни масиви.
19.	Анализ на съвременните видове уязвимости и експлойти в компютърните мрежи и системи. Годишник на шуменския университет „Еп. К. Преславски“ Технически науки, 2016, ISSN 1311-834X, стр. 112-122	Научно-приложен	11	О. М. Фетфов, П. Кр. Боянов, Т. Сп. Трифонов	В статията е направен анализ на съвременните уязвимости и експлойти в компютърните мрежи и системи. В резултат от сравнителния анализ на резултатите от проведените тестове и експерименти в конкретна компютърна система са открити някои слабости в компютърните мрежи и системи.
20.	Сравнителен анализ на съвременните видове антивирусни програми. Годишник на шуменския университет „Еп. К. Преславски“ Технически науки, 2016, ISSN 1311-834X, стр. 123-133	Научно-приложен	11	О. М. Фетфов, П. Кр. Боянов, Т. Сп. Трифонов	В статията е направен сравнителен анализ на съвременните видове антивирусни програми, използвани в компютърните мрежи и системи. Направени са препоръки към администраторите на киберсигурността, свързани с анализ на уязвимостите и слабостите в компютърните и мрежови системи, както и използването на антивирусен софтуер за стабилна и сигурна поддръжка от разстояние на всички компютърни ресурси и процеси в избрана компютърна система.

1	2	3	4	5	6
4. Научни доклади и статии в сборници на международни симпозиуми и конференции (6 бр., 34 стр.)					
1.	Algorithms for Building Extended Galois Field and Calculations in it. In *Proceedings of International Scientific Conference Computer Science'2015*, 2015, pp. 133-138. ISBN: 978-619-167-177-9	Научно-приложен	6	A. Tasheva	*The paper aims to suggest algorithms for building Extended Galois Field and conducting calculations in it. The algorithm analysis shows that the proposed algorithm for primitive polynomial finding is faster than traditional polynomial search and when table operations in GF(p^m) are used the algorithms are faster than traditional polynomial addition and subtraction.* В статията са предложени алгоритми за генериране на разширено поле на Галоа *GF*(p^m) и реализиране на основните аритметични операции в него. Предложеният алгоритъм за намиране на примитивен полином в *GF*(p^m) е по-бърз от традиционните алгоритми за претърсване на всички полиноми. Предложеното използване на таблични операции в *GF*(p^m) повишава бързодействието на алгоритмите за събиране и изваждане на полиноми в сравнение с традиционните.
2.	Research of the characteristics of a steganography algorithm based on LSB method of embedding information in images. In *Proceedings of International Scientific Technical Conference Technics. Technologies. Education. Safety '15*, Vol. 2, Information Technologies, Natural and Mathematical Sciences. 2015. pp. 56-59. ISSN: 1310 – 3946.	Научно-приложен	4	Stoyanova V	*The article deals with the steganography system which hides text inside images without losing data. The secret message is hidden in the cover image using Last Significant Bit (LSB) algorithm. To evaluate steganography system properties the measures like Signal-to-Noise Ratio (SNR), Peak Signal-to-Noise Ratio (PRSN), Mean Squared Error (MSE) and Structural Similarity Index for measuring (SSIM) are used. Experimental results show the advantages of the described steganography system.* Статията разглежда стеганографска система скриваща текстова информация в изображения без загуба на данни. Тайното съобщение се скрива в изображението посредством използване на алгоритъма на най-младшия бит (*LSB*). За да се оценят характеристиките на стеганографската система са използвани мерки, като отношение сигнал-шум (*SNR*), отношение на пиковата стойност на сигнал-шум (*PRSN*), средно квадратична грешка (*MSE*) и индекс за измерване на структурна прилика (*SSIM*). Експерименталните резултати показват предимствата на описаната стеганографска система спрямо традиционната.
3.	About Balance Property of the p-ary Generalized Self-Shrinking Generator Sequence In *Proceedings of the 14th International Conference on Computer Systems and Technologies*, ACM International Conference Proceeding Series, New York, NY, USA, 2013, pp. 299-306.	Научно-приложен	8	A. Tasheva, O. Nakov	*The Pseudo Random Sequences (PRSs) have been widely used for encrypting sensitive data in wireless networks, communication systems and other. The balance property of the previously proposed p-ary Generalized Self-Shrinking Generator (pGSSG) is examined. The theoretical value of the balance property of the sequences produced by the pGSSG is established and proven. Test results for it are compared to the theoretical ones. It is shown that the pGSSG sequences have the needed properties to be considered as balanced.* Псевдослучайните последователности (*PRSs*) са широко използвани за криптиране на чувствителни данни в безжични мрежи, комуникационни системи и други. В статията се изследва свойството

1	2	3	4	5	6
	http://dl.acm.org/citation.cfm?id=2516786 SCOPUS				балансираност на предложеният *p*-ичен Обобщен Самосвиващ Генератор (*pGSSG*). Математически е установена и доказана теоретичната стойност на свойството балансираност на последователностите, генерирани от *pGSSG*. Резултатите от проведените практически тестове на балансираността са сравнени с доказаните теоретични такива. Показано е, че изходните *pGSSG* последователности притежават необходимите качества, за да бъдат считани за балансирани.
4.	A comprehensive testing and analysis of the computer and network security vulnerabilities using the scanning program NESSUS. In *Proceedings of the 9th Baltic – Bulgarian Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics*, June 17-21, 2013, Riga, Latvia, ps. 162-165.	Научно-приложен	4	P. Kr. Boyanov	*In this paper a comprehensive and detailed computer systems vulnerabilities analysis is made. Several hosts are completely investigated against crucial security weaknesses and holes in their systems are found by means of the vulnerability system scanner Nessus. Thanks to this investigation some recommendations to computer users and security professionals to improve their system performance and detect and prevent malicious cyber-attacks are presented.* В статията е направен цялостен и подробен анализ на уязвимостите в компютърните системи. Множество хоста са напълно изследвани за критични слабости в тяхната сигурност и дупки в техните системи са открити с помощта на скенера за уязвимости Nessus. Благодарение на това изследване са предложени някои препоръки към компютърните потребители и професионалисти, работещи в областта на сигурността с цел да се подобри ефективността на системата и своевременно откриване и предотвратяване на злонамерени кибератаки.
5.	An Algorithm for Computer Synthesis of Pairs of Generalized Mutually Orthogonal Complementary Signals. In *Proceedings of the International Conference on Computer Systems and Technologies -* ***CompSysTech'06,*** ISBN-10:954-9641-46-5 ISBN-13:978-954-9641-46-2 pp. IIIA.22-1 - IIIA.22-6	Научно-приложен	6	B. Bedzhev, V. Mutkov	*The present communication-information systems must satisfy large number of strong requirements, concerning their quality of service. The simultaneous providing of these requirements is possible on the base of complex radio signals with pseudo random inner structure, which autocorrelation function (ACF) has ideal shape. With regard our paper aims to suggest a mathematical algorithm for synthesis of a new class of phase manipulated (PM) signals, named pairs of generalized mutually orthogonal complementary signals. They consist of two sets of generalized complementary signals (GCSs), which are unique among all PM signals with following their features:* *- their summary (aggregated) ACF has an ideal shape, similar to a delta pulse;* *- if a GCS with small length is known, then it is easy to create derivative GCSs with unlimited length;* *- the aggregated cross-correlation function (CCF) of the two sets of a pair is zero everywhere.* Съвременните комуникационно-информационни системи трябва да отговарят на множество изисквания относно предоставяното от тях качество на обслужване. Едновременното предоставяне на тези

1	2	3	4	5	6
					изисквания е възможно на базата на сложни радиосигнали с псевдослучайна вътрешна структура, чиято автокорелационна функция (*ACF*) има идеална форма. В тази връзка, статията цели да предложи математически алгоритъм за синтез на нов клас фазово манипулирани (*PM*) сигнали, наречени двойки обобщени взаимно ортогонални комплементарни сигнали. Те се състоят от две множества от обобщени комплементарни сигнали (*GCSs*), които са уникални сред всички PM сигнали със следните техни функции: - тяхната обобщена (сумарна) *ACF* има идеална форма, подобна на делта импулс; - ако е известен *GCS* с малка дължина, то е лесно да се създаде производно *GCSs* с неограничена дължина; - обобщената взаимнокорелационна функция (*CCF*) на две множества от двойки е нула навсякъде.
6.	A Method for Computer Design of Families of Generalized Mutually Orthogonal Complementary Signals. In *Proceedings of the International Conference on Computer Systems and Technologies -* ***CompSysTech'06,*** ISBN-10:954-9641-46-5 ISBN-13:978-954-9641-46-2 pp. IIIB.2-1 - IIIB.2-6	Научно-приложен	6	B. Bedzhev, V. Mutkov	*The scrutiny of the trends in the developing of communication devices shows that the so-named multicarrier code division multiple access (MC-CDMA) systems are a promising attempt for enhancement of quality of service and especially of the rate of information transmission. With regard our paper aims to suggest a mathematical method for synthesis of a new class of complementary sequences, named families of generalized mutually orthogonal complementary signals. They consist of sets of generalized complementary signals (GCSs), which are unique among all Phase Manipulated (PM) signals with following their features: their summary (aggregated) ACF has an ideal shape, similar to a delta pulse; if a GCS with small length is known, then it is easy to create derivative GCSs with unlimited length; the aggregated cross-correlation function (CCF) of the every two sets of a family is zero everywhere.* Тенденциите в разработването на комуникационни устройства показват, че системите с множествен достъп с кодово разделяне и множество носещи (MC-CDMA) предлагат подобряване на качеството на услугите и особено на скоростта на предаване на информация. В тази връзка, статията цели да предложи математически метод за синтез на нов клас комплементарни последователности, наречени семейства от обобщени взаимно ортогонални комплементарни сигнали. Те се състоят от множества от обобщени комплеметарни сигнали (*GCSs*), които са уникални сред всички фазово манипулирани (*PM*) сигнали със своите характеристики: тяхната обобщена (сумарна) автокорелационна функция (*ACF*) има идеална форма, подобна на делта импулс; ако е известен *GCS* с малка дължина, то е лесно да се създаде производно

1	2	3	4	5	6
					GCSs с неограничена дължина; обобщената взаимнокорелационна функцията (*CCF*) на всеки две множества от семейството е нула навсякъде.
5. Научни доклади в сборници от научни конференции (15 бр., 128 стр.)					
1.	Обобщен самосвиващ генератор на псевдослучайни последователности. Сборник научни трудове на НК „Новите предизвикателства пред системите за информационна сигурност“, Издателство на НВУ „В. Левски“, 2015, стр. 56-70. ISBN 978-954-9681-65-9	Научно-приложен **Пленарен доклад**	15	-	В статията се представя нов метод за генериране на *p*-ични *PRSs* с повишена нелинейност и сигурност, който може да се използва като генератор на ключов поток в поточните шифри. Предложеният *p*-ичен обобщен самосвиващ генератор *pGSSG* позволява лесно и ефективно генериране на *p*–ична псевдослучайна последователност с повишена нелинейност. Доказаната експоненциална зависимост на периода T *и* линейната сложност λ на генерираната от *pGSSG* последователност от дължината на градивния *pLFSR* регистър позволява предложената архитектура да генерира нелинейни псевдослучайни последователности с много големи периоди на повторение при сравнително проста схема на управление.
2.	Генериране на p-ични кодове на Рийд-Соломон. Сборник научни трудове на научна конференция MATTEX 2014, том 2, раздел „Комуникационна и компютърна техника и технологии“, Университет-ско издателство „Еп. К. Преславски“, с. 55-63. ISSN: 1314-3921	Научно-приложен	9	-	Реалните приложения на кодовете на Рийд-Соломон използват представяне на символите в полета на Галоа $GF(2^8)$. В множество изследователски статии в теоретичен план конструирането на кодовете на Рийд-Соломон се представя над произволно поле $GF(q)$ от q на брой елементи, където q е степен на просто число. Независимо от това теоретично представяне, примерите поясняващи кодовете на Рийд-Соломон са над полета с основа 2. Затова целта на тази статия е да разгледа по-подробно конструирането на кодовете на Рийд-Соломон като семейство кодове над произволно поле $GF(p^n)$, като се изведат особеностите произтичащи от генерирането на кодовете при полета с основа различна от 2.
3.	Сравнителен анализ на злонамерени уеб-базирани атаки. Сборник научни трудове на научна конференция „Защита на информацията - състояние и перспективи“, 7-8 юни 2013, стр. 178-184. ISBN 978-954-9681-49-9	Научно-приложен	7	Петър Кр. Боянов	Целта на този доклад е да се направи сравнителен анализ на най-актуалните злонамерени уеб-базирани атаки и заедно с това да се предоставят определени мерки за защита от злонамерени уеб-приложения. Този доклад е структуриран по следния начин. В раздел 2 са представени и сравнени предишни научни разработки и решения на уеб-базирани атаки. В раздел 3 е илюстрирана методологията на най-злонамерените уеб-базирани атаки. Резултатите от изследването са

1	2	3	4	5	6
					показани в раздел 4. Изводите и бъдещата работа са представени в раздел 5.
4.	Неоторизирано проникване в компютърна система с активирани защитна стена и антивирусен софтуер. *Компютърни науки и технологии, година XI, брой 1/2013*, стр. 41-46, ТУ-Варна, ISSN 1312-3335 Юбилейна научна конференция с международно участие 45 години катедра "Компютърни науки и технологии"	Научно-приложен	6	П. Кр. Боянов	В статията са представени резултати от осъществено неоторизирано проникване в операционната система Microsoft Windows XP SP3 с цел получаване на пълен достъп до ресурсите на избраната компютърната система. Атаката е реализирана успешно, въпреки че в дадения хост са активирани защитна стена и антивирусен софтуер. Благодарение на специално избрана платформа за злонамерено проникване и определен злонамерен експлойт за тази операционна система е получен пълен безжичен отдалечен достъп до ресурсите на този хост. Затова е необходимо да се използва по-сигурна и надеждна операционна система.
5.	Анализ на сигурността в GSM комуникациите. *Компютърни науки и технологии, година XI, брой 1/2013*, стр. 97-103. ТУ-Варна, ISSN 1312-3335 Юбилейна научна конференция с международно участие 45 години катедра "Компютърни науки и технологии"	Научно-приложен	7	А. Т. Ташева	В статията е направен анализ на основните атаки на по-силния *GSM* шифър A5/1. Разгледани са първите реални хардуерни реализации на атаки, представени в общодостъпната литература. В резултат на анализа е направен извод за необходимостта от допълнително криптиране на информацията в *GSM* комуникациите когато се предават чувствителни и конфиденциални данни.
6.	Система за скриване на конфиденциална информация чрез комбинирано използване на криптографски и стеганографски методи. Сборник доклади на международна научна конференция “Немус 2012“. Пловдив, 2012	Научно-приложен	8	Ташева, А. Т.	Основната идея за комбинираното използване на двата метода в системата за скриване на конфиденциална информация, предложена в доклада, е криптиране на данните с *AES* блоков шифър и след това скриването им в изображение, което не привлича вниманието. Вследствие на това се повишава надеждността на скриване на информацията, което се доказва от направения сравнителен анализ на качеството на стего-изображенията при различните нива на защита.
7.	Криптиране на електронната поща: възможности и компромиси. Сборник научни трудове на научна конференция на Факултет ”А, ПВО и КИС”, гр. Шумен, 13-	Научно-приложен	9	-	Корпоративния шпионаж е един от най-бързо разрастващият се бизнес в наши дни. Негов обект са множеството данни за клиенти, служители, интелектуална собственост или поверителна финансова информация. Във връзка с това бизнесът трябва да гарантира, че чувствителната информация се съхранява сигурно и че нейният трансфер е съобразен

1	2	3	4	5	6
	15 ноември 2011, част I, „Комуникационни и информационни системи”. Шумен, Химера, 2012, с. 148 – 156. ISSN 1313-7433				със законите за поверителност, с цел да осигури безопасни сделки за своите клиенти и неприкосновеността на личния живот на своите служители. В статията се дискутират основните особености на криптографията с публичен ключ и компромисите, които корпоративните потребители и физическите лица трябва да правят, за да защитят конфиденциалната информация, предавана с електронна поща.
8.	4G безжичните системи: изисквания и характеристики. Сборник научни трудове на научна конференция на Факултет ”А, ПВО и КИС”, гр. Шумен, 13-15 ноември 2010, част I, „Комуникационни и информационни системи”. Шумен, Химера, 2011, стр. 175-183. ISSN 1313-7433	Научно-приложен	6	-	В доклада по-подробно се разглеждат изискванията на *IMT-Advanced*, както и основните характеристики на двете кандидат-технологии, които се борят за 4G статус, *LTE-Advanced* и IEEE 802.16m. Обсъждат се техните различни подходи при спазване на изискванията за *IMT-Advanced*.
9.	Анализ на двоичните последователности, използвани в CDMA системите. Сборник научни трудове на научна сесия на Факултет ”А, ПВО и КИС”, 13-15 ноември 2009, част 1. Шумен, Химера, 2010, с. 89-98. ISSN 1313-7433	Научно-приложен	10	Р. А. Богданов	В статията основно място е отделено на двоичните последователности, използвани в *CDMA* системите за разделяне на каналите на един потребител, разделяне на потребителите в рамките на една клетка и за намаляване на смущенията между базовите станции. В резултат на направения анализ са сравнени техните основни характеристики. Представени са математическия апарат и схемите на функциониране на кодовете, използвани във възходящия и низходящия канал на *CDMA*.
10.	Оценка на изчислителната сложност на алгоритмите за генериране на големи прости числа за целите на криптографията. Сборник научни трудове на Научна конференция „Проблеми на информационната сигурност”, 2009. Шумен, 2010. ISSN 1314-0647. CD, статия № 12	Научно-приложен	9	Р. А. Богданов	Разгледани са изискванията към алгоритмите за генериране на прости числа, предявявани с цел да се избегне възможността за намаляване нивото на сигурност и въпросите, на които трябва да се отговори при решаване на задачата за генериране на големи прости числа, приложими в асиметричната криптография. В статията са разгледани едни от често използваните детерминирани методи за генериране на прости числа, техните характеристики, предимства и недостатъци. Извършена е оценка на аритметичната сложност, направено е сравнение на асимптотичната сложност на алгоритмите в брой аритметични операции и са представени някои особености в тяхната

1	2	3	4	5	6
					практическата реализация. От направеното сравнение са обобщени изводи и препоръки.
11.	Техники за намаляване на интерференцията в UWB комуникационните системи. Сборник научни трудове, част I, „Комуникационни и информационни системи.”, 2008, с. 305 - 312	Научно-приложен	13	Т. Д. Ташев, Р. А. Богданов	В доклада са представени основните съотношения, характеризиращи работата на широколентовите комуникационни системи в условия на интерференция. Описани са и симулационно са изследвани основните подходи за рандомизация на спектъра на предавания сигнал. Симулационно е изследвана съвместната работа на две *UWB* комуникационни системи, използващи съответно разширяване на спектъра и импулсно-амплитудна модулация *PAM* (Pulse Amplitude Modulation), модулация *TH-SSPAM* и с непосредствено разширяване на спектъра и *PAM* модулация (*DS-SSPAM*) в системите GSM900, *UMTS/WCDMA* и *GPS*. В резултат на направените изследвания са показани спектрите на моделирания *UWB* предаван сигнал. Симулационното изследване доказва, че рандомизацията намалява влиянието, както на тяснолентовия, така и на широколентовия интерферентен сигнал, при което спектърът на предавания сигнал се изглажда, като енергийните пикове в него се разпределят по-равномерно.
12.	Съвременни широколентови технологии. Сборник научни трудове на международна научна конференция, посветена на Джон Атанасов и Джон Фон Нойман, том 2, Шумен, 2009, с. 354-361. ISBN 978-577-540-6 9 (т.2)	Научно-приложен	8	Р. А. Богданов	В доклада са обобщени основните характеристики на съвременните широколентови технологии, като е отделено особено място на свръх-широколентовите системи. Представени са тенденциите в развитието на широколентови технологии. Разгледани са методите за генериране на широколентови сигнали, техните предимства и трудностите възникващи при използването им. *UWB* има редица особености, които я правят привлекателна за потребителите на комуникационни приложения. За разлика от конвенционалните системи, *UWB* предавателят генерира кратковременни импулси, които могат да се разпространяват без да е необходимо допълнително радиочестотно смесване на сигнали. *UWB* приемникът е хомодинен крос корелатор, базиран на архитектурата, използвана за пряко преобразуване на радиочестотата в основната лента, без да е необходимо междинно честотно преобразуване. *UWB* системите осигуряват ниска вероятност за прихващане/детекция, което ги прави ефективни за военни приложения и такива за сигурност. Това прави реализацията по-проста от тази в конвенционалната суперхетеродинна система.

1	2	3	4	5	6
13.	Анализ на сигурността в безжичните ZIGBEE персонални мрежи. Сборник научни трудове, част I, „Комуникационни и информационни системи.”, 2006, с. 393 - 399, ISBN-13: 978-954-9681-19-2	Научно-приложен	7	Т. Д. Ташев	В статията е направен сравнителен анализ на сигурността в безжичните *ZigBee* персонални мрежи по три основни показателя: автентичност, конфиденциалност и цялостност. В заключение са обобщени основните преимущества и слабости в сигурността на *ZigBee* мрежите.
14.	Метод за преобразуване на *p*–ични псевдослучайни последователности в двоични при запазване баланса на единиците и нулите. Научни трудове на РУ”А. Кънчев”, том 45, серия 3.2., 2006, ISSN 1311-3321, стр. 266-270	Научно-приложен	5	Т. Д. Ташев	В статията е предложен метод за преобразуване на всяко *p*–ично число в двоична последователност, при който разпределението на единиците и нулите е равномерно. Доказано е, че използването на метода преобразува *p*–ичната псевдослучайна последователност в двоична като запазва баланса на единиците и нулите в нея. В края на статията са анализирани свойствата и възможните сфери на приложение на метода.
15.	Линейна сложност на двоичните псевдослучайни последователнос-ти, генерирани от обобщения свиващ мултиплексиращ генератор. Сборник научни трудове от международна научна конференция „Хемус’06”, ВА Г. С. Раковски”, София 2006, ISSN 1312-2916, с. 164-172	Научно-приложен	9	Т. Д. Ташев, Б. Й. Беджев	В статията са доказани експоненциалните граници на линейната сложност на двоичните псевдослучайни последователности, генерирани от обобщения свиващ мултиплексиращ генератор GSMG (Generalized Shrinking Multiplexing Generator) с градивни линейни преместващи регистри с обратни връзки *LFSR* (Linear Feedback Shift Register). Статията е организирана по следния начин. Първо е направено кратко въведение в проблема. След това е описан принципът на действие на *GSMG* архитектурата, реализирана с *LFSR* регистри. Теоретически са доказани експоненциалните граници на линейната сложност на генерираните последователности. Накрая е направена оценка на линейната сложност и периодът на някои конкретни *2PRS* последователности.

Разпределение на научните трудове за придобиване
на академична длъжност „професор“ по видове:

Вид	**Брой**	**Страници**
Монография	**1**	**205**
Учебно-методически трудове	**5**	**515**
Статии в научни списания и публикации в годишници	**20**	**138**
Научни доклади и статии в сборници на международни симпозиуми и конференции	**6**	**34**
Научни доклади в сборници от научни конференции	**15**	**128**
Общо:	**47**	**1020**

07.10.2016 г.
гр. Шумен

доц. д.н. инж. Жанета Ташева