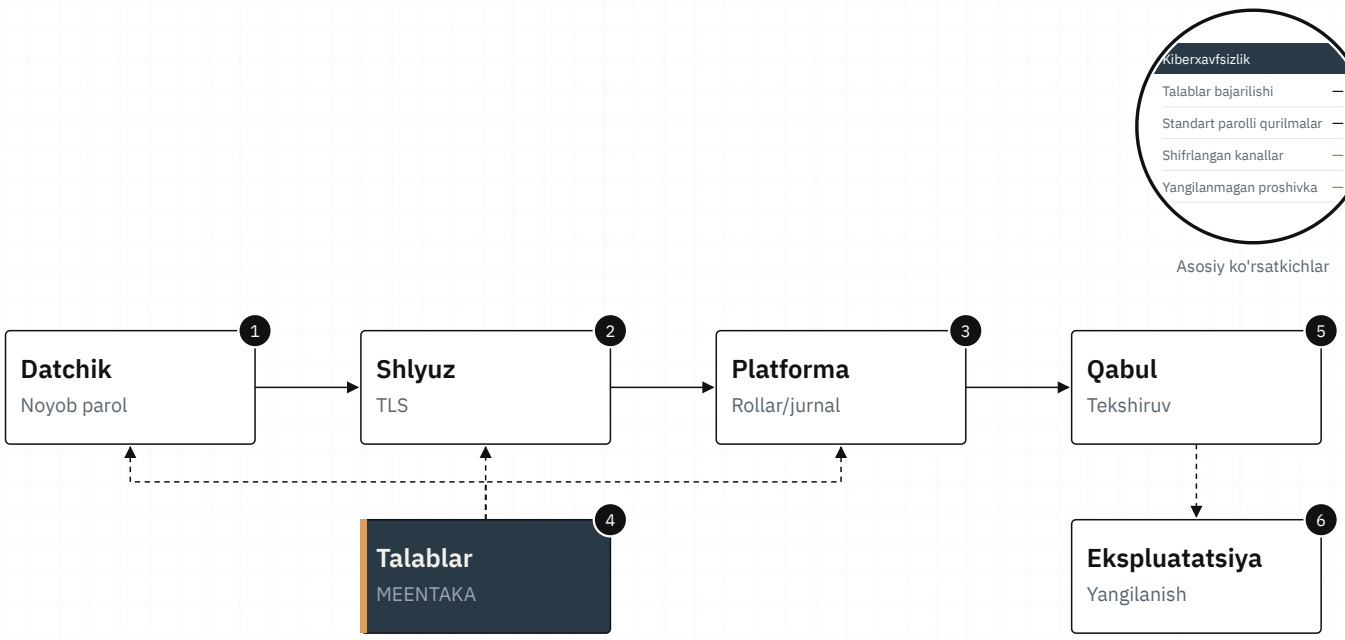
MEENTAKA

KX-04

KIBERXAVFSIZLIK · KIBERXAVFSIZLIK · XAVFSIZ DIZAYN

Datchik, shlyuz va platforma: xavfsizlik — loyihaning birinchi kunidan

Har bir yangi datchik va bulutli panel — yangi kirish nuqtasi. Raqamlashtirish loyihasi xavfsizlikni keyinga qoldirsa, keyin qimmatga tushadi.



Hujjat turi	Kod	Til	Holat
Yechim hujjati	KX-04	O'zbekcha	Noyabr 2026

01 — Qisqacha

Datchik o'rnatildi. Paroli zavod sozlamasida qoldi.

IBM ma'lumotiga ko'ra sanoat sektorida bitta ma'lumot sizishining o'rtacha zarari 5 mln dollar. Kiberxavfsizlik markazi 2026-yilda bostirib kirishlarni aniqlash, zararli dasturlardan himoya, axborotni muhofaza qilish vositalari va amaliy dasturiy ta'minotga oid milliy standartlarni ishlab chiqdi. MEENTAKA o'z IoT va ombor yechimlarini shu yondashuv bilan loyihalaydi.

MAQSAD

Datchik o'rnatildi. Paroli zavod sozlamasida qoldi.

YECHIM

Har bir IoT/WMS loyihasi uchun xavfsizlik talablari ro'yxati: noyob parollar, shifrlangan kanallar (TLS), rollar bo'yicha kirish, jurnal, proshivka yangilash, ma'lumotlarni saqlash joyi; qabulda tekshiruv ro'yxati.

NATIJA

O'lchanadigan ko'rsatkichlar: talablar bajarilishi, standart parolli qurilmalar, shifrlangan kanallar, yangilanmagan proshivka.

Kimlar uchun

Loyiha rahbari
Talablar.

IT/xavfsizlik
Qabul.

Yetkazib beruvchi
Dizayn.

Ekspluatatsiya
Yangilanish.

> Xavfsizlik — qo'shimcha modul emas, loyiha talabi.

QISQA FAKTLAR

$5,00 mln
Sanoat sektorida ma'lumot sizishining o'rtacha zarari (IBM 2025).[1]

O'zMSt 838–841
2026 milliy kiberxavfsizlik standartlari.[2]

PF–38
2026–2030 strategiya.[3]

Manbalar — oxirgi betda.

02 — Kontekst

Sohada nima ma'lum

Rasmiy va xalqaro manbalar.

Fakt	Manba
Sanoat sektorida o'rtacha zarar $5,00 mln; global $4,44 mln.[1]	IBM Cost of a Data Breach 2025
O'zMSt 838:2026 (IDS/IPS), 839:2026 (zararli dasturlardan himoya), 840:2026 (himoya vositalari tasnifi), 841:2026 (amaliy dasturiy ta'minot talablari).[2]	Kiberxavfsizlik markazi (csec.uz)
2026–2030 Kiberxavfsizlik strategiyasi.[3]	PF–38

Bu raqamlarni qanday o'qish kerak

Milliy standartlarning majburiylik doirasi va qo'llanish sohasi rasmiy matnda tekshirilishi kerak.

Faktlar manbada qanday berilgan bo'lsa, shunday keltirilgan. Yetkazib beruvchi ma'lumotlari shunday belgilangan va boshqa korxonada kafolatlanmaydi.

03 — Muammo

Loyihada nima unutiladi

Odatdagi bo'shliqlar:

01
Standart parol
Qurilmalar zavod sozlamasida.

02
Shifrlanmagan kanal
Datchikdan bulutgacha ochiq matn.

03
Yangilanish
Proshivka yangilash yo'li yo'q.

04
Rollar
Hammada administrator huquqi.

Yo'qotishni qanday hisoblash mumkin

Kirish nuqtasi	`butun tarmoq xavfi`
Qayta loyihalash	`keyin tuzatish xarajati`
Ma'lumot	`sizish zarari`
Muvofiqlik	`talablarga mos kelmaslik`

Formulalar namunaviy; aniq qiymat auditda o'lchanadi.

Rahbar o'ziga beradigan savollar

> Har qurilmada noyob parol bormi?

> Datchikdan platformagacha kanal shifrlanganmi?

> Rollar bo'yicha kirish bormi?

04 — Yechim arxitekturasi

Talablar → arxitektura → qabul testi → ekspluatatsiya

Har bir IoT/WMS loyihasi uchun xavfsizlik talablari ro'yxati: noyob parollar, shifrlangan kanallar (TLS), rollar bo'yicha kirish, jurnal, proshivka yangilash, ma'lumotlarni saqlash joyi; qabulda tekshiruv ro'yxati.

Foydalanuvchilar	Loyiha rahbari · IT/xavfsizlik · Yetkazib beruvchi · Ekspluatatsiya
Qurilma	Noyob parol · Proshivka · Port
Kanal	**TLS** · **Sertifikat** · **VPN**
Platforma	**Rollar** · **Jurnal** · **Zaxira**
Ekspluatatsiya	Yangilanish · Monitoring · Javob
Integratsiya	1C · ESF / EDO · Datchik va PLC · Telegram ogohlantirish

Boshqaruv paneli

Loyiha xavfsizlik talablari bajarilishi, qurilmalar holati

Qora qatorlar — MEENTAKA qatlami. Mavjud uskuna va tizimlar saqlanadi; ma'lumot ulardan yig'iladi.

05 — Modullar katalogi

Nima o'rnatiladi

Har bir modul alohida ishga tushadi; paket korxona ehtiyojiga qarab yig'iladi.

Modul	Vazifa	Tayyorlik
Xavfsizlik talablari ro'yxati	Loyiha	◐ **Muhandislik imkoniyati**
Qabul tekshiruvi	Topshirish	◐ **Muhandislik imkoniyati**
Proshivka va sertifikatlar boshqaruvi	Ekspluatatsiya	◐ **Muhandislik imkoniyati**
Mustaqil xavfsizlik sinovi	Ruxsat etilgan hamkor	○ **Ishlab chiqilmoqda**

● Tijoriy mavjud ◐ Muhandislik imkoniyati ○ Ishlab chiqilmoqda

Korxona tomonidan kerak

- Loyiha rahbari
- Arxitektura sxemasi
- Qurilmalar ro'yxati
- Yetkazib beruvchi hujjatlari

Va'da qilinmaydi

- Sertifikatlash, attestatsiya yoki MAI obyektini rasmiy baholash (vakolatli organlar va akkreditatsiyalangan tashkilotlar vazifasi)
- Penetratsion test yoki xakerlik xizmatlari (faqat ruxsat etilgan hamkorlar orqali)
- "100% himoya" yoki hujum bo'lmasligi kafolati
- Yuridik maslahat

06 — Joriy qilish

Kichikdan boshlaymiz, o'lchab kengaytiramiz

Audit → pilot → kengaytirish → obuna. Har bosqich oldingisining o'lchangan natijasiga tayanadi.

1–2 hafta
Talablar sharhi
Aktivlar va jarayonlar.

Natija: xavflar xaritasi.

30 kun
Pilot (1 loyiha)
Bitta sex yoki tizim, 30 kun.

Natija: birinchi natijalar.

2–3 oy
Barcha raqamli loyihalar
Butun korxona.

Natija: doimiy jarayon.

Doimiy
Qo'llab-quvvatlash
Oylik hisobot.

Natija: talablar bajarilishi.

Muddatlar taxminiy; auditdan keyin aniqlanadi.

O'lchanadigan ko'rsatkichlar

Ko'rsatkich	Birlik	Manba
Talablar bajarilishi	%	Tekshiruv
Standart parolli qurilmalar	Soni	Audit
Shifrlangan kanallar	%	Audit
Yangilanmagan proshivka	Soni	Tizim

07 — Keyingi qadam

Raqamli loyihangiz xavfsiz loyihalanganmi

O'n savol. "Yo'q" javoblari — auditda birinchi ko'riladigan joylar.

01 Har qurilmada noyob parol bormi?

02 Datchikdan platformagacha kanal shifrlanganmi?

03 Rollar bo'yicha kirish bormi?

04 Harakatlar jurnali saqlanadimi?

05 Proshivka yangilash tartibi bormi?

06 Ma'lumot qayerda saqlanishi aniqmi?

07 Qabulda xavfsizlik tekshiruvi bormi?

08 Milliy standartlar talablari o'rganilganmi?

09 Kiberxavfsizlik uchun mas'ul shaxs tayinlanganmi?

Xavfsiz dizayn sharhi

IoT yoki ombor tizimi loyihangizni xavfsizlik talablari ro'yxati bo'yicha ko'rib chiqamiz.

meentaka.uz · info@meentaka.uz · +998 99 321 47 77

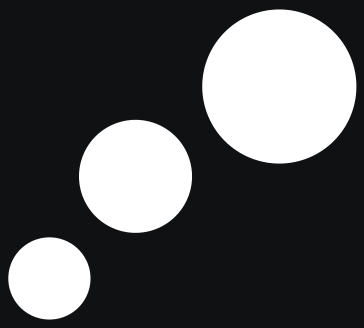
Natijada olasiz

- Aktivlar va xavflar xaritasi
- Ustuvor choralar rejasi
- Loyiha va oylik qo'llab-quvvatlash

Manbalar

1. IBM Cost of a Data Breach 2025 (mart 2024–fevral 2025): global o'rtacha zarar $4,44 mln; sanoat sektorida $5,00 mln; aniqlash va cheklash o'rtacha 241 kun; fishing — eng ko'p uchraydigan hujum vektori (16%).
2. Kiberxavfsizlik markazi (csec.uz): 2026-yilda O'zMSt 838–841:2026 milliy standartlari ishlab chiqilgan (bostirib kirishlarni aniqlash, zararli dasturlardan himoya, axborotni muhofaza qilish vositalari, amaliy dasturiy ta'minot talablari).
3. Farmon PF–38 (10.03.2026; spot.uz, norma.uz): 2026–2030 yillarga Kiberxavfsizlik strategiyasi va yo'l xaritasi; 01.04.2026 dan davlat organlari va tashkilotlari kiberxavfsizlikka mablag' ajratishi shart; Adliya, Energetika vazirliklari va Soliq qo'mitasida kiberxavfsizlik bo'limlari; DXX mustaqil ekspertlar ishtirokida zaifliklarni topish tanlovlarini maxsus platformada o'tkazadi.

Hujjat 2026-yil noyabr holatiga ochiq manbalar asosida tayyorlangan. Ma'lumotlar manbada qanday berilgan bo'lsa, shunday keltirilgan. Hujjat huquqiy yoki moliyaviy maslahat emas; rasmiy matnlarni lex.uz va soliq.uz da tekshiring.



MEENTAKA

Nashr etuvchi

© 2026 MEENTAKA. «The Endurance Industrial Technologies» MChJ

Hujjat raqami
MT-KX-04-UZ · 11.2026

Aloqa
meentaka.uz · info@meentaka.uz · +998 99 321 47 77