

ENERGIYA XAVFSIZLIGINI TA'MINLASHNING TIZIMLI TAHLILI VA ALGORITMI

Isaqov Abdusaid Jalilovich

- *Energiya fakulteti dekani, texnika fanlari doktori, professor, “Toshkent irrigatsiya va qishloq xo'jaligini mexanizatsiyalash muxandislari instituti” milliy tadqiqot universiteti*
tel.: +998-977210670, Isakovsaid72@mail.ru

Xoliqova Manzura Qoyirovna

Toshkent davlat agrar universiteti, «Axborot tizimlari va texnologiyalari» kafedrasii
assistenti, tel.: +998934758834, manzuraxoliqova37@gmail.com

Annotatsiya: *Ushbu maqolada energiya sohasini kiberxavfsizlik bilan bog'liqligi haqida ma'lumotlar keltirilgan. Buning uchun zamonaviy dasturlash tillaridan foydalanish, algoritm yaratish, tizimli tahli qilish kabi zamonaviy bir qancha ma'lumotlar aytib o'tildan. Energiya xavfsizligini ta'minlashning bosqichlari keltirib o'tilgan.*

Kalit so'zlar: *algoritm, ob'yekt, dastur, model, tizimli tahlil, qaror qabul qilish, raqamli texnologiya, bulutli texnologiya, kiberxavfsizlik, kiberhujum, kibertahdid*

Bugungi kunga barcha sohalarda yangi zamonaviy axborot-kommunikatsiya texnologiyalarini ishlab chiqish va joriy etish, shu jumladan, energiya sohasini ham raqamli o'zgartirish kontsepsiyasini ilgari surish energetika sohasining o'ziga xos xususiyatlari bilan birgalikda kibertahdidlarni energiyaga strategik tahdidlar ro'yxatiga kiritish zarurligini belgilab beradi [1].

Bir tomondan, sun'iy intellekt texnologiyalaridan foydalanish, shuningdek, sanoat buyumlar interneti, katta ma'lumotlar, mashinalarni o'rganish, bulutli texnologiyalar, raqamli texnologiyalar kabi istiqbolli texnologiyalar, taqsimlangan registrlar energiya ob'ektlariga kiberhujumlar xavfini oshiradi [2].

Boshqa tomondan, kiberxavfsizlik sohasida zamonaviy dasturlash usullarini qo'llash kiber vaziyatdan xabardorlik deb ataladigan yondashuv doirasida faol rivojlanmoqda. Kibervaziyatli xabardorlik - bu kiberxavfsizlik sohasida sun'iy intellekt usullarini qo'llash bilan bog'liq bo'lgan soha bo'lib, kiberxavfsizlik buzilishining mumkin bo'lgan holatlari haqida xabardorlikni oshirishga va kiber tahdidlarni avtomatik ravishda aniqlashga qaratilgan [3].

Kibertahdid- kibermakonda shaxs, jamiyat va davlat manfaatlariga tahdid soluvchi shart-sharoitlar va omillar majmiudir.

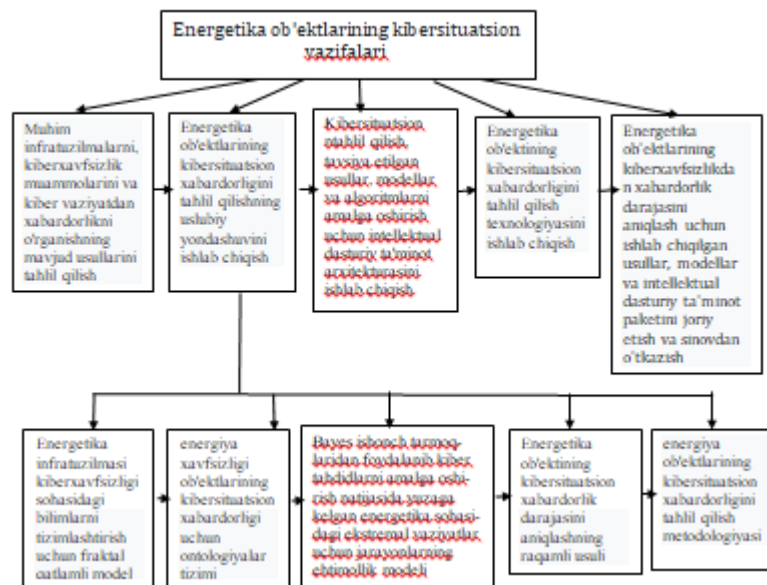
Kiberxavfsizlik — kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati

Kiberhujum deb kibermakonda apparat, apparat-dasturiy va dasturiy vositalardan foydalangan holda qasddan amalga oshiriladigan, kiberxavfsizlikka tahdid soladigan harakatga aytiladi.

Kiber vaziyatdan xabardorlik bo'yicha tadqiqotlarda algoritmlash, dasturlash, semantik modellashtirish, Bayes e'tiqod tarmoqlari, ekspert tizimlari texnologiyasi va kognitiv grafika kabi sun'iy intellekt usullari qo'llaniladi.

Buning uchun kiber vaziyatdan xabardorlikni tahlil qilish usullari, kiber tahdidlarni tahlil qilishning semantik usullari va energiya ob'ektlari misolida tavsiya etilgan usullarni qo'llab-quvvatlash uchun intellektual dasturiy ta'minot tizimlarini yaratish usullaridan foydalanish va qayta tiklanuvchi zamonaviy dasturlardan foydalanish kerak [1].

Bundan maqsadimiz energetika ob'ektlarining kibersituatsion xabardorligini tahlil qilish uchun usullar, modellar va intellektual dasturiy ta'minot to'plamini ishlab chiqishdir. Quyida energetika ob'ektlarining kibersituatsion vazifalarining algoritmi keltirilgan.



1-rasm. Energetika ob'ektlarining kibersituatsion vazifalari

Bundan ko'rinib turibdiki, ketma-ketliklar algoritmi umumiy tushuncha va texnologiyani ishlab chiqishda muqobil energiya manbalari aqlli tarmoqlarni yaratish shuningdek, tegishli infratuzilma jarayonlari, modellari ishlab chiqiladi [2].

Energiya xavfsizligini ta'minlash uchun quyidagi bosqichlarni amalga oshirish kerak:

- 1) Maxsus bulutda arxitektura ishlab chiqish
- 2) kiber vaziyatdan xabardorlikni tahlil qilish
- 3) intellektual dasturiy ta'minot to'plamini ishlab chiqish
- 4) taklif qilingan usullar va modellarni amalga oshirish
- 5) ekspert tizimining integratsiyasi
- 6) Bayes ishonch tarmoqlarining tarkibiy qismi
- 7) vizual xavf komponentini avtomatik kodlash
- 8) algoritm(ataka hujumga qarshi)
- 9) zamonaviy dastur(online va offline)
- 10) model va modellashtirish
- 11) tizimli tahlil qilish
- 12) qaror qabul qilish algoritmlarini ishlab chiqish

Demak, o'z-o'zidan ko'rinib turibdiki elektr energiya sohasi kibertahdidlarga uchramasligi uchun yangi yechimlar va modellarni ishlab chiqish kerak bo'ladi.

Kiberxavfsizlikni ta'minlash uchun esa tezkor qarorlarni qabul qilish, usullar, modellar, va tahlil dasturlarini ishlab chiqish zarur.

FOYDALANILGAN ADABIYOTLAR.

1. Isaqov A.J., Ismailova M.I., A., Bayzakov T.M. “Elektr yoritish va nurlatish” УДК 63: 535.21 (075.8) ,Т. 2007 у.
2. Isaqov A. J., Xoliqova M. Q. “Elektr to'lovlarini to'lashning zamonaviy dasturlash tili tomonidan bajarilishi”, “The multidisciplinary journal of science and technology”, ISSN: 2582-4686 SJIF 2021-3.261, SJIF 2022-2.889, 2023-5.384 ResearchBib IF: 8.848 / 2023
3. Гаськова, Д.А. Анализ нарушений кибербезопасности в энергетическом секторе // «Системные исследования в энергетике» / Труды молодых ученых ИСЭМ СО РАН. Вып. 47. – Иркутск: ИСЭМ СО РАН. – 2017.
4. Massel, A.G. Dynamic Fuzzy Cognitive Models as a Means of Visual Analytics and Cognitive Graphics / A.G. Massel, D.A Gaskova // Proceedings of the 21th international workshop on computer science and information technologies (CSIT'2019). Publisher: Atlantis Press. – 2019.
5. Хасанзода, Н. Основные положения концепции «Интеллектуальные сети» (Smart Grid) / Н. Хасанзода, А.В. Герасименко // «Электроэнергетика, гидроэнергетика, надёжность и безопасность»: Республиканская научнопрактическая конференция ТТУ им. акад. М.С. Осими. Душанбе: «Промэкспо», – 2016
6. Vitenburg, E. Decision-Making based on Enterprise's Information System's Monitoring Data / E. Vitenburg, A. Nikishova, E. Maksimova // International MultiConference on Industrial Engineering and Modern Technologies (FarEastCon 2020). – Papers 9271428. – IEEE, 2020
7. Кибербезопасность 2021-2022. Тренды и прогнозы [Электронный ресурс]. – Режим доступа: <https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-2021-2022-trendy-i-prognozy/>
8. Lex.uz. O'RQ-764-сон 15.04.2022. Kiberxavfsizlik to'g'risida