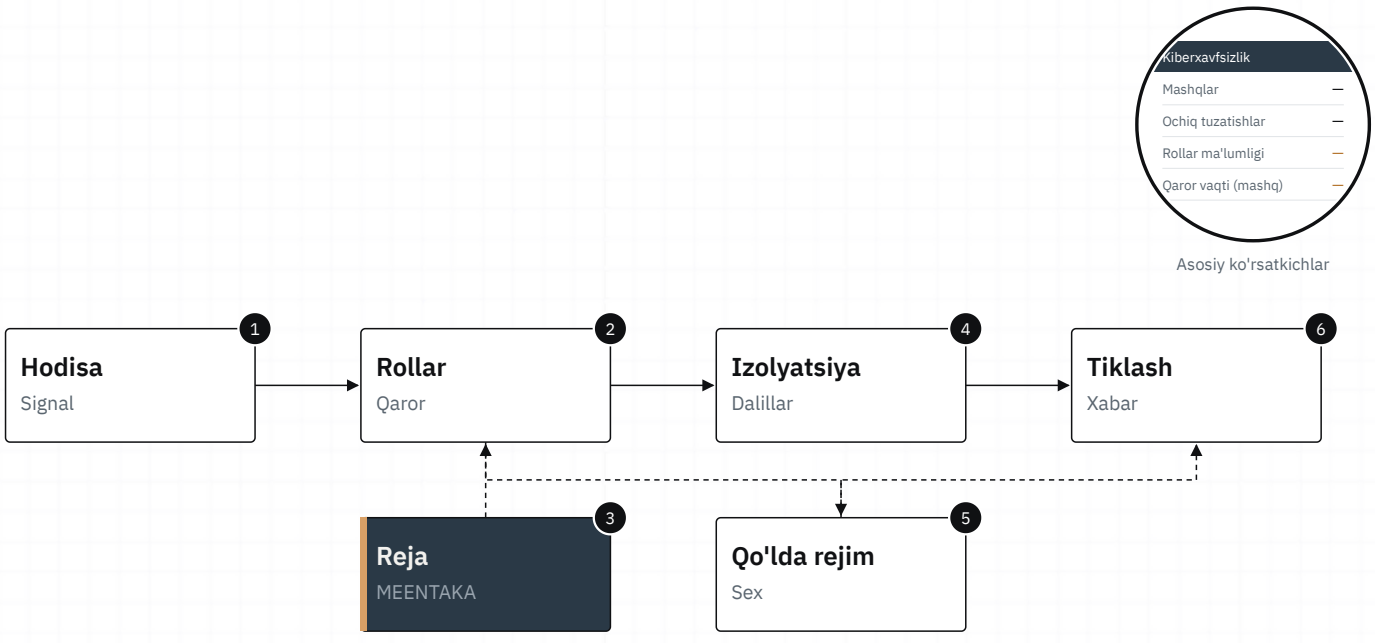
KIBERXAVFSIZLIK · KIBERXAVFSIZLIK · HODISAGA JAVOB

Kiberhodisa sodir bo'ldi: birinchi 24 soatda kim nima qiladi

Hodisaga javob rejasi bo'lmasa, birinchi soatlar vahima va noto'g'ri qarorlarga ketadi. Zavodda esa noto'g'ri qaror — jismoniy oqibat.



Hujjat turi	Kod	Til	Holat
Yechim hujjati	KX-09	O'zbekcha	Noyabr 2026

01 — Qisqacha

Ekranlarda talab xati. Liniyani to'xtatamizmi?

Dragos ishlab chiqarish va sanoat uchun asosiy beshta nazorat choralaridan biri sifatida jismoniy oqibatlarni hisobga oladigan OT/ICS ga xos hodisaga javob rejasini ko'rsatadi; ko'p tashkilotlar hodisa paytida aslida nima bo'lganini aniqlay olmaydi. Qonun MAI subyektlaridan hodisalarni vakolatli organga xabar qilishni talab qiladi.

MAQSAD

Ekranlarda talab xati. Liniyani to'xtatamizmi?

YECHIM

Hodisaga javob rejasi: rollar va aloqa ro'yxati, OT uchun xavfsiz to'xtatish/qo'lda rejim tartiblari, izolyatsiya va dalillarni saqlash, tashqi xabar berish; har yarim yilda stol-ustidagi mashq.

NATIJA

O'lchanadigan ko'rsatkichlar: mashqlar, ochiq tuzatishlar, rollar ma'lumligi, qaror vaqti (mashq).

Kimlar uchun

Bosh direktor
Qaror.

Bosh muhandis
Xavfsiz to'xtatish.

IT/xavfsizlik
Izolyatsiya.

Kommunikatsiya/
Xabar berish.

> Reja hodisa kuni yoziladimi — u kech.

QISQA FAKTLAR

42 kun

OT da ransomware o'rtacha aniqlanmay qolish vaqti (Dragos).[1]

5

Dragos tavsiya qilgan OT kiberxavfsizlik asosiy nazorat choralari.[1]

Xabar

MAI subyektlari hodisalarni xabar qilishi shart (O'RQ–764).[2]

Manbalar — oxirgi betda.

02 — Kontekst

Dunyoda va O'zbekistonda nima ma'lum

Xalqaro tahlil va qonun.

Fakt	Manba
Asosiy nazorat choralaridan biri — jismoniy oqibatlarni hisobga oluvchi ICS ga xos hodisaga javob rejasi; ko'p tashkilotlar hodisa sababini aniqlay olmaydi.[1]	Dragos 2026 (secureworld.io, controleng.com)
MAI operatorlari tarmoqlarini real vaqtda kuzatishi va kiberhodisalarni DXX ga darhol xabar qilishi kerak.[2]	O'RQ–764 sharhi (regulations.ai)

Bu raqamlarni qanday o'qish kerak

Xabar berish tartibi va muddatlari rasmiy hujjatlarda tekshirilishi kerak. MEENTAKA hodisani rasmiy tergov qilmaydi.

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

03 — Muammo

Birinchi soatlarda nima buziladi

Odatdagi xatolar:

01
Kim qaror qiladi
Rollar yozilmagan.

02
Izolyatsiya
Hamma narsa o'chiriladi — dalillar ham.

03
Jarayon
Liniya xavfsiz holatga keltirilmaydi.

04
Xabar
Kimga va qachon xabar berish noma'lum.

Yo'qotishni qanday hisoblash mumkin

Kechikkan qaror	`soat × zarar`
Dalillar	`sababni topa olmaslik`
Uskuna	`noto'g'ri to'xtatish`
Javobgarlik	`xabar bermaslik`

Formulalar namunaviy; aniq qiymat auditda o'lchanadi.

Rahbar o'ziga beradigan savollar

> Hodisaga javob rejasi yozilganmi?

> Kim qaror qilishi aniqmi?

> Liniyani xavfsiz to'xtatish tartibi bormi?

04 — Yechim arxitekturasi

Rollar → stsenariylar → stol-ustidagi mashq → yangilangan reja

Hodisaga javob rejasi: rollar va aloqa ro'yxati, OT uchun xavfsiz to'xtatish/qo'lda rejim tartiblari, izolyatsiya va dalillarni saqlash, tashqi xabar berish; har yarim yilda stol-ustidagi mashq.

Foydalanuvchilar	Bosh direktor · Bosh muhandis · IT/xavfsizlik · Kommunikatsiya/yurist
Rollar	Qaror · Texnik · Aloqa
Stsenariy	**Ransomware** · **Masofaviy kirish** · **Sizish**
Harakat	**Izolyatsiya** · **Qo'lda rejim** · **Dalillar**
Tiklash	Ketma-ketlik · Xabar · Saboqlar
Integratsiya	1C · ESF / EDO · Datchik va PLC · Telegram ogohlantirish

Boshqaruv paneli
Reja holati, oxirgi mashq, ochiq tuzatishlar

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
Hodisaga javob rejasi	OT/IT	◐ **Muhandislik imkoniyati**
Stol-ustidagi mashq	Yarim yillik	◐ **Muhandislik imkoniyati**
Aloqa va xabar shablonlari	Hujjatlar	◐ **Muhandislik imkoniyati**
Tergov va kriminalistika	Ruxsat etilgan hamkor	○ **Ishlab chiqilmoqda**

● Tijoriy mavjud ◐ Muhandislik imkoniyati ○ Ishlab chiqilmoqda

Korxona tomonidan kerak

- Rahbariyat
- Bosh muhandis
- IT
- Yurist

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
Reja loyihasi
Aktivlar va jarayonlar.

Natija: xavflar xaritasi.

30 kun
Birinchi mashq
Bitta sex yoki tizim, 30 kun.

Natija: birinchi natijalar.

2–3 oy
Muntazam mashqlar
Butun korxona.

Natija: doimiy jarayon.

Doimiy
Qo'llab-quvvatlash
Oylik hisobot.

Natija: tuzatishlar ijrosi.

Muddatlar taxminiy; auditdan keyin aniqlanadi.

O'lchanadigan ko'rsatkichlar

Ko'rsatkich	Birlik	Manba
Mashqlar	Soni/yil	Jurnal
Ochiq tuzatishlar	Soni	Reja
Rollar ma'lumligi	%	Mashq
Qaror vaqti (mashq)	Daqiqa	Mashq

07 — Keyingi qadam

Hodisa kuni nima qilishni bilasizmi

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

01 Hodisaga javob rejasi yozilganmi?

02 Kim qaror qilishi aniqmi?

03 Liniyani xavfsiz to'xtatish tartibi bormi?

04 Qo'lda boshqaruv rejimi bormi?

05 Dalillarni saqlash tartibi bormi?

06 Kimga xabar berish ma'lummi?

07 Oxirgi mashq qachon bo'lgan?

08 Tashqi hamkor tayinlanganmi?

09 Kiberxavfsizlik uchun mas'ul shaxs tayinlanganmi?

Hodisa mashqi

Rahbariyat va muhandislar bilan "ransomware zavodda" stol-ustidagi mashqini o'tkazamiz.

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. regulations.ai: O'RQ–764 — MAI operatorlari real vaqtda monitoring va hodisalarni darhol xabar qilish.
3. "Kiberxavfsizlik to'g'risida"gi Qonun O'RQ–764 (15.04.2022, lex.uz): muhim axborot infratuzilmasi (MAI) — strategik va ijtimoiy-iqtisodiy ahamiyatga ega avtomatlashtirilgan boshqaruv tizimlari, axborot tizimlari, tarmoq va texnologik jarayonlar resurslari majmui; MAI subyektlari — bunday obyektlarga egalik qiluvchi davlat organlari va yuridik shaxslar; DXX MAI obyektlarining yagona reyestrini yuritadi (kun.uz).

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-09-UZ · 11.2026

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