TEXNOLOGIK JARAYONLARDA KIBERXAVFSIZLIK MASALALARI

Uzaqbergenov Aytbay Jumabay ulı
Texnologik jaryonlar, ishlab chiqarishni avtomatlashtirish va boshqarish 3-TJA-22 kurs talabasi
Nukus Texnika Universiteti Nukus sh.

Annotatsiya: Ushbu maqolada texnologik jarayonlarda kiberxavfsizlik muammolari va ularning zamonaviy sanoatdagi ahamiyati tahlil qilinadi. Maqolada ishlab chiqarish va boshqa sanoat sohalarida qo‘llaniladigan boshqaruv tizimlarining kiberhujumlarga qanday zaifligi ko‘rsatilib, DDoS-hujumlar, zararli dasturiy ta’minot, phishing va ichki xatolar kabi asosiy tahdidlar tahlil qilinadi. Shuningdek, kiberxavfsizlikni ta’minlash uchun tizimlarni yangilash, kuchli autentifikatsiya, tarmoqlarni segmentatsiya qilish, xodimlarni o‘qitish va monitoring qilish kabi samarali usullar bayon etilgan. Maqola texnologik jarayonlarning barqaror va xavfsiz ishlashi uchun kiberxavfsizlikning muhimligini ta’kidlaydi va ushbu sohaga doir zamonaviy yondashuvlarni taklif etadi.

Kalit so‘zlar: Texnologik jarayonlar, Kiberxavfsizlik, Avtomatlashtirish, SCADA tizimlari, DDoS-hujumlar, Zararli dasturiy ta’minot (malware), Phishing, Avtomatlashtirilgan boshqaruv tizimlari, Kiberhujumlar, Ishlab chiqarish xavfsizligi, Raqamli transformatsiya

Аннотация: В данной статье анализируются проблемы кибербезопасности в технологических процессах и их значение в современной промышленности. В статье показана уязвимость систем управления, используемых в производстве и других отраслях промышленности, к кибератакам, и проанализированы основные угрозы, такие как DDoS-атаки, вредоносное ПО, фишинг и внутренние ошибки. Также описаны эффективные методы обеспечения кибербезопасности, такие как обновление систем, сильная аутентификация, сегментация сетей, обучение персонала и мониторинг. В статье подчеркивается важность кибербезопасности для стабильной и безопасной работы технологических процессов и предлагаются современные подходы в этой области.

Ключевые слова: Технологические процессы, Кибербезопасность, Автоматизация, SCADA системы, DDoS-атаки, Вредоносное ПО (malware), Фишинг, Автоматизированные системы управления, Кибератаки, Производственная безопасность, Цифровая трансформация

Abstract: This article analyzes cybersecurity problems in technological processes and their significance in modern industry. The article shows how vulnerable management systems used in manufacturing and other industrial sectors are to cyberattacks, and analyzes key threats such as DDoS attacks, malware, phishing, and

internal errors. Effective methods for ensuring cybersecurity, such as system updates, robust authentication, network segmentation, and employee training and monitoring, are also described. The article emphasizes the importance of cybersecurity for the stable and safe operation of technological processes and offers modern approaches to this area.

Keywords: Technological processes, Cybersecurity, Automation, SCADA systems, DDoS attacks, Malware, Phishing, Automated control systems, Cyberattacks, Production security, Digital transformation

Zamonaviy sanoatda texnologik jarayonlarning avtomatlashtirilishi va raqamlashtirilishi tobora ortib bormoqda. Buning natijasida ishlab chiqarish, energetika, transport, tibbiyot kabi ko‘plab sohalarda boshqaruv tizimlari Internetga yoki korporativ tarmoqlarga ulangan holatda ishlaydi. Biroq, ushbu raqamlashtirish jarayoni bilan birga kiberxavfsizlik muammolari ham keskin oshmoqda. Kiberhujumlar tufayli texnologik jarayonlarning buzilishi ishlab chiqarishni to‘xtatishi, moliyaviy yo‘qotishlar, va hattoki odamlar hayotiga xavf tug‘dirishi mumkin. Shu bois texnologik jarayonlarni himoya qilish sohasidagi kiberxavfsizlik masalalari dolzarb va muhim hisoblanadi.

Texnologik jarayonlarda kiberxavfsizlikning ahamiyati

Texnologik jarayonlarni boshqarishda qo‘llaniladigan SCADA (Supervisory Control and Data Acquisition), DCS (Distributed Control Systems), PLC (Programmable Logic Controllers) kabi tizimlar ko‘pincha Internetga yoki mahalliy tarmoqlarga ulanadi. Bu tizimlar ishlab chiqarishni real vaqt rejimida nazorat qilish, jarayonlarni avtomatik boshqarish imkonini beradi. Biroq, ularning tarmoqqa ulanib qolishi xavfsizlik nuqtai nazaridan katta zaiflikni yuzaga keltiradi.

Kiberxavfsizlikning yetarli darajada ta’minlanmasligi ishlab chiqarish liniyalarida noto‘g‘ri boshqaruvga, jarayonlarning to‘xtashiga yoki noto‘g‘ri ishlashiga olib keladi. Masalan, kimyoviy zavodda boshqaruv tizimiga qilingan kiberhujum xavfli kimyoviy moddalar oqimini nazoratdan chiqarishi mumkin. Shu sababli texnologik jarayonlarni kiberhujumlardan himoya qilish nafaqat ishlab chiqarish samaradorligini, balki inson hayotini va atrof-muhitni himoya qilishni ham ta’minlaydi.

Kiberxavfsizlik tahdidlari va hujum turlari

Texnologik jarayonlarga qaratilgan kiberhujumlarning asosiy turlari quyidagilar:

DDoS-hujumlar (Distributed Denial of Service): Ushbu hujumda tizim yoki tarmoqqa ko‘p sonli so‘rovlar yuborilib, uning normal ishlashini to‘xtatishga harakat qilinadi. Masalan, ishlab chiqarish tizimining boshqaruv serveriga ko‘p so‘rov yuborilib, tizim “tiqilib” qoladi.

Zararlangan dasturiy ta’minot (malware): Viruslar, trojanlar, ransomware kabi zararli dasturlar tizimga kirib, ma’lumotlarni o‘g‘irlaydi, shifrlaydi yoki buzadi. Misol

uchun, ransomware turidagi hujumlarda tizim fayllari shifrlanib, ularni qayta tiklash uchun pullik talab qilinadi.

Phishing va ijtimoiy muhandislik: Kiberjinoyatchilar xodimlarning shaxsiy ma’lumotlari, parollarini o‘g‘irlash uchun soxta email yoki saytlar orqali aldov usullarini qo‘llaydi. Natijada tizimga ruxsatsiz kirish mumkin bo‘ladi.

Ichki xatolar va maqsadli ichki hujumlar: Ba’zida tashkilot ichidagi xodimlarning xato yoki ataylab qilgan harakatlari ham tizim xavfsizligini buzadi. Masalan, zaif parollarni ishlatish yoki ruxsatsiz dastur o‘rnatish.

Zero-day zaifliklari: Dasturiy ta’minotdagi hali aniqlanmagan zaifliklardan foydalanish orqali tizimga ruxsatsiz kirish.

Kiberxavfsizlikni ta’minlash usullari

Texnologik jarayonlarda xavfsizlikni ta’minlash uchun bir necha darajali chora-tadbirlar qo‘llaniladi:

Tizimlarni doimiy yangilash va patchlar o‘rnatish: Ishlab chiqarish tizimlarining dasturiy ta’minotidagi zaifliklarni bartaraf etish uchun yangilanishlar muntazam ravishda o‘rnatilishi zarur. Bu esa kiberhujumlarga qarshi dastlabki himoya qatlamini yaratadi.

Kuchli autentifikatsiya tizimlari: Foydalanuvchilarning tizimga kirishini himoya qilish uchun kuchli parollar, ikki faktorli autentifikatsiya (2FA), biometrik ma’lumotlar (barmoq izi, yuz tanish) qo‘llaniladi. Bu usullar hisoblarni o‘g‘irlash va ruxsatsiz kirish xavfini kamaytiradi.

Tarmoqlarni segmentatsiya qilish: Muhim ishlab chiqarish tizimlari korporativ va internet tarmoqlaridan ajratib qo‘yiladi. Bu orqali hujumchi faqat bitta segmentga kira olsa ham, butun tizimga ta’sir qilish imkoniyati kamayadi.

Xodimlarni kiberxavfsizlik bo‘yicha o‘qitish: Xodimlarga phishing, ijtimoiy muhandislik usullaridan himoyalanish, kuchli parol yaratish, shubhali xabarlarga javob bermaslik bo‘yicha muntazam treninglar o‘tkazish zarur. Chunki inson omili kiberxavfsizlikdagi eng zaif nuqta hisoblanadi.

Monitoring va tahlil tizimlari: Tizimdagi har qanday shubhali yoki ruxsatsiz faoliyatni aniqlash uchun real vaqt rejimida monitoring tizimlari ishlaydi. Bu tizimlar potentsial hujumlarni erta aniqlash va ularga tezkor javob berishga yordam beradi.

Zaxira nusxalarini yaratish: Kiberhujumdan keyin ma’lumotlarni tiklash uchun doimiy zaxira nusxalari yaratiladi va xavfsiz joyda saqlanadi.

Texnologik jarayonlarda kiberxavfsizlik zamonaviy sanoat va iqtisodiyotning ajralmas qismiga aylandi. Hujumlar faqat iqtisodiy yo‘qotishlarga olib kelmay, balki inson hayotiga tahdid solishi mumkin. Shu sababli korxonalar o‘z ishlab chiqarish tizimlarini himoya qilishga jiddiy e’tibor berishi zarur. Bu nafaqat texnologik yechimlarni, balki inson omilini ham hisobga olgan keng qamrovli yondashuvni talab qiladi. Zamonaviy kiberxavfsizlik vositalarini qo‘llash, xodimlarni muntazam o‘qitish,

tizimlarni doimiy yangilash va monitoring qilish texnologik jarayonlarning barqaror va xavfsiz ishlashini ta’minlashda muhim rol o‘ynaydi.

FOYDALANILGAN ADABIYOTLAR

1. Abdullaev, B. “Kiberxavfsizlik asoslari va zamonaviy tahdidlar.”Toshkent: “Ilm ziyo”, 2021.
2. Rustamova, M. “Texnologik jarayonlarda axborot xavfsizligi.” Toshkent: “Texnologiya”, 2020.
3. Mirzayev, D. “Sanoatda avtomatlashtirish va xavfsizlik muammolari.” Toshkent: O‘zbekiston Fanlar Akademiyasi, 2022.
4. Иванов, А. И. “Кибербезопасность в автоматизированных производственных системах.” Москва: “Техносфера”, 2019.
5. Петрова, Е. В. “Угрозы и защита информационных систем в промышленности.” Санкт-Петербург: “Питер”, 2020.
6. Кузнецов, В. А. “Основы кибербезопасности.” Москва: “Бином”, 2018.
7. https://scientific-jl.com/mod/article/view/10930
8. https://tadqiqotlar.uz/03/article/view/1298
9. https://scientific-jl.com/tad/article/view/9708
10. https://tadqiqotlar.uz/03/article/view/1298?utm_source=chatgpt.com