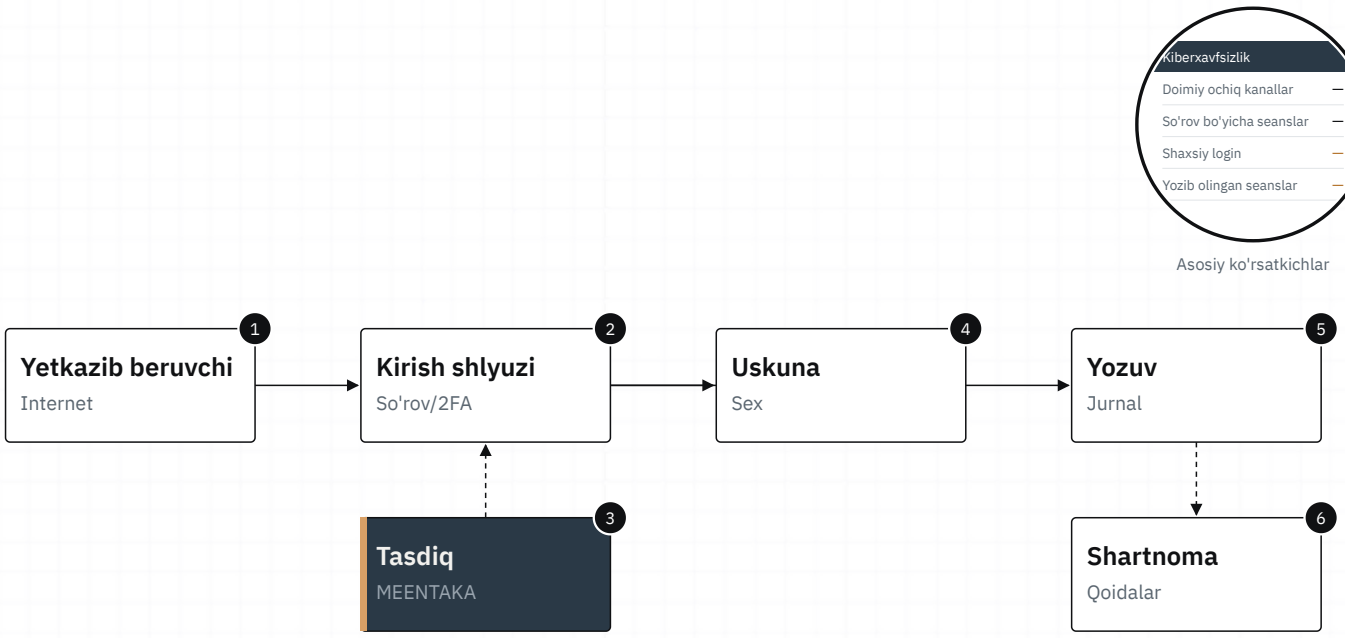
KIBERXAVFSIZLIK · KIBERXAVFSIZLIK · MASOFAVIY KIRISH

Uskuna yetkazib beruvchisi masofadan ulanadi: kim, qachon va nimaga

Xorijiy uskuna o'rnatilgan har bir zavodda masofaviy servis ulanishi bor. Ko'pincha u doimiy ochiq, umumiy parol bilan va hech kim kuzatmaydi.



Hujjat turi	Kod	Til	Holat
Yechim hujjati	KX-03	O'zbekcha	Noyabr 2026

01 — Qisqacha

Uskunangizga xorijdan kim ulanayapti — bilasizmi?

Dragos hisobotiga ko'ra hujumchilar endi oddiy kirishdan to'liq boshqaruv halqalarini o'rganishga o'tmoqda; agar sanoat jarayonini qo'llab-quvvatlovchi aktivlar ochiq yoki yomon himoyalangan bo'lsa, ularga OT tarmog'ini to'g'ridan-to'g'ri buzmasdan ham yo'l ochiq. Uskuna yetkazib beruvchilarining masofaviy ulanishlari — shunday yo'llardan biri.

MAQSAD

Uskunangizga xorijdan kim ulanayapti — bilasizmi?

YECHIM

Barcha masofaviy kanallar inventarizatsiyasi, kirishni faqat so'rov va tasdiq bo'yicha ochish, shaxsiy loginlar va ikki bosqichli autentifikatsiya, seanslarni yozib olish, yetkazib beruvchi shartnomasiga kirish qoidalari.

NATIJA

O'lchanadigan ko'rsatkichlar: doimiy ochiq kanallar, so'rov bo'yicha seanslar, shaxsiy login, yozib olingan seanslar.

Kimlar uchun

Bosh muhandis
Uskuna.

IT/xavfsizlik
Kirish.

Yetkazib beruvchi
Servis.

Ta'minot bo'limi
Shartnoma.

> Doimiy ochiq servis ulanishi — doimiy ochiq eshik.

QISQA FAKTLAR

24 kun
Zaiflik oshkor qilinganidan qurollangan eksploitgacha mediana (Dragos).[1]

Halqa
Hujumchilar butun boshqaruv halqalarini o'rganmoqda (Dragos 2026).[1]

PF–38
2026–2030 Kiberxavfsizlik strategiyasi (10.03.2026).[2]

Manbalar — oxirgi betda.

02 — Kontekst

Dunyoda va O'zbekistonda nima ma'lum

Xalqaro tahlil va rasmiy manbalar.

Fakt	Manba
Hujumchilar boshqaruv halqalarini o'rganmoqda; ochiq yoki zaif aktivlar orqali OT ga to'g'ridan-to'g'ri buzishsiz yo'l bor.[1]	Dragos 2026 Year in Review / blog
2026–2030 strategiya va yo'l xaritasi; 01.04.2026 dan tashkilotlar kiberxavfsizlikka mablag' ajratadi.[2]	PF–38 (spot.uz, norma.uz)

Bu raqamlarni qanday o'qish kerak

O'zbekiston korxonalari bo'yicha bu ko'rsatkich ochiq manbalarda topilmadi — dastlabki baholashda o'lchanadi.

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

03 — Muammo

Odatda nima topiladi

Odatdagi bo'shliqlar:

01
Doimiy ulanish
Servis kanali 24/7 ochiq.

02
Umumiy parol
Bir xil login barcha muhandislar uchun.

03
Jurnal yo'q
Ulanishlar yozilmaydi.

04
Shartnoma
Kirish qoidalari shartnomada yo'q.

Yo'qotishni qanday hisoblash mumkin

Ruxsatsiz o'zgarish	`jarayon xavfi`
Ma'lumot	`texnologik sir`
Hodisa	`to'xtash`
Javobgarlik	`kim nima qilgani noma'lum`

Formulalar namunaviy; aniq qiymat auditda o'lchanadi.

Rahbar o'ziga beradigan savollar

Barcha masofaviy kanallar ro'yxati bormi?

Kanallar faqat so'rov bo'yicha ochiladimi?

Har muhandisning shaxsiy logini bormi?

04 — Yechim arxitekturasi

Ulanishlar ro'yxati → so'rov bo'yicha kirish → yozib olish → shartnoma

Barcha masofaviy kanallar inventarizatsiyasi, kirishni faqat so'rov va tasdiq bo'yicha ochish, shaxsiy loginlar va ikki bosqichli autentifikatsiya, seanslarni yozib olish, yetkazib beruvchi shartnomasiga kirish qoidalari.

Foydalanuvchilar	Bosh muhandis · IT/xavfsizlik · Yetkazib beruvchi · Ta'minot bo'limi
Ro'yxat	Kanallar · Yetkazib beruvchi · Uskuna
Kirish	**So'rov** · **Tasdiq** · **Muddat**
Nazorat	**Shaxsiy login** · **2FA** · **Yozuv**
Shartnoma	Qoidalar · Javobgarlik · Audit
Integratsiya	1C · ESF / EDO · Datchik va PLC · Telegram ogohlantirish

Boshqaruv paneli

Masofaviy kanallar, ochiq seanslar, so'rovlar jurnali

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
Kanallar inventarizatsiyasi	Audit	◐ **Muhandislik imkoniyati**
So'rov bo'yicha kirish jarayoni	Muhandislik	◐ **Muhandislik imkoniyati**
Seanslarni yozish shlyuzi	Hamkor	○ **Ishlab chiqilmoqda**
Shartnoma bandlari shabloni	Ta'minot	◐ **Muhandislik imkoniyati**

● Tijoriy mavjud ◐ Muhandislik imkoniyati ○ Ishlab chiqilmoqda

Korxona tomonidan kerak

- Bosh muhandis
- Yetkazib beruvchilar ro'yxati
- Servis shartnomalari
- IT bo'limi

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
Kanallar auditi
Aktivlar va jarayonlar.

Natija: xavflar xaritasi.

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

Natija: birinchi natijalar.

2–3 oy
Barcha yetkazib beruvchilar
Butun korxona.

Natija: doimiy jarayon.

Doimiy
Qo'llab-quvvatlash
Oylik hisobot.

Natija: ochiq kanallar soni.

Muddatlar taxminiy; auditdan keyin aniqlanadi.

O'lchanadigan ko'rsatkichlar

Ko'rsatkich	Birlik	Manba
Doimiy ochiq kanallar	Soni	Audit
So'rov bo'yicha seanslar	%	Jurnal
Shaxsiy login	%	Audit
Yozib olingan seanslar	%	Shlyuz

07 — Keyingi qadam

Masofaviy kirish nazoratdami

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

01 Barcha masofaviy kanallar ro'yxati bormi?

02 Kanallar faqat so'rov bo'yicha ochiladimi?

03 Har muhandisning shaxsiy logini bormi?

04 Ikki bosqichli autentifikatsiya bormi?

05 Seanslar yoziladimi?

06 Shartnomada kirish qoidalari bormi?

07 Ishdan ketgan xodimlar kirishi yopiladimi?

08 Jurnal muntazam ko'riladimi?

09 Kiberxavfsizlik uchun mas'ul shaxs tayinlanganmi?

Masofaviy kirish auditi

Uskunalar yetkazib beruvchilari va xodimlarning masofaviy ulanishlari ro'yxatini tuzib, nazorat sxemasini taklif qilamiz.

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

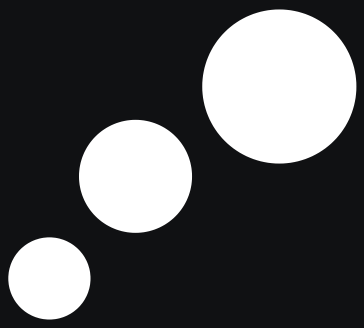
Natijada olasiz

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

Manbalar

1. Dragos 2026 OT/ICS Cybersecurity Year in Review (17.02.2026): 2025-yilda 119 ransomware guruhi 3 300 sanoat tashkilotiga ta'sir qilgan; sanoatga ransomware hujumlari +64%; qurbonlarning uchdan ikki qismidan ko'prog'i ishlab chiqarish; OT da ransomware o'rtacha 42 kun aniqlanmay qolgan, to'liq OT ko'rinishiga ega tashkilotlarda — 5 kun; oshkor qilishdan qurollangan eksploitgacha mediana 24 kun (controleng.com).
2. 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-03-UZ · 11.2026

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