TRENDS IN THE DEVELOPMENT OF COMMUNICATION SYSTEMS, EXPLOITING ELECTRICAL POWER LINES

Dobry S. Stoyanov, Lyuboslav M. Bochev, Dimitar St. Dimov

Communication Networks and Systems Department, Artillery, Air Defense Communication and Information Systems Faculty, National Military University „V. Levski", Shumen, Bulgaria
dobri_stoyanov@mail.bg, luboslavbochev@abv.bg, dimcata99@abv.bg

ТЕНДЕНЦИИ В РАЗВИТИЕТО НА КОМУНИКАЦИОННИТЕ СИСТЕМИ, ИЗПОЛЗВАЩИ ЕЛЕКТРОЕНЕРГЕТИЧЕСКИ ЛИНИИ

Добри С. Стоянов, Любослав М. Бочев, Димитър Ст. Димов

Катедра „Комуникационни мрежи и системи", факултет „Артилерия, противовъздушна отбрана, комуникационни и информационни системи", гр. Шумен, България
dobri_stoyanov@mail.bg, luboslavbochev@abv.bg, dimcata99@abv.bg

***Abstract**: Today the providing of high resistance of electro-energy systems' management to different cyberattacks is a very important engineer problem. It could be solved by enhancement of independent communication channels, exploited for transmission of sensor and managing information. Accounting this situation, in the paper the trends in the development of communication systems, exploiting electrical power lines are analyzed. On this base the approaches for applying of these systems for improvement of the cyberresistence of electro-energy systems' management are systematized.*

***Keywords**: cybersecurity, smart grids, power line communication*

I. Увод

Още с появата на електроенергетическите мрежи възниква проблемът за предаване на команди и различна служебна информация от един техен елемент (възел) към друг. Прокарването паралелно на електроенергетическите линии (ЕЕЛ) на специални телефонни и телеграфни линии, които да се използват за тези цели, се е считало за нерационално. По тази причина още в началото на двадесети века в мрежите за постоянен ток в САЩ телеграфни сигнали се предавали непосредствено по проводниците на ЕЕЛ. По-късно, с развитието на средствата за радиовръзка, подобна технология започнала да се използва и в мрежите за променлив ток [1].

Постепенно предаването на различна служебна информация по проводниците на ЕЕЛ се превръща в един от основните видове връзка (комуникация). При нея приемо-предавателната апаратура се включва към ЕЕЛ чрез електрически филтри с различна конструкция. Подобни системи

позволяват предаването както на гласова информация и телеметрични данни, така и на команди за телеуправление [1].

Интересът към комуникационните системи, използващи ЕЕЛ, през последното десетилетие се засили тъй като в икономически водещите страни в света се развива технологията Smart Grid (интелектуална мрежа). При нея се използват „умни електромери", „умни асансьори", „умни домове", слънчева и вятърна енергия, което дава съществени ползи на потребителя при заплащането на услугите на енергетическите дружества. Електроснабдяващите фирми, на свой ред, получават положителен ефект благодарение изглаждането на графика на максимално натоварване и намаляване загубите на електроенергия [2].

Водеща роля при модернизацията на електроенергетиката на нови принципи има електрическата мрежа, тъй като тя е структурата, осигуряваща надеждна връзка между генериращите инсталации и потребителите. Най-новите технологии, използвани в мрежите, адаптацията на характеристиките на оборудването към режимната ситуация, активното взаимодействие с генериращите инсталации и потребителите, позволяват създаването на ефективно функционираща система, в която се вграждат съвременните информационно-диагностични подсистеми, както и подсистемите за автоматизация управлението на всички елементи, включени в процесите на производство, предаване, разпределение и потребление на електроенергия [2].

В резултат се създава така наречената Интелектуална електроенергетическа система с активно-адаптивна мрежа (ИЕС ААМ), означаваща система, в която всички субекти на електроенергетическия пазар (генериращи инсталации, мрежи, потребители) вземат активно участие в процесите на предаване и разпределение на електроенергията.

Реализацията на идеологията ИЕС ААМ е насочена към достигане на качествено ново ниво на ефективност на функционирането и развитието собствено на електрическите мрежи, както и към повишение системната надеждност и пропускателна способност, подобряване качеството и надеждността на електроснабдяване на потребителите. Практическото въплъщение на идеологията на ИЕС ААМ обаче критично зависи от успешното решаване на проблема за осигуряване на висока киберсигурност при управлението на елементите на енергийната инфраструктура. В [3] са анализирани общите подходи за повишаване киберсигурността при управлението на елементите на енергийната инфраструктура. В резултат е обоснован изводът, че за тази цел могат да се използват поотделно или комбинирано следните два подхода:

П 1) увеличаване на броя N_{ch} на независимите канали за връзка, по които се предават командите при управлението на елементите на енергийната инфраструктура;

П 2) намаляване на вероятността p за успешно имитиране на вредоносната команда в един канал за връзка.

Предвид на този извод задачите на настоящия доклад са:

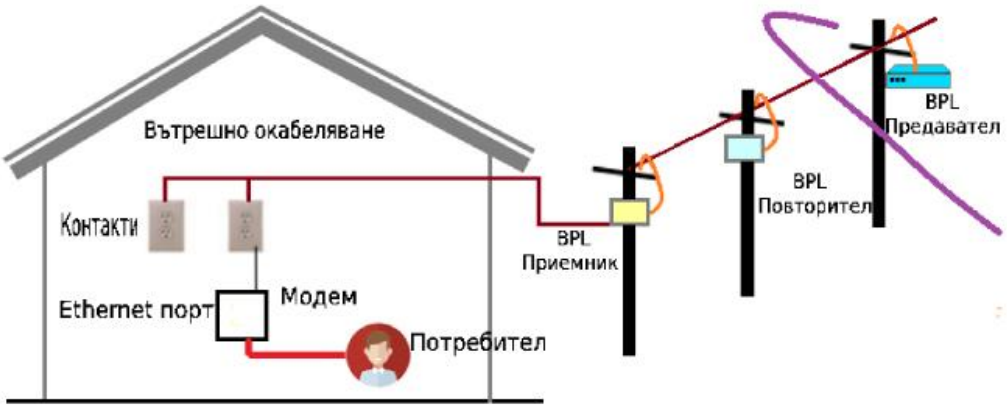
1) да се направи анализ на тенденциите в развитието на комуникационните системи, използващи електроенергетически линии;

2) да се систематизират подходите за повишаване киберсигурността при управлението на елементите на енергийната инфраструктура, базиращи се на комуникационни системи, използващи електроенергетически линии.

Тези задачи се решават в следващите два раздела на доклада.

II. Анализ на тенденциите в развитието на комуникационните системи, използващи електроенергетически линии

Общият вид на комуникационна система [4], използваща електроенергетически линии, е показан на фиг. 1.



Фиг. 1: *Общ вид на комуникационни системи, използващи електроенергетически линии*

От фиг. 1 се вижда, че *комуникационните системи, използващи електроенергетически линии* (КСИЕЛ, *Power Line Communications* - PLC), могат да се разделят на два основни структурни класа (СК) в зависимост от функциите и конструкциите на ЕЕЛ:

СК 1) комуникационни системи, използващи електроенергетически линии в дома, офиса, публична сграда и т.н.;

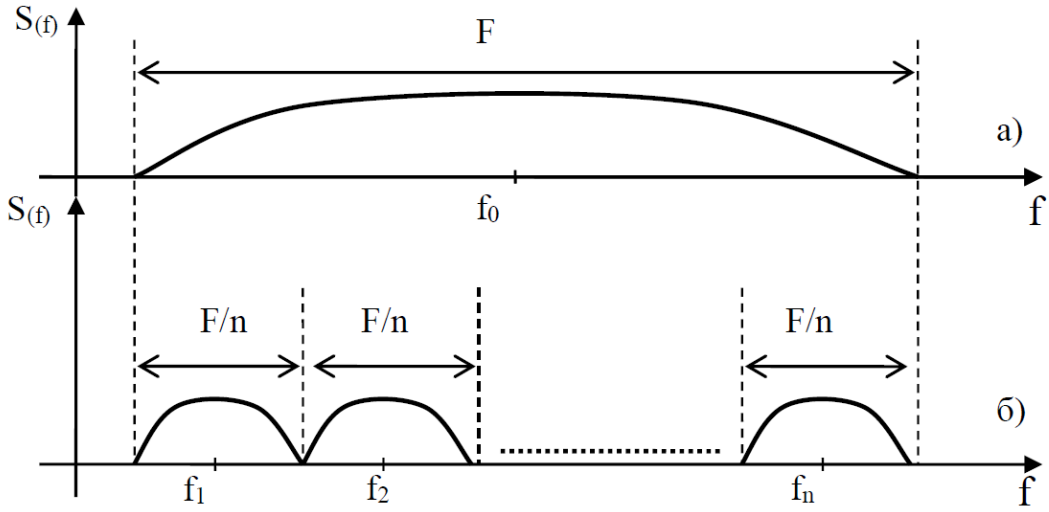
СК 2) комуникационни системи, използващи електроенергетически линии за пренос на електрическа енергия от генериращите инсталации до потребителите.

За първия клас (СК 1) КСИЕЛ са характерни следните особености. Първо, напрежението по електроенергетическите линии в дома, офиса е с ефективна стойност $220\,[V]$ или по-малка (например $110\ V$, $36\ V$, $24\,[V]$). Второ, пренасянето на електрическата енергия по принцип не използва трансформатори. Трето, геометричните размери на вътрешното окабеляване е от порядъка на десетки метри, което ограничава обхвата на съответните КСИЕЛ.

В противоположност, за втория клас (СК 2) КСИЕЛ е характерно, че напрежението по електроенергетическите линии за пренос на електрическа енергия от генериращите инсталации до потребителите има много висока ефективна стойност, която е от порядъка на няколко хиляди и дори стотици хиляди волта (например $12\ kV$, $20\ kV$, $110\ kV$, $220\ kV$, $330\ kV$, $400\ kV$ и т.н.). Освен това, пренасянето на електрическата енергия по линиите за средно и високо напрежение по принцип използва трансформатори, които в редица случаи блокират (филтрират) разпространението на радио-сигнали с честота над $500\,[kHz]$. От друга страна обаче, обхватът на КСИЕЛ, използващи линиите със средно и високо напрежение, е от порядъка на десетки и дори стотици километри. В някои случаи в КСИЕЛ от втория клас (СК 2) се използват междинни усилватели, компенсиращи затихването на сигналите при разпространението им.

Друг съществен признак за класификация на КСИЕЛ е методът за използване на електромагнитния спектър. В тази връзка следва специално да се отбележи, че всички използвани в мо-

мента КСИЕЛ [1], [4] прилагат принципа на *честотно разделяне и мултиплексиране* (ЧРМ, *frequency division and multiplexing* – FDM) на комуникационните канали, който за пълнота на изложението в доклада се припомня с помощта на фиг. 2.



Фиг. 2: *Честотно разделяне и мултиплексиране на комуникационните канали*

Както е известно, в комуникационните системи с ЧРМ честотната лента F на комуникационната система (фиг. 2а) се разделя на n канала с ширина F/n (фиг. 2б). При това отделните потребители използват един или няколко канала като спектрите на използваните от тях сигнали трябва да се „побират" в предоставените канали с някакъв „запас", който типично е $0{,}1.\,(F/n)$.

Следва дебело да се подчертае, че честотните ленти на КСИЕЛ са в диапазона

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

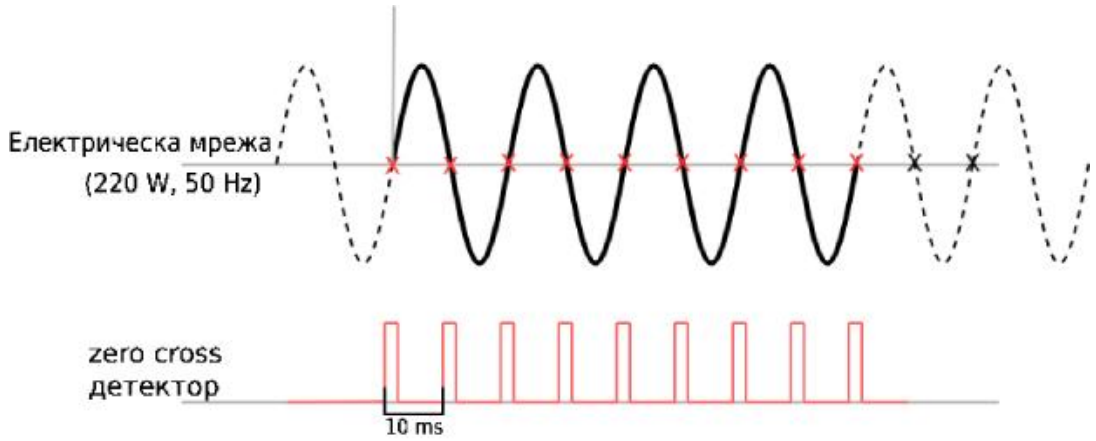
Ограничението (1) на честотните ленти на КСИЕЛ произтича от следните факти. Първо, основният принцип на КСИЕЛ е употребата на вече изградените ЕЕЛ и за пренасяне на информация не трябва да пречи на нормалното функциониране на други комуникационни системи. Второ, електромагнитните вълни с честоти над $500[kHz]$ 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. По-конкретно, през 1922 г. първата КСИЕЛ, използваща амплитудна модулация на някаква носеща честота, започва да пренася телеметрична информация като използва ЕЕЛ с високо напрежение и честотния диапазон $15 \;\; kHz \div 500[kHz]$. Такива КСИЕЛ се експлоатират и до днес. Потребителски продукти, базиращи се на КСИЕЛ, като например за контрол на малки деца (baby alarms), се появяват през 1940 г.

През тридесетте години на миналия век се внедряват КСИЕЛ, използващи ЕЕЛ със средно $(10 \;\; kV \;\div\; 20[kHz])$ и ниско (240/415 [V]) напрежение, както и амплитудна манипулация на носещата честота (ripple carrier signaling). При тези системи се използва някаква ниска носеща честота (често наричана *тон*) в диапазона $100 \;\; Hz \;\div\; 2400[Hz]$ като битовете 1 и 0 се предават чрез бавно включване и изключване на тона. Всеки отделен участък от електроенергетическата мрежа

има свой собствен тон (носеща честота), което практически елиминира електромагнитните смущения между съседните участъци.

След това френската електрическа компания Électricité de France (EDF) конструира прототипи, които са в основата на стандарта IEC 61334 (тяхното действие е въведено в Р. България с БДС EN 61334-5-1:2003), дефиниращи системата "*spread frequency shift keying*" (S-FSK, *честотна манипулация с разлят спектър* - ЧМРС). Работата на КСИЕЛ с ЧМРС [1] ще бъде пояснен с помощта на фиг. 3.



Фиг. 3: *Принцип на работа на КСИЕЛ с ЧМРС*

В КСИЕЛ с ЧМРС пренасянето на информация се извършва само в строго определени времеви прозорци с продължителност от порядъка на $1\,ms$, разположени в моментите, когато напрежението в ЕЕЛ става почти $0\,[V]$. Чрез този подход се минимизира влиянието на широколентовите шумове, създавани от искрането на електрическите съединения, което е най-интензивно при максимумите на напрежението в ЕЕЛ.

Началото на всеки прозорец се задава от специално електронно устройство, наречено *zero cross detector* (*детектор на пресичането на нулата*). След като се отчете фактът, че честотата на напрежението в ЕЕЛ е $50\,[Hz]$, се вижда, че количеството на времевите прозорци за $1\,s$ е 100, а периодът на следването им е $10\,ms$.

Съгласно стандарта, във всеки времеви прозорец се предават серийно 1, 2, 4 или 8 бита. Всеки бит физически се пренася от две различни носещи честоти (два различни тона) като единият тон означава 1, а другият тон – 0. В стандарта не са дефинирани точни честоти на тоновете, но те обикновено са в диапазона $20\ \ kHz\ \div\ 100[kHz]$ и трябва да бъдат разделени със защитен интервал от поне $10\ \ kHz$. Освен това, най-старшите битове се изпращат първи за разлика от обикновените серийни портове. В приемника отношението *сигнал-шум* (С/Ш) се подобрява като се измерва или само мощността на тона, означаващ 1, или само мощността на тона, означаващ 0, или само разликата в мощностите на двата тона. След това приетите битове 1 и 0 се групират в байтове от по 8 бита, а байтовете – пакети от по 42 байта. Първите 4 байта във всеки пакет са преамбюл за измерване текущото състояние на канала. Те се следват от 38 байта, които формират едно съобщение. Пакетите се разделят с групи от 3 „празни" байта.

Следва да се отбележи, че всеки отделен участък от електроенергетическата мрежа има свой собствен тон (носеща честота), което практически елиминира електромагнитните смущения

между съседните участъци. При това типичната скорост на предаване на информация в КСИЕЛ с ЧМРС е 200 $[b/s] \div 1200\ [b/s]$.

През седемдесетте години на миналия век електрическата компания Tokyo Electric Power Co провежда експерименти с КСИЕЛ с ЧМРС, които демонстрират устойчива двустранна връзка (пълен дуплекс) между няколко стотици устройства. Днес такива системи широко се използват в Италия и някои други страни от Европейския съюз.

Отвореният протокол за умна мрежа (ОПУМ, *Open Smart Grid Protocol* - OSGP) е един от най-широко прилаганите в момента протоколи за умни измерители (датчици). Днес повече 5 000 000 умни датчици, използващи КСИЕЛ с *бинарна фазова манипулация* на носещата честота (БФМ, *Binary Phase Shift Keying* – BPSK) и OSGP, са инсталирани по целия свят. OSGP алиансът, основан през 2006 г., се стреми към утвърждаване на фамилия спецификации на Европейския институт за телекомуникационни стандарти (ЕИТС, European Telecommunications Standards Institute - ETSI), които заедно със стандарта ISO/IEC 14908 за контрол на мрежите да се използват за управление на процесите в умните мрежи. OSGP е оптимизиран за осигуряване на сигурно и ефективно пренасяне на команди и контролна информация за: умни датчици, модули за директно управление на натоварването, соларни панели, шлюзове и други устройства на умните мрежи. Следва специално да се отбележи, че OSGP следва модерния структурен подход на OSI протокола и има потенциала да посрещне успешно разрастващите се предизвикателства на умните мрежи.

На физическо ниво OSGP използва ETSI 103 908 като свой технологичен стандарт. Поконкретно, носещата честота е 86,232 $[kHz] \pm 200ppm$, а скоростта на предаване на бинарните символи, реализирани чрез БФМ, е 3592.98 $[Bd]$ (т.е. честотата на тактовите импулси е точно $1/24$ от носещата честота).

Комуникационните системи, използващи разпределителните ЕЕЛ (*Distribution Line Carrier* (DLC) Systems), имат носещи честоти в интервала 9 $kHz \div 500[kHz]$ и скорости на предаване на информацията до 576 $[kb/s]$.

В най-съвременните КСИЕЛ се използва *ортогонално честотно разделяне и мултиплексиране* (ОЧРМ, *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 ОЧРМ честотната лента на комуникационната система се разделя на стотици и дори хиляди канали (например $n = 256, 512, 1024, 2048, 4096, 8192$ на фиг. 2б) 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 тази връзка следва да се отбележи, че през 2009 г. беше основан така наречения PRIME (*PoweRline Intelligent Metering Evolution*) алианс, който внедри КСИЕЛ с ОЧРМ и цифрова обработка на сигналите. В тази система честотата на дискретизация е 250 kHz, броят на каналите е $n = 512$, типът на модулацията – *диференциална фазова манипулация* (ДФМ, *differential phase shift keying* – DPSK). Каналите са разположени в честотния диапазон 42 $kHz \div 89\ [kHz]$, максималната скорост на предаване на информацията е 128,6 $[kb/s]$, но максимална шумоустойчивост се постига при скорост на предаване на информацията 21,4 $[kb/s]$.

През 2011 г. няколко компании, включително оператори на разпределителни електроенергетически мрежи (ERDF, Enexis), доставчици на електро-измервателна апаратура (Sagemcom, Landis&Gyr) и на специализирани интегрални схеми (Maxim Integrated, Texas Instruments, STMicroelectronics, Renesas), създадоха така наречения G3-PLC алианс, разпространяващ G3-PLC протокола. Този протокол се прилага за управление на голям брой елементи и подсистеми на умните мрежи. На физическо ниво той може да оперира в Европа в честотните ленти CENELEC A ($35\ kHz \div 91\ kHz$) или CENELEC B ($98\ kHz \div 122\ kHz$), в Япония - в честотната лента ARIB ($155\ kHz \div 403\ kHz$), а в САЩ и останалата част от света – в честотната лента FCC ($155\ kHz \div 487\ kHz$). Предаването на и приемането на сигналите се осъществява с ОЧРМ и цифрова обработка на сигналите като честотата на дискретизация е $400\ kHz$, а фазовата манипулация е адаптивна (т.е. типът на сигналната азбука се избира в съответствие с конкретното интензивност на шумовете в използваната ЕЕЛ). G3-PLC протоколът е проектиран да осигурява изключително устойчива и сигурна комуникация между различни устройства, включително когато по свързващата ги ЕЕЛ има трансформатори за преобразуване на напрежението от средно в ниско. Използвайки IPv6, G3-PLC позволява комуникация между датчици, мрежови превключватели и други елементи на умните мрежи. През декември 2011 г. G3 PLC технологията беше утвърдена официално от *Международния съюз по далекосъобщения* (МСД, *International Telecommunication Union* - ITU) чрез стандарта G.9903 Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks (Тяснолентови ОЧРМ приемо-предаватели за КСИЕЛ в G3-PLC мрежи).

КСИЕЛ, базиращи се на технологията *широколентов достъп чрез ЕЕЛ* (ШДЕЕЛ, *Broadband over power line* - BPL), използват ЕЕЛ между трансформаторите със средно напрежение, както и ЕЕЛ между трансформаторите с ниско напрежение и потребителските електрически контакти (където ефективната стойност на напрежението е $110\ V \div 240\ V$) за канализиране на сигналите. Тези КСИЕЛ позволяват да се избегнат разходите за прокарване на кабели за класически комуникационни системи, за свързване на антени, приемо-предаватели и рутери за безжични мрежи. КСИЕЛ с ШДЕЕЛ използват същите носещи честоти, както и класическите РКС. За намаляване на възможните взаимни смущения, в съвременните КСИЕЛ с ШДЕЕЛ се използват семейства от *дискретно честотни сигнали* (ДЧС). При тези сигнали носещата честота се изменя скокообразно (*frequency-hopping* (FH) signals). Параметрите на сигналите на КСИЕЛ с ШДЕЕЛ се регламентират от стандарта IEEE 1901 (HomePlug).

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 ЕЕЛ (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. 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

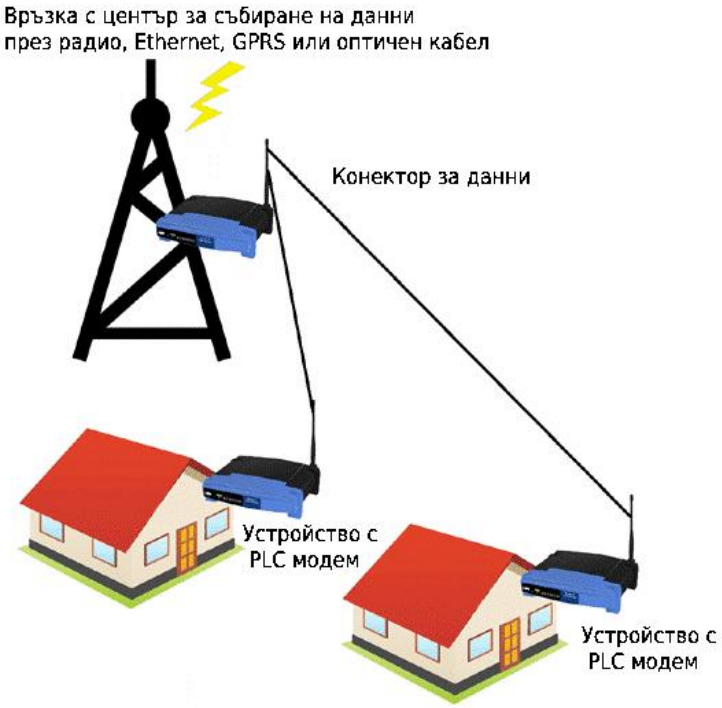
целия честотен диапазон $20\,MHz \div 20\,GHz$, който е много по-широк от диапазон $2\,MHz \div 80\,MHz$, определен за КСИЕЛ с ШДЕЕЛ.

III. Подходи за повишаване киберсигурността при управлението на елементите на енергийната инфраструктура, базиращи се на комуникационни системи, използващи електроенергетически линии

Както беше отбелязано по-горе, в [3] е обоснована възможността да се повиши киберсигурността при управлението на елементите на енергийната инфраструктура чрез увеличаване на броя N_{ch} на независимите канали за връзка, по които се предават командите.

Предвид на анализа, направен в предходния раздел на доклада, тази възможност може да се реализира на базата на КСИЕЛ чрез следните подходи.

П 1) Изграждане на КСИЕЛ с 3 ЕЕЛ (фиг. 4). Действително, по принцип електроенергетическите мрежи са трифазни и се състоят от 3 ЕЕЛ – по една ЕЕЛ за всяка от фазите. В резултат количеството на независимите канали за връзка, по които се предават командите управление на елементите на енергийната инфраструктура, се увеличава 3 пъти.



Фиг. 4: *КСИЕЛ с 3 ЕЕЛ*

П 2) Създаване в КСИЕЛ на много голямо количество логически канали с помощта на сложни дискретни сигнали с голяма база. По-конкретно, шумоподобната вътрешно-импулсна структура на сложни дискретни сигнали с голяма база позволява в честотната лента на КСИЕЛ да се предават и приемат едновременно цели семейства от такива сигнали практически без да се създават взаимни електромагнитни смущения (*multi access interferences* - MAIs) [5], [6], [7], [8].

IV. ЗАКЛЮЧЕНИЕ

В доклада са анализирани тенденциите в развитието на комуникационните системи, използващи електроенергетически линии. На тази основа са систематизирани подходите за повишаване киберсигурността при управлението на елементите на енергийната инфраструктура, базиращи се на комуникационни системи, използващи електроенергетически линии. Обоснованите изводи могат да бъдат полезни при внедряването и развитието на интелектуални електроенергетически системи в Република България.

References

[1] “Связь через ЛЭП” (2021), достъпна на https://ru.wikipedia.org/wiki/Связь_по_ЛЭП

[2] Erol-Kantarci, M., (2021), “Smart Grid? Yes, AI Says: Bring It on!,” IEEE CTN Issue: April 2021

[3] Стоянов, Д., Бочев, Л., Радев, Ив., (2021), „Подходи за повишаване киберсигурността при управлението на енергийната инфраструктура“, Proceedings of International Scientific Conference “Defense Technologies” DefTech 2021, Faculty of Artillery, Air Defense and Communication and Information Systems (под печат)

[4] Pandit, A., (2019), “What is Power Line Communication (PLC) and How it works,” достъпна на https://circuitdigest.com/article/what-is-power-line-communication-plc-and-how-does-it-work

[5] Iliev, M., Bedzhev, B., Bedzheva, M., and Kanchev, K., (2019), “A Survey of Periodic Binary Nearly Perfect Signals with Lengths N≡1mod4”, Proceedings of 16th Conference on Electrical Machines, Drives and Power Systems, ELMA 2019, June 6 – 8, 2019, Varna, Bulgaria

[6] Iliev, M., Bedzheva, M., Kanchev, K., and Bedzhev, B. (2019), “A Survey of Periodic Binary Nearly Perfect Signals with Lengths N≡3mod4”, Proceedings of 29th Annual Conference of the European Association for Education in Electrical and Information Engineering – EAEEIE 2019, 4th - 6th September 2019, University of Ruse, Ruse, Bulgaria

[7] Iliev, M., Bedzhev, B., Bedzheva, M., and Yanakiev, P., (2020), “A Method for Synthesis of Nearly Ideal Phase Manipulated Signals”, Proceedings of the 2020 IEEE International Conference on Information Technologies (InfoTech-2020), 17-18 September 2020, St. St. Constantine and Elena, Bulgaria

[8] Tasheva, Zh., Bogdanov, R., (2018), “A relationship between cognitive information processing in learning theory and machine learning techniques in cognitive radios,” https://www.researchgate.net/publication/325368819

БЛАГОДАРНОСТИ

Този доклад е резултат от работата по проект „Анализ и приложения на методите за оценка натовареността на електромагнитния спектър”, финансиран от Национален Военен Университет – Велико Търново, Факултет „Артилерия, ПВО и КИС”.