FRI-ONLINE-1-CCT2-08

COMPLEX SIGNALS APPLICATIONS FOR CYBERSECURITY ENHANCEMENT OF COMMUNICATION SYSTEMS, EXPLOITING ELECTRICAL POWER LINES [24]

Prof. Mihail Iliev, DcS
Department of Telecommunications,
"Angel Kanchev" University of Ruse, Bulgaria
Tel.: +359 887544257
E-mail: miliev@uni-ruse.bg

Prof. Borislav Bedzhev, DcS
Communication networks and systems Department, "Vasil Levski" National Military University, Faculty "Artillery, AD and CIS", Shumen, Bulgaria
Tel.: +359 888745681
E-mail: bedzhev@abv.bg

Eng. Dobri Stoyanov
Communication networks and systems Department, "Vasil Levski" National Military University, Faculty "Artillery, AD and CIS", Shumen, Bulgaria
Phone: +359 897567136
E-mail: dobri_stoyanov@mail.bg

Eng. Stanimir Parvanov
Air Defense Department, "Vasil Levski" National Military University, Faculty "Artillery, AD and CIS", Shumen, Bulgaria
Phone: +359 885123955
E-mail: ssparvanov@gmail.com

Abstract: *The power line communication (PLC) systems could be successfully used for enhancement of cybersecurity of smart grids management. One promising approach in this research area is the exploitation of complex signals, which are parctilally indetectable for the radio electronic intelligence of criminal or terrorist groups. Accounting this situation, in the paper a scheme for complex signals implementation in PLC systems is substantiated. The proposed scheme could be useful in the development of the new smart grids.*

Keywords: *Cybersecurity, Smart grid, Power line communication, Complex signal*

ВЪВЕДЕНИЕ

Започналата четвърта промишлена революция ще измени до неузнаваемост в положителна посока начинът на живот на човека. Нас ни очаква най-значителната за цялата история на човечеството трансформация, която ще засегне всички сфери на живот на обществото. Нещо повече, много изменения вече се наблюдават. Базово отличие на тази революция от всички предходни са синтезът и взаимодействието на следните технологии: големи бази данни и техния анализ (Big data, Big data analysis), Интернет на нещата (Internet of Things – IoT), виртуална и допълнена реалност (Virtual and augmented reality), 3D-печат (3D Printing), печатна електроника (Printed electronics), квантови изчисления (Quantum computing), блокчайн (Block-chain).

[24] Докладът е представен на заседание на секция 3.2 на 29 октомври 2021 с оригинално заглавие на български език: ПРИЛОЖЕНИЯ НА СЛОЖНИТЕ СИГНАЛИ ЗА ПОВИШАВАНЕ КИБЕРУСТОЙЧИВОСТТА НА КОМУНИКАЦИОННИТЕ СИСТЕМИ, ИЗПОЛЗВАЩИ ЕЛЕКТРОЕНЕРГЕТИЧЕСКИ ЛИНИИ

Тези технологии в момента излизат от етапа на разработване и проектиране (research and development-R&D).

Може да се обобщи, че четвърта промишлена революция ще доведе до повсеместна свързаност на хората чрез различни *комуникационно-информационни системи* (*КИС*) във всички сфери на обществото: научни изследвания, производство, търговия, здравеопазване, образование, развлечения, туризъм и т.н. За успешното изпълнение на тази мисия обаче комуникационните мрежи трябва да осигуряват пренасянето на огромни обеми информация в реално време между потребители, разположени практически върху цялата земна повърхност. Това е изключително тежък инженерен проблем поради следните причини. От една страна най-голяма пропускателна способност имат *комуникационните системи* (*КС*), използващи оптически и коаксиални кабели. От друга страна, по принцип изграждането на кабелна инфраструктура в планински, гористи и слабо урбанизирани територии е трудно и икономически неизгодно. Значителен потенциал за решаването на този проблем имат *КС, използващи енергоенергетическите* (*ЕЕ*) *линии* (КСИЕЛ, Power Line Communications - PLC). Действително, ЕЕ мрежите непрекъснато се развиват почти 140 години, в резултат на което ЕЕ линиите вече са прокарани до голям брой трудно достъпни и/или слабо населени райони. Към момента в Р. България възможностите на КСИЕЛ се използват в минимална степен. Предвид на този факт задачите на настоящия доклад са:

1) да се направи анализ на тенденциите в развитието на КСИЕЛ;

2) да се систематизират подходите за повишаване киберустойчивостта на КСИЕЛ на базата на сложни сигнали.

Тези задачи се решават в следващите два раздела на доклада.

ИЗЛОЖЕНИЕ

Анализ на тенденциите в развитието на комуникационните системи, използващи енергоенергетическите линии

Както се вижда от тяхното име, КСИЕЛ се характеризират с това, че енергията на сигналите се канализира с помощта вече изградените и експлоатирани ЕЕ линии. При това използваната от тях честотна лента е

$$F_{PLC} = 0\ [Hz] \div\ 500[kHz]. \qquad (1)$$

Ограничението (1) на честотните ленти на КСИЕЛ произтича от следните факти (Stoyanov, D., Bochev, L., Radev, I., 2021. Trends…). Първо, основният принцип на КСИЕЛ е употребата на вече изградените ЕЕЛ и за пренасяне на информация не трябва да пречи на нормалното функциониране на други КС. Второ, електромагнитните вълни с честоти над $500[kHz]$ в малка степен се канализират чрез проводниците на ЕЕЛ и, на практика, те се разпространяват основно в свободното пространство, при което те се превръщат в електромагнитни смущения за обикновените *радио-комуникационни системи* (РКС).

Историческото развитие на КСИЕЛ всъщност представлява постепенно усвояване на честотния диапазон (1) с все по-съвършени технологии (Stoyanov, D., Bochev, L., Radev, I., 2021. Trends…). По-конкретно, през 1922 г. първата КСИЕЛ, използваща амплитудна модулация на някаква носеща честота, започва да пренася телеметрична информация като използва ЕЕ линиите с високо напрежение и честотния диапазон $15\ [kHz] \div 500\ [kHz]$.

В най-съвременните КСИЕЛ се използва *ортогонално честотно разделяне и мултиплексиране* (*Orthogonal Frequency Division and Multiplexing* – OFDM), осигуряващо висока скорост на предаване на информацията без да се създават радио смущения за другите РКС. Както е известно, при OFDM честотната лента на комуникационната система се разделя на стотици и дори хиляди канали (например $N_{ch} = 256, 512, 1024, 2048, 4096, 8192$) с малка ширина, по които паралелно с малка скорост се предават информационните символи (най-често битове). Големият брой на каналите едновременно осигурява много високи обща скорост на предаване на информацията и шумоустойчивост (постига се чрез адаптивно изключване на каналите, които най-силно са засегнати от шумове и смущения). В резултат на това са постигнати максимални скорости на предаване на информацията от порядъка на

$100\ [kb/s] \div 150\ [kb/s]$, но максимална шумоустойчивост се осигурява при скорост на предаване на информацията от порядъка на $20\ [kb/s] \div 30\ [kb/s]$.

Днес най-високи скорости на предаване на информацията предоставят КСИЕЛ, използващи сигнали от микровълновия обхват, чиито носещи честоти са в диапазона $2\ GHz \div 20\ GHz$. При тези КСИЕЛ сигналите се разпространяват като напречни повърхностни вълни, при което е достатъчна само една ЕЕ линия (т.е. само една метална жица, монтирана над земната повърхност). Основното предимство на микровълновите КСИЕЛ е изключително високата пропускателна способност, която надхвърля $1\ Gbit/s$ в двете посоки. Както се вижда, тя е сравнима с пропускателната способност на кабелите, изградени от оптически влакна. Тук следва да се отбележат два взаимно свързани факта (Stoyanov, D., Bochev, L., Radev, I., 2021. Trends…). Първо, няколко фирми демонстрираха микровълнови КСИЕЛ, използващи нелицензираните честотни ленти около $2{,}4\ GHz$ и $5{,}3\ GHz$. Второ, микровълновите КСИЕЛ всъщност доказаха възможността в КСИЕЛ да се използват успешно широколентови сигнали в целия честотен диапазон $20\ MHz \div 20\ GHz$, който е много по-широк от диапазона $2\ MHz \div 80\ MHz$, определен за КСИЕЛ, прилагащи технологията *широколентов достъп чрез ЕЕ линии* (*Broadband over power line* - BPL).

От изложените факти може да се направи изводът, че КСИЕЛ могат да се използват успешно за осигуряване на надеждни и високоскоростни комуникации с различни обекти, разположени в планински, гористи и слабо урбанизирани територии. Тази възможност има много голямо значение и за така наречените умни ЕЕ мрежи, позволяващи на потребителите да са активна страна в доставянето и търговията с електрическа енергия (Erol-Kantarci, M., 2021), (Iliev, M., Bedzhev, B., Stoyanov, D., Parvanov, S., 2021). Те могат да намалят в значителна степен вредните последствия от човешката дейност върху околната среда чрез рационално управление на електрическите генериращи инсталации, както и на консумацията и преноса на електрическа енергия. За успешното изпълнение на тази мисия обаче в умните мрежи трябва да се използват технически решения, осигуряващи непрекъснатост и устойчивост на процесите на управление в реално време. Перспективно направление за решаване на тази сложна инженерна задача е едновременното предаване по няколко различни шумоустойчиви комуникационни канала на команди, справочни и телеметрични данни (Stoyanov, D., Bochev, L., Radev, I., 2021. Approaches …). Предвид на този факт, както и на анализа, направен в предходния раздел на доклада, изследването на подходите за повишаване киберустойчивостта на КСИЕЛ на базата на сложни сигнали има голямо практическо значение.

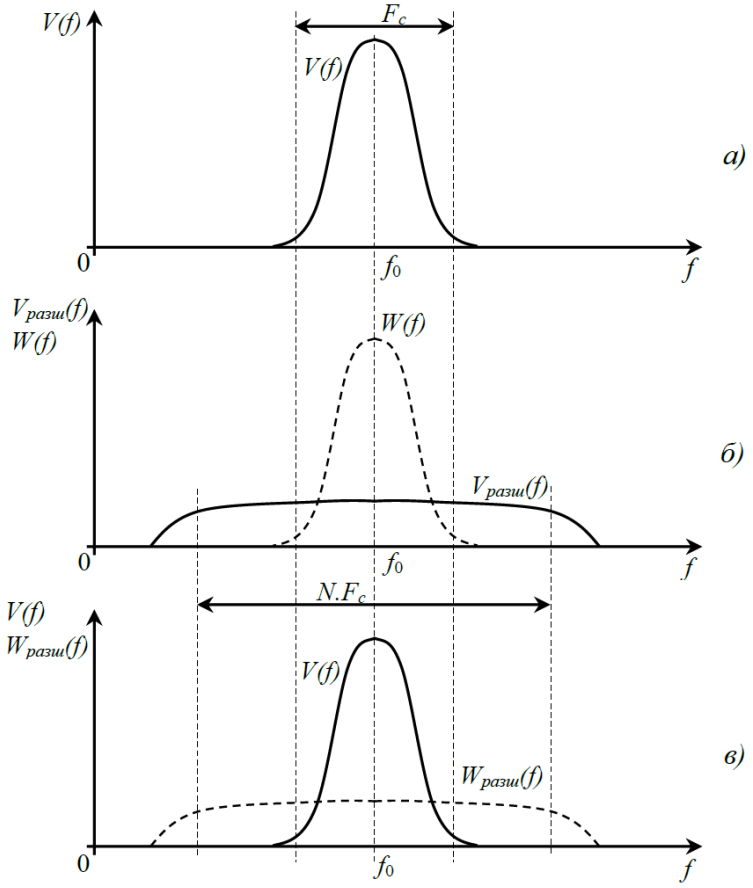
Подходи за повишаване киберустойчивостта на комуникационните системи, използващи енергоенергетическите линии на базата на сложни сигнали

Възможностите за повишаване шумозащитеността на КС в резултат на използване на *сложни сигнали* (СС) са известни още от 50-те години на миналия век (Dixon, R., 1976). Накратко те могат да бъдат описани по следния начин (Tsankov, Ts., 2018).

Когато КС използва СС, тогава под управлението на специална *разширяваща функция* (*разширяващ сигнал*) всеки един информационен символ от предаваните данни се трансформира в последователност от елементарни импулси с малка продължителност, наречени *елементарни импулси* или *чипове*. Формално-математически тази операция се описва със съотношението

$$v_{\text{разш}}(t) = v(t).g(t). \tag{2}$$

Тук $v(t)$ е прост сигнал, пренасящ един информационен символ от предавателя към приемника, $g(t)$ е разширяващата функция, а $v_{\text{разш}}(t)$ е резултантният сложен сигнал, чиято спектрална плътност $V_{\text{разш}}(f)$ има вида, показан на фиг. 1 б. Следва специално да се отбележи, че от предавателя по незащитен комуникационен канал до приемника се изпраща преднамерено разширения в спектралната област сигнал $v_{\text{разш}}(t)$.



Фиг. 1. Повишаване шумоустойчивостта на комуникационните системи в резултат на използването на сложни сигнали

Разширяващата функция $g(t)$ е уникална за всеки конкретен получател на информация и в неговия приемник се извършва корелационно приемане чрез сравняване на приетата разширяващата функция с предварително заложената. Формално-математически тази операция се описва със съотношението

$$v_{\text{разш}}(t).g^{-1}(t) = [v(t).g(t)].g^{-1}(t) = v(t). \quad (3)$$

Тук $g^{-1}(t)$ е сигнал, чието действие е обратно на действието на разширяващата функция, използвана в предавателя. По тази причина той се нарича *обратна разширяваща функция* (*сигнал*). В резултат в приемника спектралната плътност $V_{\text{разш}}(f)$ на полезните сигнали се свива до първоначалния си вид $V(f)$, показан на фиг. 1 в.

От друга страна, под въздействието на обратната разширяваща функция смущаващият сигнал $w(t)$ се трансформира в сигнала

$$w(t).g^{-1}(t) = w_{\text{разш}}(t), \quad (4)$$

като неговата спектрална плътност $W_{\text{разш}}(f)$ има вида, показан на фиг. 1 в. На входа на приемника обаче има честотно-избирателен филтър, който пропуска за по-нататъшна обработка само спектралните компоненти в честотната лента $F_{\text{с}}$ с централна честота f_0. Следователно, в резултат на използването на СС отношението сигнал/шум (*с/ш*, *signal-to-noise ratio-SNR*) по амплитуда $q_{\text{ип}}$ на изхода на приемника се подобрява право пропорционално на разширяването на спектъра сигналите, при което

$$q_{\text{ип}}^2 = 2Bq_0^2. \quad (5)$$

Тук $B = \tau_{\text{с}}(NF_{\text{с}}), B >> 1$ е базата на СС, $\tau_{\text{с}}$ и $NF_{\text{с}}$ са неговите продължителност и ширина на честотната лента съответно, а q_0 е отношението с/ш по амплитуда на входа на приемника.

От (5) се вижда, че $q_{\text{ип}}$ може да бъде достатъчно голямо дори при много малки стойности на q_0 – достатъчно е да се избере база B на СС с необходимата големина. Следователно

приемането на СС със съгласуван филтър или корелатор се съпровожда с усилване на сигнала (или подавяне на смущението) $2B$ пъти. Именно за това величината

$$K_{\text{СС}} = \frac{q_{\text{ип}}^2}{q_0^2} = 2B, \tag{6}$$

се нарича *коефициент на усилване на комуникационните системи със сложни сигнали* при обработката.

Аналогично, приемането на информация, пренасяна със СС, се характеризира с отношение с/ш по мощност:

$$h^2 = \frac{q_{\text{ип}}^2}{2} = Bq_0^2. \tag{7}$$

Съотношенията (6) и (7) са фундаментални в теорията на КС със СС. Те са получени за смущения от вида на бял шум с равномерна спектрална плътност на мощността в границите на честотната лента, ширината на която е равна на ширината на спектъра на СС. В най-общ случай е изпълнено:

$$K_{\text{СС}} \approx 2B, \tag{8}$$

като степента на приближение зависи както от вида на смущението, така и от базата на СС.

От (8) ясно се вижда, че използването от КС на СС води до повишаване на тяхната шумоустойчивост B пъти. Действително, нека отношението с/ш по мощност на изхода на приемника, осигуряващо нормална работа на КС, е $q_{\text{ип}}^2 = q_0^2$. Ако противникът започне да подавя КС със смущения, влошаващи отношението с/ш по мощност до стойност $q_{\text{ип}}^2 = \frac{1}{B}q_0^2$, тогава използването на СС с база B напълно ще компенсира вредния ефект на смущенията, тъй като $q_{\text{ип}}^2 = B\frac{1}{B}q_0^2 = q_0^2$.

Ползите от използването на КСИЕЛ със СС при внедряването и развитието на умни ЕЕ системи, както и за осигуряването на надеждни и високоскоростни комуникации с различни обекти, разположени в планински, гористи и слабо урбанизирани територии могат да се обяснят като се използва и формулата на Клод Шенон за определяне на пропускателната способност C на непрекъснат канал с нормален бял шум (Dixon, R., 1976):

$$C = F.log_2\left(1 + \frac{P_s}{P_n}\right) \approx 1{,}44.F.q_{sp}^2. \tag{9}$$

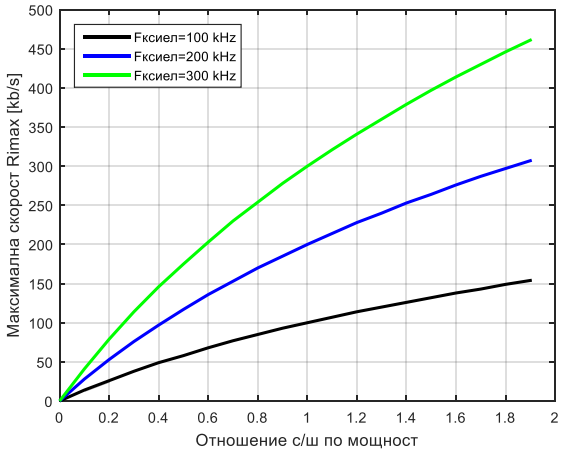
Тук: F е ширина на честотната лента на комуникационния канал, $P_s = FP_{s0}$ е мощността на използвания сигнал, P_{s0} е спектралната плътност на сигнала, $P_n = FP_{n0}$ е мощността на смущението (белия шум), P_{n0} е спектралната плътност на смущението, а $q_{sp}^2 = \frac{P_{s0}}{P_{n0}}$ е спектралното отношение с/ш по мощност.

Тук следва да се припомнят два факта. Първо, ако пропускателната способност на използвания комуникационен канал е C, тогава съществува способ за шумоустойчиво кодиране, осигуряващ скорост R_{Imax} на предаване на информацията

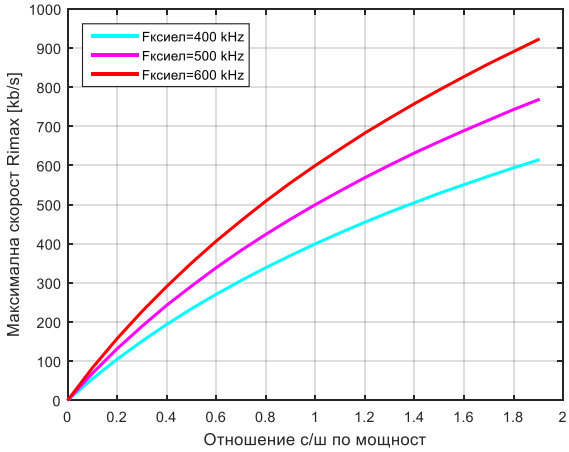
$$R_{Imax} = C\ [\frac{b}{s}]. \tag{10}$$

Второ, през последните тридесет години бяха разработени и успешно внедрени методи за шумоустойчиво кодиране (например турбо-кодовете), при които почти се достига скоростта на предаване на информацията, съгласно границата на Шенон (10).

Отчитайки тези факти, теоретичните максимални скорости на предаване на информацията R_{Imax} при ширини на честотните ленти на КСИЕЛ $F_{\text{КСИЕЛ}} = 100\ [kHz], 200\ [kHz], 300\ [kHz]$ и $F_{\text{КСИЕЛ}} = 400\ [kHz], 500\ [kHz], 600\ [kHz]$ са изчислени съгласно (9) и (10) за $q_{sp}^2 = 0 \div 1{,}9$ и са представени на фиг. 2 и фиг. 3 съответно. При това за повече нагледност е прието, че спектралните плътности на сигнала P_{s0} и смущението P_{n0} са постоянни (не зависят от честотата), при което за отношението с/ш по мощност е изпълнено $\frac{P_s}{P_n} = \frac{P_{s0}}{P_{n0}} = q_{sp}^2$.



Фиг. 2. Максимални скорости на предаване на информацията R_{Imax} при ширини на честотните ленти на КСИЕЛ $100\ [kHz], 200\ [kHz], 300\ [kHz]$



Фиг. 3. Максимални скорости на предаване на информацията R_{Imax} при ширини на честотните ленти на КСИЕЛ $400\ [kHz], 500\ [kHz], 600\ [kHz]$

Резултатите, показани на фиг. 2 и фиг. 3, демонстрират големите възможности на КСИЕЛ със СС за повишаване киберустойчивостта на умни ЕЕ системи, както и за осигуряването на надеждни и високоскоростни комуникации с различни обекти, разположени в планински, гористи и слабо урбанизирани територии.

Действително, при $SNR = 0{,}1$ и $F_{\text{КСИЕЛ}} = 100\ [kHz]$ (фиг. 2), максималната скорост на предаване на информацията е $R_{Imax} = 13{,}75\ [kb/s]$, която е достатъчна за управлението на умните ЕЕ мрежи. Същевременно, малката стойност на SNR прави практически невъзможно откриването и анализирането на използваните сигнали от радио-техническото разузнаване на криминални и терористични групи. В резултат на това, практически невъзможно става и имитирането на сигналите. От друга страна, при $SNR = 1{,}9$ и $F_{\text{КСИЕЛ}} = 500\ [kHz]$ (фиг. 3), максималната скорост на предаване на информацията е $R_{Imax} = 768{,}03\ [kb/s]$, която е достатъчна за осигуряване на нормална комуникация с екипите на планинско-спасителната служба, пожарната, граничната полиция и т.н.

ЗАКЛЮЧЕНИЕ

В доклада са анализирани тенденциите в развитието на комуникационните системи, използващи енергоенергетическите линии (Power Line Communications) и са систематизирани подходите за повишаване тяхната киберустойчивост на базата на сложни сигнали. Обоснованите изводи могат да бъдат полезни при внедряването и развитието на умни

електроенергетически системи, както и за осигуряването на надеждни и високоскоростни комуникации с различни обекти, разположени в планински, гористи и слабо урбанизирани територии в Република България.

БЛАГОДАРНОСТ

Този доклад е реализиран с подкрепата на Националната научна програма „Информационни и комуникационни технологии за единен цифров пазар в науката, образованието и сигурността (ИКТ в НОС)“, финансирана от Министерството на образованието и науката на България.

REFERENCES

Stoyanov, D., Bochev, L., Radev, I., (2021). Trends in the development of communication systems, exploiting electrical power lines. *Proceedings of International Scientific Conference "Defense Technologies" DefTech 2021, Faculty "Artillery, AD and CIS", Shumen, Bulgaria* (***Оригинално заглавие:*** *Стоянов, Д., Бочев, Л., Радев, Ив., 2021. Тенденции в развитието на комуникационните системи, използващи електроенергетически линии. Шумен: Сборник научни трудове на Международната научна конференция „Отбранителни технологии“ DefTech 2021, Факултет "Артилерия, ПВО и КИС")*.

Erol-Kantarci, M., (2021), "Smart Grid? Yes, AI Says: Bring It on!," *IEEE CTN*, Issue: April 2021.

Iliev, M., Bedzhev, B., Stoyanov, D., Parvanov, S., (2021). Technologies for enhancement of management sustainability of smart grids to imitation attacks. *Proceedings of University of Ruse - 2021, volume 60, Ruse, Bulgaria* (submitted) (***Оригинално заглавие:*** *Илиев, М., Беджев, Б., Стоянов, Д., Първанов, Ст., 2021. Технологии за повишаване устойчивостта на умните мрежи към имитационни атаки. Русе: Научни трудове на Русенския университет - 2021, том 60, (изпратен))*.

Stoyanov, D., Bochev, L., Radev, I., (2021). Approaches for cybersecurity enhancement of the energy infrastructure management. *Proceedings of International Scientific Conference "Defense Technologies" DefTech 2021, Faculty "Artillery, AD and CIS", Shumen, Bulgaria* (***Оригинално заглавие:*** *Стоянов, Д., Бочев, Л., Радев, Ив., 2021. Подходи за повишаване киберсигурността при управлението на енергийната инфраструктура. Шумен: Сборник научни трудове на Международната научна конференция „Отбранителни технологии“ DefTech 2021, Факултет "Артилерия, ПВО и КИС")*.

Dixon, R., (1976). Spread spectrum systems. New York, London, Sydney, Toronto: John Wiley & Sons

Tsankov, Ts., (2018). Nonlinear function applications for information security in communication systems. Shumen: Bishop Konastantin Preslavsky university publishing house (***Оригинално заглавие:*** *Цанков, Цв., 2018. Приложения на нелинейните функции за защита на информацията в комуникационните системи. Шумен: Университетско издателство „Епископ Константин Преславски“, ISBN 978-619-201-212-0)*.