ELEKTR ENERGETIKA TIZIMLARIDA KIBERXAVF-XATARLARNI AMALGA OSHIRISH MEXANIZMI

Karabayev Rustam Zafarovich
Toshkent axborot texnologiyalari universiteti,
Raqamli iqtisodiyot fakulteti yo‘nalishi bo‘yicha 2-kurs magistranti

Annotatsiya. *Ushbu maqolada elektr energetika tizimlarida yuzaga keladigan kiberxavf-xatarlarni amalga oshirish mexanizmlari tahlil qilingan. Zamonaviy energetika infratuzilmasining raqamlashtirilishi va avtomatlashtirilishi natijasida SCADA, IoT hamda sanoat boshqaruv tizimlari kiberhujumlar uchun asosiy nishonga aylanmoqda. Tadqiqotda elektr energetika tizimlariga qarshi amalga oshiriladigan asosiy tahdidlar, ularning kirib kelish usullari, zarar yetkazish bosqichlari hamda energetika obyektlari faoliyatiga ta’siri ko‘rib chiqilgan. Shuningdek, kiberxavf-xatarlarni aniqlash, monitoring qilish va oldini olish bo‘yicha zamonaviy himoya mexanizmlari yoritilgan. Tadqiqot natijalari elektr energetika tizimlarining barqarorligi va axborot xavfsizligini ta’minlashda muhim ahamiyat kasb etadi.*

Kalit so‘zlar*: Elektr energetika tizimi, kiberxavfsizlik, kiberxavf-xatar, SCADA tizimi, sanoat boshqaruv tizimlari, axborot xavfsizligi, kiberhujum, kritik infratuzilma, monitoring, himoya mexanizmlari.*

METHOD FOR ANALYZING CYBER RISKS IN ELECTRIC POWER SYSTEMS

Karabaev Rustam Zafarovich
Tashkent University of Information Technologies,
2st year master’s student of the Faculty of Digital Economics

Abstract. *This article examines the mechanism of cyber threat implementation in electric power systems. Due to the digitalization and automation of modern energy infrastructure, SCADA, IoT, and industrial control systems have become primary targets for cyberattacks. The study analyzes the main threats to electric power systems, methods of unauthorized access, stages of attack execution, and their impact on the operation of energy facilities. In addition, modern approaches to cyber threat detection, monitoring, and prevention are discussed. The research findings are important for ensuring the stability and information security of electric power systems.*

Key words: *Electric power system, cybersecurity, cyber threats, SCADA system, industrial control systems, information security, cyberattack, critical infrastructure, monitoring, protection mechanisms.*

МЕТОД АНАЛИЗА КИБЕРРИСКОВ В ЭЛЕКТРОЭНЕРГЕТИЧЕСКИХ СИСТЕМАХ

Карабаев Рустам Зафарович
Ташкентский университет информационных технологий, магистрант 2 курса факультета цифровая экономика

Аннотация. *В данной статье рассматривается механизм реализации киберугроз в электроэнергетических системах. В условиях цифровизации и автоматизации современной энергетической инфраструктуры системы SCADA, IoT и промышленные системы управления становятся основными объектами кибератак. В исследовании проанализированы основные угрозы для электроэнергетических систем, способы проникновения злоумышленников, этапы реализации атак и их влияние на функционирование энергетических объектов. Также рассмотрены современные методы обнаружения, мониторинга и предотвращения киберугроз. Результаты исследования имеют важное значение для обеспечения устойчивости и информационной безопасности электроэнергетических систем.*

Ключевые слова*: Электроэнергетическая система, кибербезопасность, киберугрозы, SCADA-система, промышленные системы управления, информационная безопасность, кибератака, критическая инфраструктура, мониторинг, механизмы защиты.*

KIRISH

Bugungi kunda elektr energetika tizimlari davlat iqtisodiyoti va jamiyat hayotining eng muhim strategik infratuzilmalaridan biri hisoblanadi. Energetika tarmoqlarining raqamlashtirilishi, avtomatlashtirilgan boshqaruv tizimlari, SCADA[7] (Supervisory control and data acquisition) platformalari hamda IoT[8] (Internet of things) texnologiyalarining joriy etilishi elektr energiyasini ishlab chiqarish, uzatish va taqsimlash jarayonlarining samaradorligini oshirishga xizmat qilmoqda. Shu bilan birga, ushbu texnologiyalarni keng qo‘llash kiberxavfsizlik bilan bog‘liq yangi tahdid va xatarlarning paydo bo‘lishiga sabab bo‘lmoqda.

Elektr energetika tizimlariga qilingan kiberhujumlar nafaqat texnik nosozliklarni, balki yirik iqtisodiy zararlar, elektr ta’minotidagi uzilishlar hamda kritik infratuzilma faoliyatining izdan chiqishini ham keltirib chiqarishi mumkin. Ayniqsa, sanoat boshqaruv tizimlari va masofadan boshqarish texnologiyalariga noqonuniy kirish holatlari energetika obyektlari xavfsizligiga jiddiy tahdid soladi. So‘nggi yillarda dunyoning turli davlatlarida energetika tizimlariga qarshi amalga oshirilgan kiberhujumlar ushbu sohaning zaif jihatlarini yaqqol namoyon etdi.

[7] **SCADA** (Supervisory Control and Data Acquisition – Nazorat va ma’lumotlarni yig‘ish) - bu yirik sanoat va infratuzilma jarayonlarini real vaqt rejimida masofadan boshqarish, monitoring qilish hamda avtomatik ma’lumot to‘plash uchun mo‘ljallangan apparat-dasturiy ta'minot tizimidir

[8] IoT (Internet of Things - Narsalar interneti) - bu internet orqali ma’lumot to‘playdigan, o‘zaro almashadigan va inson artishuvsiz vazifalarni avtomatik bajaradigan jismoniy qurilmalar (narsalar) tarmog‘i

Mazkur tadqiqotning dolzarbligi elektr energetika tizimlarida kiberxavf-xatarlarni amalga oshirish mexanizmlarini chuqur o‘rganish, tahdidlarning asosiy manbalarini aniqlash hamda zamonaviy himoya usullarini ishlab chiqish zarurati bilan izohlanadi. Tadqiqot davomida energetika tizimlariga ta’sir qiluvchi asosiy kiberxatarlar, ularning amalga oshirilish bosqichlari va oqibatlari tahlil qilinadi.

Gipoteza. Agar elektr energetika tizimlarida kiberxavfsizlikni ta’minlash bo‘yicha kompleks himoya mexanizmlari, jumladan, tarmoq monitoringi, tahdidlarni erta aniqlash tizimlari, SCADA va sanoat boshqaruv tizimlarini segmentatsiyalash hamda xodimlarning kiberxavfsizlik bo‘yicha malakasini oshirish choralari samarali joriy etilsa, unda kiberxavf-xatarlarning amalga oshirilish ehtimoli va ularning energetika infratuzilmasiga salbiy ta’siri sezilarli darajada kamayadi.

Adabiyot tahlili. Elektr energetika tizimlarida kiberxavfsizlik masalalari ilmiy va amaliy adabiyotlarda keng yoritilgan. Mavjud tadqiqotlarni bir necha asosiy yo‘nalishlarga ajratish mumkin: kritik infratuzilmani himoya qilish, sanoat boshqaruv tizimlari xavfsizligi hamda aqlli elektr tarmoqlari (Smart Grid) barqarorligini ta’minlash.

Ushbu sohadagi fundamental ishlardan biri Cybersecurity in the Electricity Sector: Managing Critical Infrastructure kitobi hisoblanadi [1]. Muallif Rafal Leszczyna energetika tizimlarida kiberxavfsizlikni boshqarishning tizimli yondashuvini ishlab chiqib, xavflarni baholash, xarajatlarni tahlil qilish hamda xavfsizlik standartlariga moslashuv masalalariga alohida e’tibor qaratadi. Tadqiqotchining fikricha, samarali kiberxavfsizlik nafaqat texnik himoya vositalarini, balki tashkiliy va iqtisodiy choralarni ham o‘z ichiga olgan kompleks himoya mexanizmini talab qiladi.

Yana bir muhim ilmiy manba Cyber-security of SCADA and Other Industrial Control Systems asari hisoblanadi [2]. Ushbu tadqiqotda SCADA tizimlaridagi zaifliklar hamda ularni himoyalash mexanizmlari tahlil qilingan. Mualliflar Edward J. M. Colbert va Alexander Kott sanoat boshqaruv tizimlaridagi nosozliklar energetika infratuzilmasining ishlashiga jiddiy ta’sir ko‘rsatishi mumkinligini ta’kidlaydilar. Shuningdek, ular tarmoq monitoringi, xavflarni baholash va tizimlarni xavfsiz loyihalash muhim himoya omillari ekanligini qayd etadi.

Industrial Network Security kitobida [3] Eric D. Knapp sanoat tarmoqlarida qo‘llaniladigan boshqaruv tizimlari va tarmoq infratuzilmalarining zaif tomonlarini o‘rgangan. Muallifning ta’kidlashicha, sanoat korxonalarida segmentatsiya, autentifikatsiya va real vaqt monitoring tizimlarini joriy etish kiberhujumlarning oldini olishda muhim ahamiyatga ega.

Shuningdek, Practical Industrial Cybersecurity asarida [4] Pascal Ackerman energetika va sanoat obyektlarida kiberxavfsizlikni ta’minlashning amaliy usullarini bayon qilgan. Muallif SCADA va OT tizimlarida himoya mexanizmlarini kuchaytirish, zararli dasturlardan himoyalanish va inson omili bilan bog‘liq xavflarni kamaytirish zarurligini ko‘rsatadi.

Bundan tashqari, Eugene Kaspersky tomonidan olib borilgan tadqiqotlarda sanoat obyektlariga qarshi yo‘naltirilgan murakkab zararli dasturlar, xususan Stuxnet kabi kiberqurollarning xavfi tahlil qilingan [5]. Tadqiqot natijalariga ko‘ra, energetika tizimlarini himoya qilish uchun ko‘p bosqichli xavfsizlik mexanizmlarini joriy etish zarur hisoblanadi.

Tadqiqot metodologiyasi. Mazkur tadqiqotda elektr energetika tizimlarida kiberxavf-xatarlarni amalga oshirish mexanizmlarini tahlil qilish hamda ularning oldini olish bo‘yicha samarali himoya choralarini ishlab chiqish maqsad qilingan. Tadqiqot metodologiyasi nazariy, tahliliy va amaliy yondashuvlar asosida shakllantirildi.

Tadqiqotning dastlabki bosqichida elektr energetika tizimlari va sanoat boshqaruv texnologiyalari bo‘yicha ilmiy adabiyotlar, xalqaro standartlar hamda xorijiy tajribalar o‘rganildi. Cybersecurity in the Electricity Sector: Managing Critical Infrastructure asarida [6] Rafal Leszczyna energetika tizimlarida xavflarni boshqarish, xavfsizlik standartlarini joriy etish va risklarni baholash usullarini yoritgan. Muallifning fikricha, energetika infratuzilmasida kiberxavfsizlikni ta’minlash kompleks boshqaruv yondashuvini talab qiladi.

Tadqiqot davomida tizimli tahlil metodidan foydalanildi. Ushbu metod yordamida elektr energetika tizimlarining asosiy komponentlari, jumladan SCADA va Smart Grid tizimlarining ishlash mexanizmlari o‘rganildi. Cyber-security of SCADA and Other Industrial Control Systems tadqiqotida [7] Edward J. M. Colbert va Alexander Kott sanoat boshqaruv tizimlaridagi zaifliklar va ularning energetika infratuzilmasiga ta’sirini tahlil qilgan. Mualliflar tarmoq monitoringi va hujumlarni aniqlash tizimlari energetika xavfsizligini ta’minlashda muhim omil ekanligini ta’kidlaydi.

Mazkur tadqiqotda risklarni baholash metodologiyasiga ham alohida e’tibor qaratildi. Energetika tizimlariga qarshi ehtimoliy kiberhujumlarning xavf darajasi, iqtisodiy oqibatlari va texnologik ta’siri baholandi. Industrial Network Security kitobida [8] Eric D. Knapp sanoat tarmoqlarida tarmoq segmentatsiyasi, autentifikatsiya va xavfsizlik monitoringi tizimlari kiberxatarlarni kamaytirishda muhim rol o‘ynashini ko‘rsatadi.

Tadqiqot metodologiyasida qiyosiy tahlil usuli ham qo‘llanildi. Ushbu usul orqali dunyoning turli davlatlarida energetika tizimlariga qarshi amalga oshirilgan kiberhujumlar va ularning oqibatlari o‘rganildi. Jumladan, Ukrainadagi elektr tarmoqlariga qilingan kiberhujumlar va Stuxnet zararli dasturi bilan bog‘liq hodisalar tahlil qilindi. Eugene Kasperskytomonidan olib borilgan tadqiqotlarda [9] sanoat obyektlariga qarshi zararli dasturlarning qo‘llanilishi energetika infratuzilmasiga katta zarar yetkazishi mumkinligi qayd etilgan.

Tadqiqot natijasi. Mazkur tadqiqot davomida elektr energetika tizimlarida uchraydigan asosiy kiberxavf-xatarlar, ularning amalga oshirish mexanizmlari hamda energetika infratuzilmasiga ta’siri tahlil qilindi. Tadqiqot natijalari shuni ko‘rsatdiki, energetika tizimlarida raqamlashtirish jarayonining jadallashuvi bilan bir qatorda kiberxavf-xatarlar soni va murakkabligi ham ortib bormoqda.

Tahlillar asosida elektr energetika tizimlariga tahdid soluvchi asosiy xavf manbalari sifatida SCADA tizimlari, sanoat boshqaruv platformalari, IoT qurilmalari hamda masofaviy boshqaruv tarmoqlari aniqlandi. Ushbu tizimlarda autentifikatsiya mexanizmlarining yetarli darajada himoyalanmaganligi, eskirgan dasturiy ta’minot va zaif tarmoq protokollaridan foydalanish kiberhujumlar uchun qulay sharoit yaratishi kuzatildi.

Tadqiqot metodologiyasida qo‘llanilgan tizimli tahlil usuli orqali energetika tizimlarining zaif nuqtalari aniqlanib, ularning kiberxavfsizlik darajasi baholandi. Tadqiqot natijalariga ko‘ra, energetika obyektlariga qarshi amalga oshiriladigan kiberhujumlarning asosiy maqsadi tizim faoliyatini izdan chiqarish, ma’lumotlarni o‘zgartirish yoki elektr ta’minotida uzilishlarni yuzaga keltirishdan iborat ekanligi aniqlandi.

Ayniqsa, zararli dasturlar, fishing hujumlari va tarmoq orqali ruxsatsiz kirish usullari eng ko‘p uchraydigan tahdidlar sifatida qayd etildi. Tadqiqot natijalari shuni ko‘rsatdiki, inson omili va xodimlarning kiberxavfsizlik bo‘yicha bilimlari yetarli emasligi ham energetika tizimlari xavfsizligiga salbiy ta’sir ko‘rsatmoqda.

1-jadval

Elektr energetika tizimlarida uchraydigan asosiy kiberxavf-xatarlar[9]

№	Kiberxavf turi	Amalga oshirish usuli	Energetika tizimiga ta’siri
1	Fishing hujumlari	Elektron pochta va zararli havolalar orqali	Maxfiy ma’lumotlarning o‘g’irlanishi
2	Zararli dasturlar (malware)	Tarmoqqa zararli kod joylashtirish	Tizim ishlashning izdan chiqishi
3	DDoS hujumlari	Server va tarmoqqa ortiqcha yuklama berish	Energetika xizmatlarining vaqtincha to‘xtashi
4	SCADA tizimiga hujum	Boshqaruv tizimiga noqonuniy kirish	Elektr ta’minotda uzilishlar
5	IoT qurilmalariga hujum	Zaif autentifikatsiya va parollar	Qurilmalar ustidan nazorat yo‘qolishi

Tadqiqot davomida monitoring va modellashtirish metodlari yordamida ehtimoliy hujum ssenariylari o‘rganildi. Olingan natijalarga ko‘ra, hujumlarning asosiy qismi bir necha ketma-ket bosqichlarda amalga oshirilishi aniqlandi. Birinchi bosqichda hujumchilar tarmoqqa kirish imkoniyatini qo‘lga kiritadi. Ikkinchi bosqichda ular tizim ichida harakatlanib, SCADA tizimlariga kirishga harakat qiladi. Yakuniy bosqichda esa tizim ishiga zarar yetkazish, ma’lumotlarni o‘zgartirish yoki energetika obyektlari faoliyatini to‘xtatish kabi zararli harakatlar amalga oshiriladi.

Tadqiqot natijalari asosida SCADA tizimlari energetika infratuzilmasining eng muhim va eng zaif elementlaridan biri ekanligi aniqlandi. Ushbu tizimlarning zaifligi elektr energiyasini ishlab chiqarish va uzatish jarayonlarining markazlashtirilgan boshqaruviga bog‘liqdir. Agar SCADA tizimlari faoliyati buzilsa, butun energetika tarmog‘ida nosozliklar yuzaga kelishi mumkin.

[9] Muallif tomonidan tadqiqot jarayonida ishlab chiqilgan

Risklarni baholash metodologiyasi asosida energetika tizimlaridagi tahdidlarning ehtimollik va ta’sir darajalari tahlil qilindi. Tahlillar natijalariga ko‘ra, SCADA tizimlariga qarshi hujumlar eng yuqori xavf darajasiga ega ekanligi aniqlandi.

2-jadval

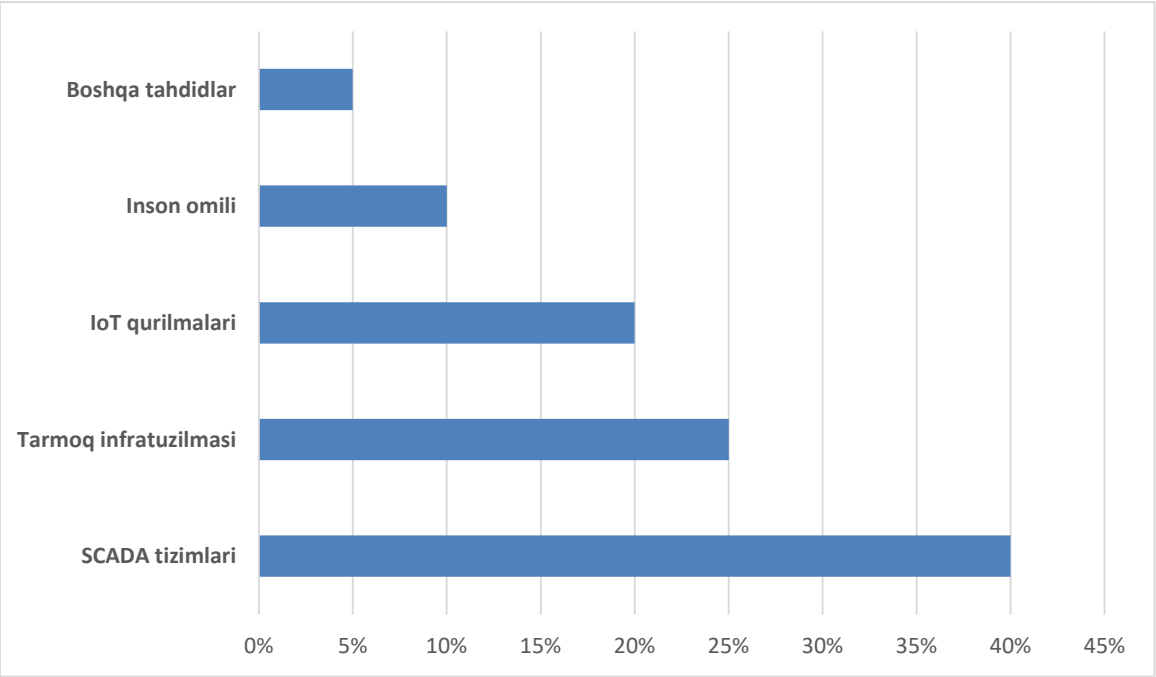
Energetika tizimlarida kiberxavf darajasini baholanishi[10]

№	Kiberxavf turi	Ehtimollik darajasi	Ta’sir darajasi	Umumiy xavf
1	Fishing hujumlari	Yuqori	O‘rta	Yuqori
2	Zararli dasturlar (malware)	Yuqori	Kritik	Kritik
3	DDoS hujumlari	O‘rta	Yuqori	Yuqori
4	SCADA tizimiga hujum	O‘rta	Yuqori	Yuqori
5	IoT qurilmalariga hujum	Yuqori	O‘rta	Yuqori

Statistik tahlillar asosida so‘nggi yillarda energetika sektoriga qarshi amalga oshirilgan kiberhujumlar soni ortib borayotgani kuzatildi. Ayniqsa, davlat va xususiy energetika korxonalariga qarshi yo‘naltirilgan murakkab APT (Advanced persistent threat) hujumlari energetika infratuzilmasining barqaror faoliyatiga jiddiy xavf tug‘dirmoqda.

Xalqaro tajribalar tahlili shuni ko‘rsatdiki, Ukrainadagi elektr tarmoqlariga qilingan kiberhujum natijasida minglab iste’molchilar elektr energiyasiz qolgan. Bu esa energetika tizimlarining kiberxavfsizlikka qanchalik bog‘liq ekanligini yaqqol namoyish etdi. Shuningdek, Stuxnet zararli dasturining sanoat obyektlariga ta’siri SCADA tizimlarining zaif tomonlarini ochib berdi.

[10] Muallif tomonidan tadqiqot jarayonida ishlab chiqilgan



1-rasm. Elektr energetika tizimlarida zaif nuqtalar taqsimoti[11]

Monitoring natijalari asosida energetika tizimlarida real vaqt rejimida xavfsizlik nazoratini amalga oshirish muhimligi aniqlandi. Tadqiqot davomida SIEM tizimlari, tarmoq monitoringi va sun’iy intellekt asosidagi xavfsizlik platformalari tahdidlarni erta aniqlashda samarali vosita ekanligi qayd etildi.

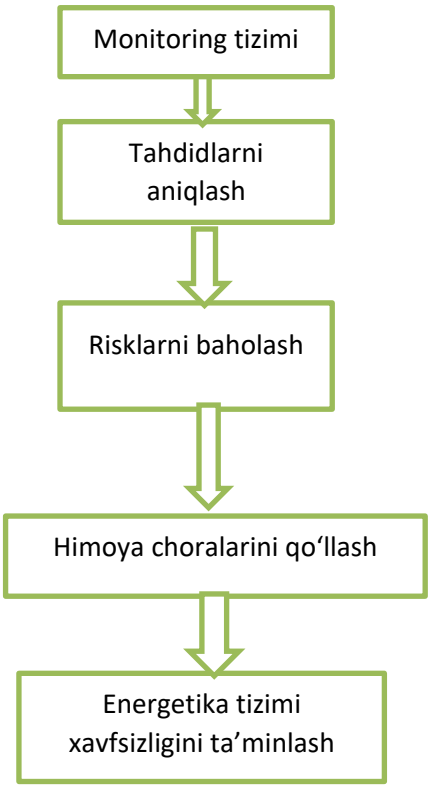
Tadqiqot natijalariga ko‘ra, elektr energetika tizimlarida samarali kiberxavfsizlikni ta’minlash uchun texnik va tashkiliy choralarni birgalikda qo‘llash zarur. Tahlillar asosida quyidagi asosiy himoya choralarining samarali ekanligi aniqlandi:

- tarmoq segmentatsiyasini joriy etish;
- ko‘p bosqichli autentifikatsiya tizimidan foydalanish;
- real vaqt monitoringi va SIEM tizimlarini qo‘llash;
- SCADA dasturiy ta’minot tizimlarini muntazam yangilab borish;
- xodimlar uchun kiberxavfsizlik bo‘yicha treninglar tashkil etish;
- sun’iy intellekt asosidagi tahdidlarni aniqlash tizimlarini joriy qilish.

Tadqiqot natijalari asosida elektr energetika tizimlarida kiberxavf-xatarlarni kamaytirish uchun kompleks himoya tizimini shakllantirish zarurligi aniqlandi. Bunda texnik vositalar bilan bir qatorda tashkiliy boshqaruv, xavfsizlik siyosati va xodimlar malakasini oshirish muhim omil hisoblanadi.

Natijalar shuni ko‘rsatdiki, zamonaviy energetika tizimlarida kiberxavfsizlikni ta’minlash davlat darajasidagi strategik vazifa hisoblanadi. Energetika infratuzilmasining barqaror ishlashi iqtisodiy xavfsizlik, milliy xavfsizlik hamda jamiyatning uzluksiz faoliyati bilan bevosita bog‘liqdir.

[11] Muallif tomonidan tadqiqot jarayonida ishlab chiqilgan



2-rasm. Elektr energetika tizimlarida himoya mexanizmlarining o‘zaro bog’liqligi[12]

O‘tkazilgan tadqiqotlar shuni ko‘rsatdiki, elektr energetika tizimlarida zamonaviy xavfsizlik texnologiyalarini joriy etish orqali kiberhujumlarning salbiy ta’sirini sezilarli darajada kamaytirish mumkin. Shu sababli energetika sektorida xalqaro standartlarga asoslangan kiberxavfsizlik siyosatini shakllantirish, ilg‘or texnologiyalarni joriy etish va xodimlarning malakasini muntazam oshirib borish dolzarb vazifa hisoblanadi.

Xulosa. Mazkur tadqiqot davomida elektr energetika tizimlarida kiberxavf-xatarlarni amalga oshirish mexanizmlari, ularning energetika infratuzilmasiga ta’siri hamda zamonaviy himoya usullari kompleks ravishda tahlil qilindi. Tadqiqot natijalari shuni ko‘rsatdiki, energetika tizimlarining raqamlashtirilishi va avtomatlashtirilishi bilan bir qatorda ushbu sohada kiberxavfsizlikka bo‘lgan ehtiyoj ham keskin ortib bormoqda.

Tahlillar asosida elektr energetika tizimlarida eng katta xavf SCADA tizimlariga qarshi amalga oshiriladigan kiberhujumlar bilan bog‘liqligi aniqlandi. Ushbu tizimlarning zaifligi elektr energiyasini ishlab chiqarish, uzatish va taqsimlash jarayonlariga bevosita ta’sir ko‘rsatishi sababli, energetika infratuzilmasining barqaror ishlashi uchun jiddiy tahdid hisoblanadi. Tadqiqot davomida fishing hujumlari, zararli dasturlar, DDoS hujumlari hamda IoT

[12] Muallif tomonidan tadqiqot jarayonida ishlab chiqilgan

qurilmalariga qarshi amalga oshiriladigan tahdidlar energetika tizimlarida eng ko‘p uchraydigan kiberxavf turlari sifatida qayd etildi.

Risklarni baholash natijalari shuni ko‘rsatdiki, energetika infratuzilmasidagi zaifliklarning asosiy qismi eskirgan dasturiy ta’minot, himoyalanmagan tarmoq segmentlari va inson omili bilan bog‘liqdir. Xususan, xodimlarning kiberxavfsizlik bo‘yicha bilim va ko‘nikmalarining yetarli emasligi fishing va ijtimoiy muhandislik hujumlarining muvaffaqiyatli amalga oshirilishiga sabab bo‘lishi mumkinligi aniqlandi.

Tadqiqotda qo‘llanilgan monitoring, modellashtirish va qiyosiy tahlil metodlari energetika tizimlarida tahdidlarni erta aniqlash hamda ularning oqibatlarini kamaytirishda muhim ahamiyatga ega ekanligini ko‘rsatdi. Xalqaro tajribalar, jumladan Ukrainadagi elektr tarmoqlariga qilingan kiberhujumlar va Stuxnet zararli dasturi bilan bog‘liq hodisalar energetika infratuzilmasining kiberxavfsizlik bilan uzviy bog‘liqligini tasdiqladi.

Tadqiqot natijalari asosida elektr energetika tizimlarida samarali kiberxavfsizlikni ta’minlash uchun kompleks himoya choralarini joriy etish zarurligi asoslandi. Bunda tarmoq segmentatsiyasi, ko‘p bosqichli autentifikatsiya, SIEM va real vaqt monitoring tizimlari, sun’iy intellekt asosidagi tahdidlarni aniqlash platformalari hamda xodimlar malakasini muntazam oshirib borish muhim himoya mexanizmlari sifatida baholandi.

Shuningdek, energetika sohasida xalqaro standartlar asosida yagona xavfsizlik siyosatini shakllantirish, zamonaviy texnologiyalarni joriy etish va kritik infratuzilmalarni doimiy auditdan o‘tkazish zarurligi aniqlandi. Tadqiqot natijalari energetika tizimlarida axborot xavfsizligini mustahkamlash, kiberxavf-xatarlarni kamaytirish va energetika infratuzilmasining uzluksiz ishlashini ta’minlashda muhim ilmiy-amaliy ahamiyatga ega.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. Leszczyna R. Cybersecurity in the Electricity Sector: Managing Critical Infrastructure. Springer, 2018.
2. Colbert E.J.M., Kott A. Cyber-security of SCADA and Other Industrial Control Systems. Springer, 2011.
3. Knapp E.D., Langill J.T. Industrial Network Security. Syngress, 2014.
4. Ackerman P. Practical Industrial Cybersecurity. Packt Publishing, 2017.
5. Kaspersky E. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2015.