37. Саветовање CIGRE Србија 2025
СИГУРНОСТ, СТАБИЛНОСТ, ПОУЗДАНОСТ И RESILIENCE ЕЛЕКТРОЕНЕРГЕТСКОГ СИСТЕМА
МУЛТИСЕКТОРСКО ПОВЕЗИВАЊЕ У ЕНЕРГЕТИЦИ И ПРИВРЕДИ
26 - 30. мај 2025, Копаоник

DOI: 10.46793/CIGRE37.D2.08

D2.08

ДИГИТАЛИЗАЦИЈА И ПРОБЛЕМИ САЈБЕР БЕЗБЕДНОСТИ ИНФРАСТРУКТУРЕ ОБНОВЉИВИХ ИЗВОРА ЕНЕРГИЈЕ

DIGITALIZATION AND CYBERSECURITY ISSUES OF RENEWABLE ENERGY SOURCES INFRASTRUCTURE

Славица Боштјанчич Ракас, Валентина Тимченко*

Кратак садржај: Дигитализација представља једну од основних савремених карактеристика развоја инфраструктура обновљивих енергија. Међутим, овај напредак доноси и изазове сајбер безбедности који представљају значајне ризике. Дигитална интеграција система обновљиве енергије, чини системе рањивим на разне сајбер нападе. Како обновљиви извори енергије играју све важнију улогу у глобалним енергетским мрежама, њихов потенцијал као мете за сајбер криминалце расте, са нападима који потенцијално ометају снабдевање енергијом и могу нанети велику штету. Дигитализација инфраструктуре обновљиве енергије довела је до трансформативних технологија као што су ИоТ, Дигитални близанци, Big Data и примена алгоритама машинског учења/вештачке интелигенције, од којих свака игра кључну улогу у побољшању ефикасности и решавању изазова сајбер безбедности. Употреба овог технолошког концепта наглашава двоструки изазов искоришћавања дигитализације за оптимизацију обновљиве енергије уз истовремено решавање ризика сајбер безбедности. Балансирање предности дигитализације са неопходношћу снажне сајбер безбедности представља изазов који је потребно решавати како снажнијим увођењем и применом стандардизације, тако и бољом сарадњом између влада, организација и лидера у индустрији како би се инфраструктура обновљиве енергије обезбедила од сајбер претњи..

Кључне речи: *дигитализација, обновљиви извори енергије, сајбер безбедност, Интернет ствари, стандардизација*

Abstract: Digitalization represents a cornerstone of modern renewable energy infrastructure development. However, cybersecurity challenges have emerged, alongside, posing substantial risks to the integrity of these systems. The digital integration exposes renewable energy infrastructure to various cyberattacks. As renewable energy sources become increasingly central to global energy networks, their attractiveness as targets for cybercriminals grows, with such attacks having the potential to disrupt energy supplies and cause strategic, financial, and societal harm. This digital transformation has also fostered the adoption of cutting-edge

* Славица Боштјанчич Ракас, Институт Михајло Пупин, slavica.bostjancic@pupin.rs
Валентина Тимченко, International Research & Exchanges Board, vtimcenko@irex.org

technologies such as IoT, Digital Twins, Big Data, and the implementation of machine learning and artificial intelligence algorithms, each playing a crucial role in optimizing efficiency and addressing cybersecurity challenges. These advancements underscore the dual imperative of leveraging digitalization to enhance renewable energy systems while simultaneously mitigating cybersecurity risks. Achieving this balance demands stronger adherence to standardization protocols and the proactive collaboration of governments, organizations, and industry leaders to ensure the protection of renewable energy infrastructure against evolving cyber threats..

Key words: *digitalization, renewable energy sources, cyber security, Internet of Things, standardization*

1 УВОД

Дигитализација електроенергетског (ЕЕ) система подразумева интеграцију напредних инфомационо-комуникационих технологија (ИКТ) у све аспекте производње, преноса, дистрибуције и потрошње електричне енергије, па самим тим и у обновљиве изворе енергије, као што су соларна енергија, енергија ветра, хидроенергија и биомаса. Обновљиви извори енергије играју кључну улогу у транзицији ка одрживој енергетској будућности, смањујући негативан утицај на животну средину и подстичући економски развој, а њихове предности су: смањење емисије гасова са ефектом стаклене баште; одрживост – јер се ови извори природно обнављају; смањење зависности од увоза енергената, као и подстицање економског развоја, с обзиром да инвестиције у обновљиве изворе енергије могу створити нова радна места и подстаћи економски раст.

Основне предности дигитализације обновљивих извора енергије су: повећање ефикасности производње и дистрибуције енергије, као и смањење губитака оптимизацијом рада система; побољшање поузданости и стабилности електроенергетског система захваљујући брзој идентификацији и реакцији на проблеме; смањење оперативних трошкова услед аутоматизације и оптимизације; као и одрживи развој и смањење емисија захваљујући бољем управљању ресурсима и интеграцији обновљивих извора енергије.

Основни недостаци обновљивих извора енергије су: (1) променљивост производње, јер одређени обновљиви извори енергије (сунце, ветар) зависе од временских услова, што може довести до варијација у производњи енергије; (2) високи почетни трошкови као и (3) ефикасни системи за складиштење енергије како би се обезбедила стабилност снабдевања енергијом.

Дигитализација обновљивих извора енергије подразумева интеграцију савремених технологија попут рачунарства у облаку, рачунарства у магли, Интернета ствари, *Big Data* аналитике, вештачке интелигенције и машинског учења (за потребе оптимизације рада обновљивих извора енергије; предикције потражње, као и аутоматизације контролних процеса), *Blockchain* технологије, дигиталних близанаца (*Digital Twins*) који представљају виртуелне реплике физичких система, а омогућавају симулацију и анализу рада у реалном времену као и оптимизацију перформанси кроз симулацију различитих сценарија и предикцију исхода.

Основни изазови дигитализације обновљивих извора енергије су повећање ризика од сајбер напада, интероперабилност као и стандардизација. Са дигитализацијом инфраструктуре обновљивих извора енергије, иста све чешће постаје мета сајбер

напада. У раду ће бити представљено шта се под дигитализацијом подразумева, као и пример архитектуре система обновљивих извора енергије засноване на Интернету ствари. Биће описани основни изазови као и потенцијална решења обезбеђивања сајбер безбедности.

2 ДИГИТАЛИЗАЦИЈА ОБНОВЉИВИХ ИЗВОРА ЕНЕРГИЈЕ

Дигитализацијом се унапређују системи обновљивих извора енергије побољшањем ефикасности, поузданости и одрживости. Међутим, суочавање са ризицима сајбер безбедности и обезбеђивање компатибилности и даље представљају кључне изазове. Дигитализација се ослања на низ технологија како би се постигао одговарајући ниво оптимизације рада обновљивих извора енергије, адекватна контрола процеса и обезбеђивање поузданих и прецизних предикција. Међу најчешће коришћеним технологијама налазе се рачунање у облаку (*Cloud Computing*), Интернет ствари (IoT, *Internet of Things*), алгоритми машинског учења (ML, *Machine Learning*) и вештачке интелигенције (AI, *Artificial Intelligence*), блокчејн (*Blockchain*), дигитални близанци (*Digital Twins*), итд [1].

Примена напредних ИКТ технологија трансформише ову индустрију на различите начине [2]. **Рачунарство у облаку** омогућава ЕЕ компанијама удаљени приступ као и удаљени надзор и управљење системима ОИЕ (обновљиви извори енергије), што повећава флексибилност као и брзе реакције на промене у захтевима за потрошњу или производњу електричне енергије. Поред тога, технологија рачунарства у облаку омогућава праћење производње електричне енергије из уређаја за прикупљање енергије, управљање уређајима за конверзију енергије и системима за складиштење електричне енергије. Такође, системи за надзор и управљање који су засновани на облаку омогућавају прикупљање, чување и анализу велике количине података у циљу увида у перфомансе система и идентификовање потенцијалних мера за унапређење система. Прикупљени подаци могу да утичу и на оптимизацију перформанси (дефинисање угла постављања соларних панела, брзине ветротурбине, као и балансирање тока електричне енергије у циљу максималне ефикасности).

Примена **машинског учења/вештачке интелигенције (ML/AI)** подразумева развој алгоритама и рачунарских програма који се у енергетском сектору, односе на предиктивно одржавање, интеграцију обновљивих извора енергије, предвиђање и оптимизацију потрошње енергије, као и управљање енергетском мрежом.

Блокчејн представља систем дељених и дистрибуираних структура података (блокова), који омогућава безбедно чување дигиталних трансакција без потребе за централним ауторитетом. Овом технологијом се обезбеђују транспарентност и безбедност, јер подаци не могу да се мењају без сагласности свих учесника у мрежи. У енергетском сектору, блокчејн се најчешће примењује за евиденцију порекла енергије (сертификати о пореклу енергије); за трговину енергијом (грађани који имају соларне панеле, могу директно продавати вишак електричне енергије својим комшијама), децентрализовано управљање микромрежама (производњом, складиштењем и потрошњом енергије, транспарентно и аутоматизовано). Предности блокчејна су већа транспарентност у производњи и трговини енергијом, смањење трошкова посредника, повећање поверења у извор енергије, подстицај децентрализацији енергетских система.

Интернет ствари (IoT) представља повезивање различитих физичких уређаја, као што су сензори, бројила, соларни панели, батерије и паметни уређаји на Интернету, а могу

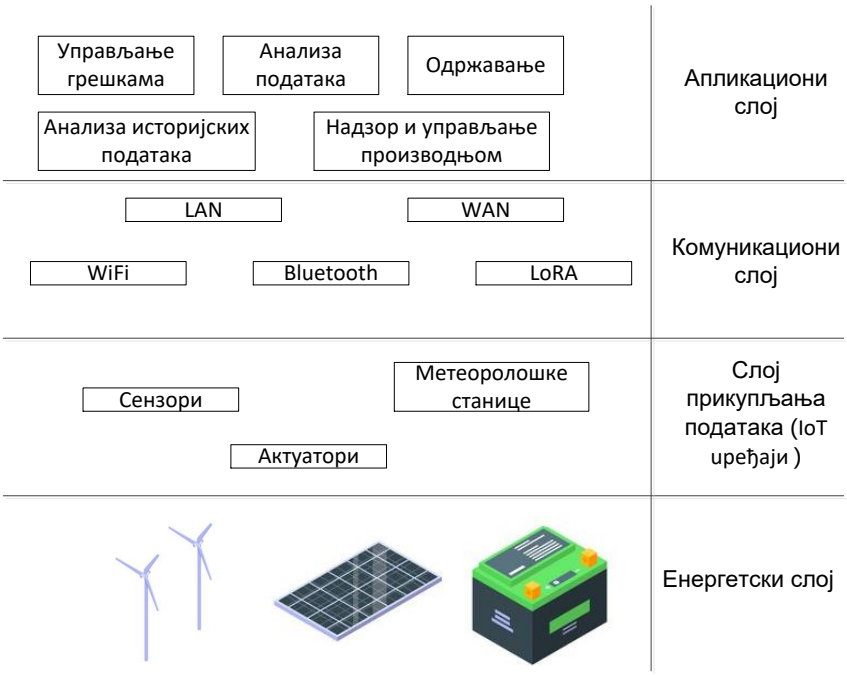
да прикупљају, шаљу и примају податке. Када су у питању ОИЕ, IoT омогућава ефикаснији рад и брзу дијагностику, оптимизацију потрошње енергије, интеграцију различитих извора енергије (на пример, ако у једном тренутку нема сунца, систем може аутоматски прећи на ветар или батерију), паметно складиштење енергије, итд. Предности примене IoT у обновљивим изворима енергије су повећана ефикасност система, смањење губитака у енергији, аутоматизација управљања, боља предвидивост и планирање, мањи трошкови.

Big Data представља огромне количине података које се прикупљају у реалном времену из различитих извора, као и њихову обраду, анализу и коришћење заједно са применом алгоритама машинског учења и вештачке интелигенције, у циљу доношења паметнијих одлука. Примена ове технологије у обновљивим изворима енергије се пре свега односи на прогнозирање производње енергије; оптимизација рада електрана, предиктивно одржавање, анализу потрошње и понашање корисника, итд. Предности примене *Big Data* у енергетици су боље прогнозе и планирање, већа поузданост и сигурност система, уштеда енергије и трошкова, аутоматизација и брже доношење одлука,као и увид у понашање потрошача.

Дигитални близанац представља виртуелну реплику стварног физичког система, која на основу података из стварног (преко IoT сензора, мерења, софтвера) омогућава симулацију, анализу и оптимизацију система у реалном времену. Савремена архитектура дигиталног близанца користи се за постизање високе поузданости, расположивости и одрживости у оквиру комплексног енергетског сектора, уз смањене трошкове. Примена концепта дигиталног близанца у обновљивим изворима енергије се односи на моделовање соларних или ветроелектрана, оптимизацију производње, интеграцију више извора у један систем, тестирање без ризика, итд. Предности примене дигиталних близанаца су прецизније управљање производњом, предиктивно одржавање (мањи број кварова и застоја), смањење трошкова одржавања и експлоатације, већа ефикасност и поузданост система, уз могућност тестирања без ризика.

2.1 *Комуникациона архитектура система обновљивих извора енергије заснованог на Интернету ствари*

Пример IoT-базиране архитектуре система ОИЕ приказан је на слици 1 [3], [4]. Најнижи односно **енергетски слој** обухвата производњу и потрошњу електричне енергије у домаћинствима. Извор електричне енергије могу бити различити обновљиви извори (енергија ветра, сунца) као и конвенционални извори (дизел генератори) и системи за складиштење енергије (батерије). Потрошачи су расподељени у три главне категорије: стамбене, комерцијалне и индустријске потрошаче. **Слој прикупљања података** обухвата различите IoT уређаје, попут сензора, актуатора и мерних уређаја, који су повезани са енергетским слојем и прикупљају различите податке који се преносе до апликационог слоја преко **мрежног (комуникационог) слоја**. На основу података из различитих извора енергије као што су ветроелектране, фотонапонски системи, дизел генератори и батеријски системи, систем управљања ОИЕ (контролни центар) може радити у изолованом режиму или у режиму повезаном на електромрежу. Пренос података се може остварити путем локалне рачунарске мреже (LAN, *Local Area Network*) као и регионалне рачунарске мрежу (WAN, *Wide Area Network*). Комуникациона веза може да буде реализовано жично (PLC, Ethernet, оптичка влакна итд.) и бежично (Wi-Fi, ZigBee, WiMAX, LoRa, мобилне мреже итд.). Подаци се чувају у контролном центру за различите услуге као што су управљање грешкама, одржавање, анализа података, итд (**апликациони слој**).



Слика 1. IoT-базирана комуникациона архитектира система ОИЕ [3], [4]

3 ИЗАЗОВИ ДИГИТАЛИЗАЦИЈЕ ОБНОВЉИВИХ ИЗВОРА ЕНЕРГИЈЕ

Обновљиви извори енергије (ОИЕ) у великој мери зависе од међусобно повезаних дигиталних система за надзор, контролу и складиштење. Иако ова дигитална побољшања унапређују ефикасност и стабилност мреже, она такође уводе рањивости које сајбер нападачи могу да искористе. Један компромитовани систем може имати каскадне ефекте, утичући на производњу, складиштење и дистрибуцију енергије [5]. Како сектор обновљиве енергије наставља да расте, обезбеђивање сајбер безбедности од суштинског је значаја за одржавање безбедне и отпорне инфраструктуре на нападе.

Системи као што су ветротурбине, фотонапонски панели и паметне мреже постају све сложенији и међусобно повезани. Истовремено, примена стандардизованих безбедносних стратегија за заштиту специфичних инфраструктура постаје све сложенија, што усложњава примену безбедносних стратегија у оваквим системима.

Дигитализација повећава ефикасност у производњи и дистрибуцији електричне енергије и смањује трошкове. Искуство показује да то има благотворан утицај на поузданост и стабилност система, захваљујући брзој идентификацији и решавању проблема. Имплементацијом аутоматизације она додатно доноси одређена смањења оперативних трошкова, емисија и повољно утиче на одрживи развој. Изазов лежи у правилној примени мера безбедности и приватности и одржавању инфраструктуре, комуникације и података безбедним за правилну употребу.

Основни изазови обезбеђивања сајбер безбедности дигитализованог система ОИЕ су [6]:

Сложеност и међуповезаност. Данашњи енергетски системи представљају сложену мрежу која обједињује физичку инфраструктуру и дигиталне технологије. Обухватају велике територије и укључују електране, преносне системе и контролне механизме, ослањајући се на комуникационе мреже за брзу размену података и управљање. Међутим, оваква повезаност чини системе рањивим на сајбер нападе – сваки сензор, софтвер или комуникациони канал може бити потенцијална тачка уласка за нападаче.

Недоследни безбедносни протоколи. Енергетски системи често користе опрему и технологије различитих произвођача, што доводи до различитих безбедносних мера и протокола. Такве разлике могу довести до неусклађености – на пример, соларни систем и ветропарк могу користити различите начине заштите, што отежава уочавање и отклањање безбедносних слабости. Те недоследности повећавају ризик од сајбер напада. Стандардизација безбедносних протокола је неопходна за поуздану заштиту енергетске инфраструктуре.

Недостатак стандардизације. Један од главних проблема код обновљивих извора енергије је недостатак стандардизације у области сајбер безбедности, што умањује ефикасност заштите у енергетским мрежама и отежава интеграцију нових технологија, као што је повезивање паметних мрежа са традиционалним системима. Стари системи нису прилагођени модерним решењима попут рачунарства у облаку и IoT-а. Иако напредне ИКТ технологије унапређују оптимизацију, истовремено повећавају безбедносне ризике приликом интеграције старих и нових система.

Рад у реалном времену. Савремени енергетски системи у великој мери зависе од обраде података у реалном времену како би одржали баланс између производње и потрошње енергије. Ово је нарочито важно у условима повећане потражње или при коришћењу променљивих ОИЕ. Међутим, та зависност од брзе анализе података отвара простор за сајбер нападе који могу нарушити рад система. Уколико дође до нарушавања или манипулације подацима, може доћи до погрешног управљања енергијом, што може изазвати неефикасну дистрибуцију, нестабилност у мрежи, па чак и нестанак електриче енергије.

Преклапање физичке и сајбер безбедности. У одрживим енергетским системима физичка и сајбер безбедност су тесно повезане и међусобно зависне. Физички приступ може довести до дигиталних угрожавања, док сајбер напади могу угрозити инфраструктуру. Зато је неопходан јединствен приступ који обухвата оба аспекта ради потпуне заштите система.

Децентрализована структура. Децентрализована природа обновљивих извора енергије представља једну од њихових кључних одлика, јер се састоје од великог броја географски дислоцираних јединица. То значајно отежава примену безбедносних мера, с обзиром да није могуће централизовано управљање безбедношћу, што у великој мери повећава сложеност заштите. Свака појединачна јединица може бити мета сајбер напада, а разлике у приступу корисника и коришћење различитих безбедносних решења без јасних политика додатно повећавају ризик од рањивости и неусклађености.

Технолошка сложеност и нове сајбер претње. Иако увођење напредних ИКТ технологија у системе обновљивих извора енергије доприносе већој ефикасности и аутоматизацији, истовремено повећавају и простор за сајбер нападе. Велики број повезаних уређаја, често са слабим безбедносним мерама, чини IoT уређаје лаким метама. Посебно су рањиви када су повезани са кључним системима као што су системи за надзор и управљање (SCADA). Сајбер напади попут оног на компанију Deutsche Windtechnik 2022. године, када је изгубљена контрола над скоро 2.000 ветротурбина на више од једног дана, показују колико је неопходно хитно унапређење и редовно ажурирање безбедносних мера. [7]

Недостатак сарадње између актера у енергетском сектору. Једна од главних препрека за развој ефикасних стратегија сајбер безбедности у енергетици је слаба сарадња између различитих актера, пре свега између ЕЕ компанија и провајдера услуга сајбер безбедности. Управо је та сарадња кључна за развој свеобухватних безбедносних

решења, као што су јединствени стандарди и протоколи, примена специфичних оквира и метода евалуације ризика од сајбер напада, а који су прилагођени сложености паметних мрежа и повезаних енергетских система.

4 САЈБЕР НАПАДИ

Број сајбер напада на системе обновљивих извора енергије значајно је порастао у последњој деценији, што је последица управо све веће дигитализације и повезивања енергетских система, што их чини подложнијим нападима. Према извештају организације Eurelectric, број успешних сајбер напада на енергетску инфраструктуру у Европи удвостручио се између 2020. и 2022. године, са 48 успешних напада само у 2022. години [8]. 2022. године немачка компанија за одржавање ветропаркова (Deutsche Windtechnik) била је мета сајбер напада који је довео до губитка контроле над скоро 2000 ветротурбина на више од једног дана.

Неки од најчешћих напада у систему ОИЕ обухватају убацивање злонамерних података, нападе репродукције (*replay attacks*), ускраћивање услуге (DoS) и нападе бруталном силом на акредитиве (*brute force*). Проблем се не решава идентификацијом најопаснијих претњи, већ је неопходна примена корака за отклањање рањивости као што су небезбедни комуникациони протоколи, слабе технике енкрипције, недостатак или погрешно успостављена контрола приступа, недостатак или злоупотреба енкрипције, ауторизације и аутентикације [9].

Озбиљан проблем у енергетском сектору постају и *ransomware* напади односно хакерски напади којима се шифрују подаци жртве и захтева финансијска накнада у замену за кључ за дешифровање. У области обновљивих извора енергије, последице ових напада могу бити веома озбиљне. Напад на контролне системе ветроелектрана или соларних електрана може проузроковати нестанак електричне енергије, оштећење опреме и значајне финансијске губитке. Поред тога, опоравак од *ransomware* напада може бити дуготрајан и скуп, јер често захтева враћање система из резервних копија или плаћање откупнине, што не гарантује увек повратак података. Један од водећих произвођача ветротурбина (Nordex) претрпео је ову врсту напада који је утицао на њихове IT системе и операције. Такође, и норвешка компанија за производњу алуминијума и обновљиве енергије (Norsk Hydro) претрпела је 2019. године сличан напад који је утицао на више од 3.000 сервера и хиљаде рачунара, што је довело до значајних оперативних поремећаја [10].

5 СТРАТЕГИЈЕ УНАПРЕЂЕЊА САЈБЕР БЕЗБЕДНОСТИ

Због све већег броја напада, као и у циљу заштите система и обезбеђивања стабилности и безбедност података и инфраструктуре, у наставку су наведени одређени механизми који доприносе унапређењу сајбер безбедности ОИЕ [11], [12].

Строга контрола приступа је неопходна како би се спречио неовлашћен приступ систему за надзор и управљање, VPN-у (*Virtual Private Network*), телеметријским подацима итд. Мере контроле приступа треба да обухвате двофакторксу аутентификацију, биометријску идентификацију и политике управљања лозинкама, како би само овлашћена лица могла да приступају систему.

Сегментација мреже. Сегментацијом мреже може се изоловати систем за надзор и управљање од корпоративне мреже електроенергетске компаније, чиме се знатно отежава приступ потенцијалним нападачима. Мрежном сегментацијом се ограничава приступ (само овлашћени корисници и уређаји могу приступити одређеним сегментима), смањује се ризик од ширења напада (у случају компромитовања једног дела мреже, нападач не може лако да се прошири на друге делове), повећава се надзор и

контрола, побољшавају се перформансе мреже (мање мреже су често ефикасније и лакше за управљање) што доприноси укупној стабилности система.

Фајревол (*Firewall*) представља прву линију одбране од сајбер напада. То је сигурносни механизам (хардвесрки, софтверски, комбинација оба) који контролише и филтрира мрежни саобраћај између различитих делова мреже. Функционише по унапред дефинисаним правилима, како би спречио неовлашћен приступ, а дозволио само безбедне и дозвољене везе. Фајерволом се штити мреже од нежељеног екстерног приступа, као и интерна комуникација измежу различитих система у органзацији.

Системи за превенцију и детекцију напада (IDPS, *Intrusion Detection and Prevention Systems*). представљају механизам заштите који детектује сумњиве активности и аутоматски предузима мере, као што су блокирање саобраћаја, искључивање компромитованих уређаја, обавештавање администратора, ажурирање безбедносних правила у реалном времену, итд. Применом овог механизма у систему ОИЕ, штити се контролни систем (SCADA), врши се превенција DoS/DDoS (*Denial of Service/Distributed DoS*) напада, контрола удаљеног приступа, штите се телеметријски и дијагностички подаци, и омогућава се реаговање у реалном времену.

Енкрипција. Примена енкрипције у системима обновљивих извора енергије постаје све важнија због све веће дигитализације и умрежавања ових система.. Умрежени енергетски системи ослањају се на SCADA системе за надзор и управљање. Неопходно је да у таквим системима комуникација буде безбедна, односно мора да се обезбеди поверљивост и интегритет података, а то може да се постигне путем енкрипције. Енкрипцијом се у овим системима штити пренос података (нпр. соларни панели шаљу информацију о производњи), комуникација између уређаја (нпр. паметних инвертера, контролера батерија, мрежних претварача), подаци о корисницима (паметна бројила скупљају податке о потропњи корисника).

6 ЗАКЉУЧАК

Транзиција ка чистијим изворима енергије је ту, тако да заштита ових система од сајбер претњи постаје један од најважнијих изазова. Дигитализација има изузетно важну трансформативну улогу у контексту инфраструктура које се заснивају на коришћењу обновљивих извора енергије, доносећи бројне предности у повећању ефикасности, интеграцији напредних информационо-комуникационих технологија. Међутим, иако је у питању неизбежна трансформација која углавном води ка унапређењу перформанси, неопходно је да се одговори на бројне изазове сајбер безбедности који са њом долазе. Квалитетно балансирање дигиталног напретка са робусним мерама сајбер безбедности је потребно да се заснива на сталном унапређивању метода анализе ризика, примена свих неопходних стандарда, регулатива и прописа, увођење различитих проактивних мера сајбер безбедности, уз сталну примену и евалуацију различитих технолошких иновација као и подизање свести о сајбербезбедности како код корисника услуга, тако и код оних које те услуге пружају. Сталним продубљивањем разумевања изазова и постојећих решења у домену индустријске сајбербезбедности се пружа могућност за проактивно обезбеђивање сигурности система обновљивих извора енергије, и њихове заштите од разноврсних претњи које се у континуитету развијају.

7 LITERATURA

[1] D. E. Ekechukwu, P. Simpa, “The importance of cybersecurity in protecting renewable energy investment: A strategic analysis of threats and solutions”, *Engineering Science & Technology Journal*, Vol. 5, No. 6, June 2024, pp. 1845-1883.

[2] M. El Zein, G. Gebresenbet, “Digitalization in the Renewable Energy Sector”, *Energies*, No. 17, 2024, Article No, 1985, doi: 10.3390/en17091985

[3] A. M. Eltamaly, M. A. Alotaibi, A. I. Alolah, M. A. Ahmed, “IoT-Based Hybrid Renewable Energy System for Smart Campus”, *Sustainability*, Vol. 13, No. 15, Article no. 8555, doi: 10.3390/su13158555.

[4] A. Rekeraho, D. T. Cotfas, P. A. Cotfas, T. C. Bălan, E. Tuyishime, R.Acheampong, Cybersecurity challenges in IoT-based smart renewable energy. *Int. J. Inf. Secur.* 23, 101–117 (2024). https://doi.org/10.1007/s10207-023-00732-9

[5] H. A. Aghajari, T. Niknam, M. Shasadeghi, S.M. Sharifhosseini, M.H. Taabodi, E. Sheybani, G. Javidi, M. Pourbehzadi, “Analyzing complexities of integrating Renewable Energy Sources into Smart Grid: A comprehensive review”, *Applied Energy*, No. 383, 2025, Article No. 125317.

[6] R. Röttinger, “Cyberattacks On Renewable Energies: "How Hackers Are Threatening The Energy Transition And Which Technologies Can Protect Us", *European Journal of Engineering and Technology,* vol. 12, no. 1, 2024.

[7] "European Wind-Energy Sector Hacking Linked to Conti Ransomware Group," CyberSecurity Connect, April 2022. [Online]. Available: https://www.cybersecurityconnect.com.au/critical-infrastructure/7772-european-wind-energy-sector-hit-in-wave-of-hacks. [Accessed 10 April 2025].

[8] “Cybersecurity in the power sector” https://www.eurelectric.org/in-detail/cybersecurity-in-the-power-sector/?utm_source=chatgpt.com.

[9] H. Srinivasan, M. Karimi, “Threat-based Security Controls to Protect Industrial Control Systems”, preprint. https://doi.org/10.48550/arXiv.2501.13268

[10] S. Saeed, H. Gull, M. M. Aldossary, A. F. Altamimi, M. S. Alshahrani, M. Saqib, S. Z. Iqbal, A. M. Almuhaideb, „Digital Transformation in Energy Sector: Cybersecurity Challenges and Implications“, . *Information*, No. 15, 2024, Article no. 764. https://doi.org/10.3390/info15120764

[11] S. H. Rouhani, C.-L. Su, S. Mobayen, N. Razmjooy, M. Elsisi, “Cyber resilience in renewable microgrids: A review of standards, challenges, and solutions”, *Energy*, No. 309, 2024, Article No. 133081.

[12] A. B. Ige, E. Kupa, O. Ilori, “Analyzing defense strategies against cyber risks in the energy sector: Enhancing the security of renewable energy sources”, *International Journal of Science and Research Archive*, Vol. 12, No. 01, 2024, pp. 978–2995.