APPROACHES FOR CYBERSECURITY ENHANCEMENT OF THE ENERGY INFRASTRUCTURE MANAGEMENT

Dobry S. Stoyanov, Lyuboslav M. Bochev, Ivan Y. RadeV

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, secterity@abv.bg

ПОДХОДИ ЗА ПОВИШАВАНЕ КИБЕРСИГУРНОСТТА ПРИ УПРАВЛЕНИЕТО НА ЕНЕРГИЙНАТА ИНФРАСТРУКТУРА

Добри С. Стоянов, Любослав М. Бочев, Иван Й. Радев

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

***Abstract**: Today the providing of high sustainability of electro-energy feeding systems in different condition is a very significant engineer problem, which comprises large number of specific areas of research. Accounting this situation, in the paper the general approaches for cybersecurity enhancement of the energy infrastructure management are analyzed. The substantiated conclusions could be useful in the development of the new smart grids.*

***Keywords**: cybersecurity, smart grids*

I. Увод

В последното десетилетие в икономически водещите страни в света се развива технологията *Smart Grid* (*интелектуална мрежа*). Съществуват десетки пилотни проекти, в които използването на „умни електромери", „умни асансьори", „умни домове", слънчева и вятърна енергия 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 [1].

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 функциониращa 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 [2].

В състава на ИЕС електрическата мрежа от пасивен компонент за транспорт и разпределение на електроенергия се превръща в активен елемент, чиито параметри и характеристики се изменят в реално време в зависимост от режимите на работа на енергосистемата.

За реализацията на тази нова функция електрическите мрежи се екипират със съвременни бързодействащи устройства на силовата електроника и електромашинни вентилни системи, системи, осигуряващи получаването на своевременна (on-line) информация за режимите на работа на мрежата и състоянието на оборудването. В електрическите мрежи и потребителите широко се използват различни типове акумулатори и генератори на електрическа енергия, в резултат на което потребителите получават възможност да станат активни участници в процеса на разпределение и потребление на електроенергията [1].

ИЕС ААМ се оборудват и със съвременни системи за автоматизация управлението на нормалните и аварийните режими на работа, използващи мощни компютърни средства и единна комуникационна мрежа за управление и оценка на текущите стойности на работните параметри.

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. Предвид на този факт задачите на настоящия доклад са:

1) да се даде систематизирано описание на компонентите на интелектуалните електрически мрежи;

2) да се обосноват общи подходи за повишаване киберсигурността при управлението на елементите на енергийната инфраструктура.

Тези две задачи се решават последователно в следващите два раздела от доклада.

II. Компоненти на интелектуалните електрически мрежи

Интелектуалната електроенергетическа система с активно-адаптивна мрежа (ИЕС ААМ) представлява електроенергетическа система от ново поколение, основана на мултиагентен принцип на организация и управление на нейното функциониране и развитие с цел ефективно използване на всички ресурси (природни, социално-производствени и човешки) за надеждно, качествено и ефективно енергоснабдяване на потребителите чрез гъвкаво взаимодействие на всички нейни субекти (всички видове генериращи инсталации, електрически мрежи и потребители) на основата на съвременни технологически средства и единна интелектуална йерархическа система за управление.

В ИЕС ААМ важна роля е отредена на активно-адаптивната електрическа мрежа, която е технологическата инфраструктура на електроенергетиката, придаваща принципно нови свойства на интелектуалната енергосистема.

Активно-адаптивната мрежа представлява съвкупност от следните компоненти на електрическите мрежи и системите за управлението им, съединяващи генериращите източници и потребителите енергии:

- линии за пренасяне на електрическа енергия с управляемо изменение на характеристиките (активни и реактивни съставящи на съпротивленията), както и системи за контрол на състоянието им (състояние на подпорните стълбове, заледяване, системи за защита от мълнии и свръхнапрежения и др).;

- устройства за електромагнитно преобразуване на електроенергията с широки възможности за регулиране на параметрите (големина и фаза на напрежението, активна и реактивна мощности, преобразувания на променлив в постоянен ток и обратно, и др.), а също и средства за акумулиране (натрупване) на енергия;

- комутационни апарати с висока отключваща способност и голям комутационен ресурс;

- изпълнителни механизми, позволяващи в реално време да се въздейства на активните елементи на мрежата, изменяйки нейните параметри и топологията (конфигурацията и съпротивлението);

- датчици на положението и текущите режимни параметри в количество, достатъчно за осигуряване оценка състоянието на мрежата в нормални, аварийни и следаварийни режими на работа на енергосистемата, с висока скорост на отчитане на показанията в цифров вид;

- съвременни цифрови устройства за защита и автоматика;

- информационно-технологически и управляващи системи, включително програмно осигуряване и технически средства за адаптивно управление с възможност за въздействие в реално време на активните елементи на мрежата и електрическите уреди/устройства на потребителите;

- бързодействаща многостепенна управляваща система със съответния информационен обмен при анализа и адаптацията на състоянието системата като цяло, както и на нейните части и елементи с различни времеви цикли за различните нива на управление.

Широкото внедряване на съвременни информационни технологии в енергетическата сфера обаче води до повишаване на риска от възникване на загуби (технически и икономически) от противоправни действия. Следва да се отбележи, че киберсигурността на енергетическия отрасъл към настоящия момент се оценява като твърде ниска и потенциално опасна (в световната практика са отбелязани голям брой аварии, предизвикани от кибератаки). Ето защо осигуряването на кибербезопасност на ИЕС ААМ е приоритетна задача за целия неин жизнен цикъл.

В процеса на планиране на киберсигурността трябва да бъдат отчетени следните специфични особености на ИЕС ААМ:

СО 1) работа в непрекъснат активен режим;

СО 2) приоритет на задачата за съхраняване функционалността на системата над задачата за съхранение на нейната информационна безопасност.

Концепцията за киберсигурност на ИЕС ААМ трябва да отчита нормите на стандартите, разработени от групата IEC TC57: IEC 61850, IEC60870, IEC 62351, касаещи безопасността на комуникационните протоколи, както и изискванията на стандарта INL Cyber Security Procurement Language 2008, серията стандарти ISO/IEC 27000 и стандарта IEC 62351-8, определящи общите

принципи и съдържанието на политиките за осигуряване безопасност на цифровите системи за управление.

Следва да се отбележи, че адекватната подготовка за справяне с рискове и безпроблемното трансгранично сътрудничество са от съществено значение за предотвратяването или управлението на кризисни ситуации на територията на Европейския съюз (ЕС). Един от наскоро приетите законодателни инструменти за постигането на тези цели е Регламент 2019/941 за готовност за справяне с рискове в електроенергийния сектор. Нормативният документ изисква държавите членки да работят за идентифицирането на всички възможни кризисни сценарии на национално и регионално ниво, които могат да повлияят на енергийните доставки. На база на тези сценарии властите трябва да разработят планове за справяне с рисковете при всеки конкретен случай.

Мерките за повишаване на киберсигурността гарантират, че Европа е добре подготвена за неочаквани кризи, какъвто е случаят с пандемията от COVID-19. Огромното нарушение на нормалния начин на живот вследствие на създалата се ситуация илюстрира зависимостта на обществото от стабилна енергийна система, жизнено важна за осигуряване на енергийните доставки за болниците, индустриалните предприятия, произвеждащи медицинско оборудване, и на хората, принудени да останат в домовете си.

Основните предизвикателства пред киберсигурността в енергийния сектор са следните:

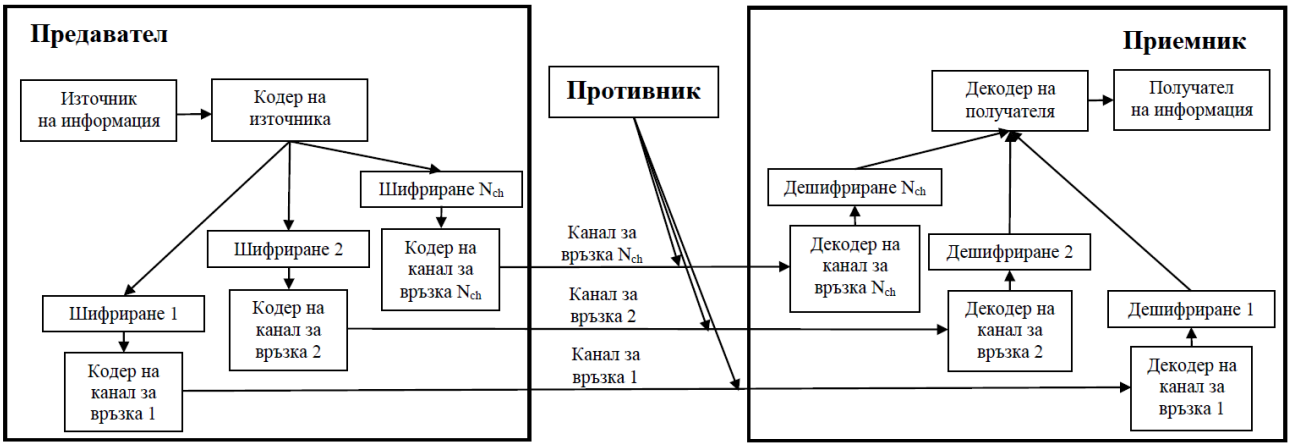
- управление на заплахи и рискове;
- адекватност на кибер-отговора в случай на кибератака;
- непрекъснатото подобряване на кибер устойчивостта;
- изграждането на необходимите капацитети и компетентности.

Системата за киберсигурност на ИЕС ААМ трябва да се реализира като интегрирана информационна технология, обединяваща оптимално следните апаратни, програмни и организационни методи [3]:

- бариерни методи (физическо ограничаване на достъпа, разграничение на правата на потребителите, пароли, роли);
- традиционни средства (антивирусни и защитни стени);
- балансирано използване на открити и класифицирани стандарти за киберсигурност;
- използване на двустранно шифриране с публичен ключ на нивото на комуникационния протокол (транспортно ниво);
- електронни цифрови подписи (ЕЦП) и системи от съответните удостоверяващи центрове;
- експертни средства на основата на активен одит.

III. Подходи за повишаване киберсигурността при управлението на елементите на енергийната инфраструктура

При анализа на компонентите на интелектуалните електроенергетически системи с активно-адаптивна мрежа (ИЕС ААМ) специално беше отбелязано, че те представляват интелектуални йерархически системи за управление. По тази причина киберсигурността на ИЕС ААМ в най-голяма степен зависи от структурата на техните комуникационни подсистеми, осигуряващи информационната свързаност на всички градивни компоненти. Този извод се пояснява на фиг. 1, където е представен модел на комуникационна система, осигуряваща киберсигурност при управлението на елементите на енергийната инфраструктура.



Фиг. 1: *Модел на комуникационна система, функционираща във враждебно радиоелектронно обкръжение*

На фиг. 1 *източникът на информация* е диспечерски пункт, който предава команди за управление режимите на работа на *получателя на информацията*, представляващ автономен елемент на енергийната инфраструктура: генерираща инсталация (система от термични слънчеви колектори, от ветрогенератори, малка водно-електрическа централа (ВЕЦ), помпено-акумулаторна ВЕЦ (ПАВЕЦ)), устройство за електромагнитно преобразуване на електроенергията с възможност за регулиране на параметрите, комутационен апарат, устройство за защита и т.н.

Командите за управление се предават по N_{ch} независими канала за свръзка, които могат да използват различни преносни среди: свободно пространство, кабели, изградени от медни проводници, оптически кабели.

Командите, формирани от източника на информация, се преобразуват както следва. Първо, в кодера на източника, каквито са например микрофон или клавиатура, командата се превръща в цифрово съобщение, което е прието да се нарича *явен текст* (*plain text*). След това, явният текст се шифрира с N_{ch} шифъра, при което се получават N_{ch} *шифро-текста* (*cipher texts*) или *шифрограми*. Накрая, в каналните кодери шифрограмите се преобразуват сигнали, които могат да преминат с минимални енергетични загуби през съответния канал за връзка.

В приемника, обработката на сигналите се извършва в огледално обратен ред на вече описания. По-конкретно, в каналните декодери приетите сигнали се преобразуват в шифрограми. След това, шифрограмите се дешифрират и се получават N_{ch} версии на явния текст. Накрая, в декодера на източника, версиите на явния текст се обработват и крайният резултат се трансформира в нискочестотен електрически сигнал, който активира изпълнителните устройства на автономния елемент на енергийната инфраструктура.

С цел предотвратяване на кибератаки, автономният елемент на енергийната инфраструктура изпълнява всяка нова команда, само ако тя е приета идентично (повтаря се) по N_{exec} или повече канала като:

$$N_{exec} = \frac{N_{ch}+1}{2}. \quad (1)$$

В (1) символът x означава най-малкото цяло число, което е по-голямо или равно на x. Например

$$2{,}5 = 3, \quad 3 = 3. \quad (2)$$

С други думи, автономният елемент на енергийната инфраструктура изпълнява всяка нова команда, само ако тя е приета идентично (повтаря се) по повече от половината свързочни канали. В противен случай, командата се отхвърля и режимът на работа на автономния елемент на енергийната инфраструктура не се променя.

Анализът на публично достъпната информация показва, че в най-обща ситуация кибератаките целят вредоносна промяна на режима на работа на автономните елементи на енергийната инфраструктура като например:

- изключване на термични слънчеви колектори през деня;
- активиране на перките на ветрогенераторите при много силен вятър, при което е възможно физическото им разрушаване;
- установяване в ПАВЕЦ на режим „изпомпване" през нощта и на режим „генериране" през деня и т.н.

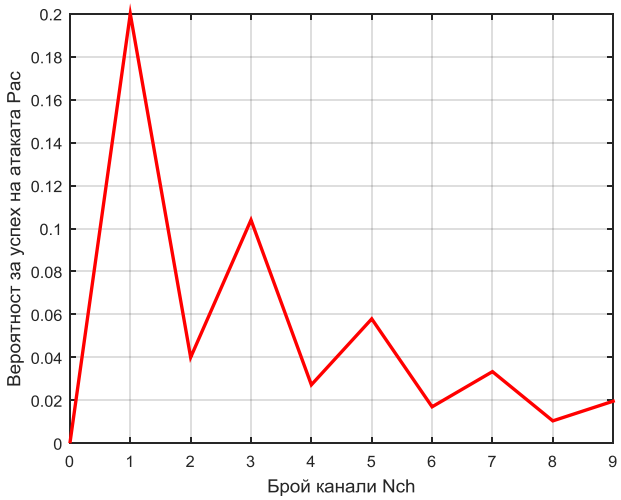
Предвид на изложеното, вероятността за успех на кибератака (P_{ca}), целяща вредоносна промяна на режима на работа на автономен елемент на енергийната инфраструктура, е:

$$P_{ca} = \sum_{i=N_{exec}}^{N_{ch}} C_{N_{ch}}^{i} p^{i} q^{N_{ch}-i} . \quad (3)$$

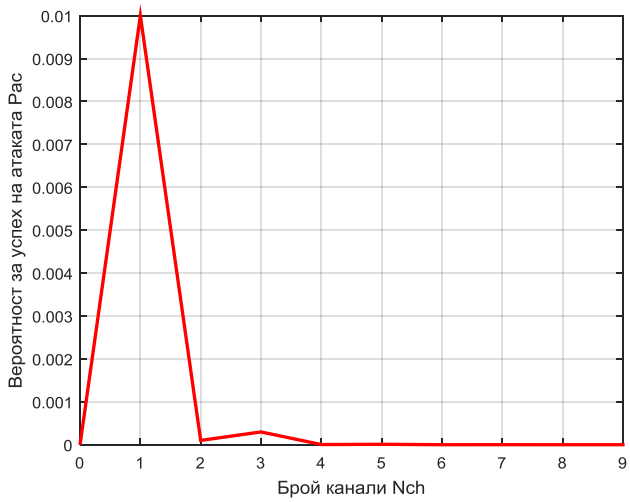
В (3) са използвани следните означения: $p, 0 \leq p \leq 1$ е вероятността за успешно имитиране на вредоносната команда в един канал за връзка, $q = 1 - p, 0 \leq q \leq 1$ е вероятността за неуспешно имитиране на вредоносната команда в един канал за връзка, а $C_{N_{ch}}^{i}$ са комбинациите от N_{ch} елемента от i-ти клас:

$$C_{N_{ch}}^{i} = \frac{N_{ch}!}{N_{ch}-i\ !\times i!} . \quad (4)$$

Резултатите от компютърното моделиране на (3) за различни стойности на параметрите N_{ch} и p са представени на фиг. 2 и фиг. 3.



Фиг. 2: *Вероятност за успех на кибератака, целяща вредоносна промяна на режима на работа на автономен елемент на енергийната инфраструктура,* $p = 0{,}2$



Фиг. 3: *Вероятност за успех на кибератака, целяща вредоносна промяна на режима на работа на автономен елемент на енергийната инфраструктура,* $p = 0{,}01$

От фиг. 2 и фиг. 3 следва изводът, че за повишаване киберсигурността при управлението на елементите на енергийната инфраструктура 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;

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

Първият подход може да се реализира като се използват следните независими канали за връзка:

- радио-канали на мобилни комуникационни системи, специализирани промишлени комуникационни системи и спътникови комуникационни системи;
- каналите на класически кабелни телефонни системи;
- каналите на оптически комуникационни системи;
- канали, използващи проводниците на електроенергетическите системи (*Power Line Communications – PLC*) [4].

Вторият подход може да се реализира чрез използване на:

- съвременни блокови и/или поточни шифри;
- сложни дискретни сигнали с голяма база, чиято шумоподобна вътрешно-импулсна структура много трудно може да бъде разгадана и правдоподобно имитирана [5], [6], [7].

IV. ЗАКЛЮЧЕНИЕ

В доклада са систематизирани подходите за повишаване киберсигурността при управлението на елементите на енергийната инфраструктура. Обоснованите изводи могат да бъдат полезни при внедряването и развитието на интелектуални електроенергетически системи в Република България.

References

[1] "Основные положения концепции интеллектуальной энергосистемы с активно-адаптивной сетью" (2012), достъпна на https://www.fsk-ees.ru/upload/docs/ies_aas.pdf

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

[3] 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

[4] Савова, Ж., Богданов, Р., (2014), „Анонимна система за комуникации в киберпространството, използваща протокол TOR", Сборник научни трудове на научна конференция на Факултет „Артилерия, ПВО и КИС" „Новата парадигма за сигурност в киберпространството", Шумен 2014, стр. 259-265

[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

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".