

Yuristning raqamli ish joyi va kiber-gigiyena

Operatsion tizim va fayllarni boshqarish asoslari. Parol menejerlari, ikki bosqichli autentifikatsiya (2FA). Zaxira nusxa olish. Fayl va qurilmalarni shifrlash. Xavfsiz ish muhitini sozlash.

Reja

1. Yuristning raqamli ish joyi: tushuncha, ahamiyati va asosiy tahdidlar
2. Operatsion tizim va fayllarni boshqarish asoslari
3. Parollar va parol menejerlari
4. Ikki bosqichli autentifikatsiya (2FA)
5. Zaxira nusxa olish
6. Fayl va qurilmalarni shifrlash
7. Xavfsiz ish muhitini sozlash
8. Huquqiy jihatlar va yuristning kasbiy majburiyatlari

Ma'ruzaning maqsadi

- Talabalarda yuridik faoliyatda raqamli xavfsizlikning ahamiyati haqida tushuncha shakllantirish;
- operatsion tizim, fayl tizimi va hujjatlarni tartibli saqlash ko'nikmalarini berish;
- parol menejeri, 2FA, zaxira nusxa va shifrlash vositalaridan amalda foydalanishni o'rgatish;
- xavfsiz ish muhitini mustaqil sozlash uchun aniq yo'riqnoma (chek-list) bilan ta'minlash.

Tayanch tushunchalar: kiber-gigiyena, operatsion tizim, fayl tizimi, parol menejeri, 2FA, TOTP, FIDO2, passkey, zaxira nusxa, 3-2-1 qoidasi, shifrlash, BitLocker, FileVault, VeraCrypt, fishing, to'lov talab qiluvchi dastur (ransomware), advokatlik siri.

Kirish

Bugungi kunda yuristning ish faoliyati deyarli to'liq raqamli muhitda kechadi: da'vo arizalari va shartnomalar kompyuterda tayyorlanadi, mijozlar bilan yozishmalar elektron pochta va messenjerlar orqali olib boriladi, sud hujjatlari elektron tizimlar orqali yuboriladi, ishlarga oid dalillar esa fayl, rasm va audio yozuvlar ko'rinishida saqlanadi. Shu bois yuristning kompyuteri, telefoni va bulutli hisoblari uning «raqamli ish joyi»ga aylangan.

Yurist boshqa ko'plab kasb egalaridan farqli ravishda o'ziga ishonib topshirilgan ma'lumotlar maxfiyligi uchun alohida javobgar. Mijoz sirlari, shaxsga doir ma'lumotlar, tijorat siri va hali e'lon qilinmagan huquqiy pozitsiya sizib chiqsa, bu nafaqat moddiy zarar, balki kasbiy obro'ning yo'qolishi, intizomiy va hatto jinoiy javobgarlikka olib kelishi mumkin.

«Kiber-gigiyena» atamasi shaxsiy gigiyena bilan o'xshatish asosida kiritilgan: qo'l yuvish kasallikning ko'p qismining oldini olgani kabi, oddiy, ammo muntazam bajariladigan raqamli odatlar (yangilanishlar, kuchli parollar, 2FA, zaxira nusxa, shifrlash) kiberhujumlarning katta qismidan himoya qiladi. Ushbu ma'ruzada ana shu odatlar tizimli ko'rib chiqiladi.

1. Yuristning raqamli ish joyi: tushuncha va asosiy tahdidlar

Yuristning raqamli ish joyi deganda u kasbiy faoliyatida foydalanadigan barcha raqamli resurslar majmui tushuniladi. Uning tarkibiy qismlari quyidagilar:

- **Qurilmalar:** ish kompyuteri yoki noutbuk, smartfon, planshet, tashqi disklar va fleshkalar;
- **Dasturiy ta'minot:** operatsion tizim, ofis dasturlari, brauzer, PDF vositalari, huquqiy axborot tizimlari (masalan, Lex.uz), elektron raqamli imzo (ERI) dasturlari;
- **Hisoblar va xizmatlar:** elektron pochta, bulutli saqlash joylari, messenjerlar, davlat elektron xizmatlari portallari, sudlarning elektron tizimlari;
- **Ma'lumotlar:** mijozlar ishi bo'yicha hujjatlar, yozishmalar, kontaktlar, kalendar, hisob-kitob ma'lumotlari;
- **Tarmoq muhiti:** ofis yoki uy Wi-Fi tarmog'i, mobil internet, ommaviy tarmoqlar.

Yuristlarga qarshi asosiy tahdidlar

Tahdid	Mazmuni	Yurist uchun oqibati
Fishing	Sud, bank, mijoz yoki davlat organi nomidan soxta xat yoki havola	Parol va hisoblarning o'g'irlanishi, zararli dastur o'rnatilishi
To'lov talab qiluvchi dastur (ransomware)	Fayllarni shifrlab, ochish uchun to'lov talab qiladi	Ish hujjatlarining yo'qolishi, muddatlarni o'tkazib yuborish

Tahdid	Mazmuni	Yurist uchun oqibati
Qurilmaning yo'qolishi yoki o'g'irlanishi	Noutbuk, telefon yoki fleshka begona qo'lga tushadi	Mijoz sirlarining oshkor bo'lishi
Kuchsiz yoki takroriy parollar	Bir parol bir nechta xizmatda ishlatiladi	Bir xizmatdan sizgan parol bilan pochtaga kirish
Inson xatosi	Xatni noto'g'ri adresatga yuborish, faylni o'chirib yuborish	Maxfiylik buzilishi, ma'lumot yo'qolishi
Ijtimoiy muhandislik	Telefon yoki messenjer orqali ishonchni qozonib ma'lumot olish	Pul mablag'lari va ma'lumotlarning yo'qotilishi

Statistik ma'lumotlar shuni ko'rsatadiki, muvaffaqiyatli hujumlarning aksariyati murakkab texnik usullar bilan emas, balki inson omili — ishonuvchanlik, shoshqaloqlik va e'tiborsizlik orqali amalga oshiriladi. Shu sababli kiber-gigiyena birinchi navbatda odatlar va intizom masalasidir.

Asosiy tamoyil: «Mijozning ma'lumoti — mijozning mulki, yurist esa uning qo'riqchisi». Raqamli xavfsizlik yuristning ixtiyoriy qo'shimcha ishi emas, balki kasbiy majburiyatining ajralmas qismidir.

2. Operatsion tizim va fayllarni boshqarish asoslari

2.1. Operatsion tizim va uning vazifalari

Operatsion tizim (OT) — kompyuterning apparat qismi va foydalanuvchi dasturlari o'rtasidagi vositachi dasturiy ta'minot. Eng keng tarqalgan OTlar: Windows, macOS, Linux (kompyuterlar uchun), Android va iOS (mobil qurilmalar uchun). OT xotira va protsessor resurslarini taqsimlaydi, fayllarni saqlaydi, foydalanuvchilarni tanib oladi va ularning huquqlarini cheklaydi, tarmoq bilan ishlashni ta'minlaydi.

Xavfsizlik nuqtai nazaridan OT bilan bog'liq eng muhim qoidalar:

- **Litsenziyali va qo'llab-quvvatlanadigan versiyadan foydalaning.** Ishlab chiqaruvchi tomonidan qo'llab-quvvatlanishi to'xtatilgan tizimlar (masalan, Windows 7; Windows 10 ning asosiy qo'llab-quvvatlanishi 2025-yil 14-oktyabrda tugagan) xavfsizlik tuzatishlarini olmaydi.
- **Avtomatik yangilanishlarni yoqing.** Yangilanishlarning katta qismi aniqlangan zaifliklarni yopadi; ularni kechiktirish ochiq eshikni qoldirish bilan barobar.
- **Administrator va oddiy hisobni ajrating.** Kundalik ishni standart (cheklangan huquqli) hisobda bajaring; dastur o'rnatish kerak bo'lgandagina administrator parolini kiring.
- **Faqat rasmiy manbalardan dastur o'rnatish** (ishlab chiqaruvchi sayti, Microsoft Store, App Store, Google Play). «Kreklangan» dasturlar zararli kodning asosiy tarqalish yo'llaridan biri.

- **O'rnatilgan himoyadan foydalaning:** Windows Defender (Microsoft Defender), tarmoqlararo ekran (firewall), macOS dagi Gatekeeper va XProtect.

2.2. Fayl tizimi: asosiy tushunchalar

Fayl — nomga ega bo'lgan, diskda saqlanadigan ma'lumotlar to'plami. Fayl nomi odatda ikki qismdan iborat: nom va kengaytma (masalan, *Shartnoma_2026.docx*). Kengaytma fayl turini va uni qaysi dastur ochishini ko'rsatadi. Papka (katalog) — fayllarni guruhlash uchun konteyner. Fayl manzili (yo'l, path) uning papkalar ierarxiyasidagi o'rnini bildiradi, masalan: *D:\Ishlar\2026\045_Karimov_mehnat_nizosi\Da'vo_arizasi_v3.docx*.

Xavfsizlik uchun muhim amaliy maslahat: **fayl kengaytmalarini doim ko'rinadigan qilib qo'ying** (Windows: Explorer → Ko'rinish → «Fayl nomlari kengaytmalari»). Shunda *Hujjat.pdf.exe* kabi niqoblangan zararli faylni darhol payqaysiz.

2.3. Yuridik hujjatlarni tartibli saqlash

Tartibsiz saqlangan fayllar nafaqat vaqt yo'qotishga, balki xavfsizlik xatolariga ham sabab bo'ladi: noto'g'ri versiyani yuborish, boshqa mijozning hujjatini ilova qilib yuborish va hokazo. Tavsiya etiladigan papka tuzilmasi:

Daraja	Namuna	Izoh
1. Yil yoki faoliyat turi	Ishlar_2026 / Maslahatlar / Shablonlar	Umumiy bo'linish
2. Ish (mijoz)	045_Karimov_A_mehnat_nizosi	Raqam + mijoz + ish mazmuni
3. Ish ichidagi bo'limlar	01_Mijoz_hujjatlari, 02_Dalillar, 03_Protsessual_hujjatlar, 04_Yozishmalar, 05_Sud_qarorlari	Raqamlash tartibni saqlaydi

Fayllarni nomlash qoidalari:

- sanani ISO formatida yozing: *2026-10-15_Apellyatsiya_shikoyati_v2.docx* — fayllar xronologik tartibda saralanadi;
- versiyani aniq ko'rsating (*v1*, *v2*, *final*), «yangi», «yangi2», «eng_so'nggi» kabi nomlardan qoching;
- bo'sh joy va maxsus belgilar o'rniga pastki chiziq () ishlating;
- fayl nomiga maxfiy ma'lumot (pasport raqami, JShShIR va h.k.) yozmang — nomlar ko'pincha shifrlanmaydi va jurnallarda qoladi.

2.4. Metama'lumotlar va hujjatni «tozalash»

Word, PDF va rasm fayllari ichida ko'zga ko'rinmaydigan qo'shimcha ma'lumotlar — muallif ismi, tahrir tarixi, izohlar, «Track Changes» (tuzatishlarni kuzatish) qoldiqlari, rasmlarda esa GPS koordinatalari saqlanadi. Qarama-qarshi tomonga yoki sudga yuboriladigan hujjatdan bu ma'lumotlar olib tashlanishi shart. Word dasturida: *Fayl* → *Ma'lumot* → *Muammolarni tekshirish* → *Hujjatni tekshirish* (*Inspect Document*). Eng ishonchli usul — yakuniy variantni PDF formatida saqlash

va PDFning xususiyatlarini tekshirish.

2.5. Faylni o'chirish xususiyatlari

Faylni «Savat»ga tashlash yoki hatto savatni bo'shatish ma'lumotni diskdan to'liq yo'q qilmaydi — maxsus dasturlar bilan uni tiklash mumkin. Shuning uchun maxfiy ma'lumotli qurilmani sotish, topshirish yoki utilizatsiya qilishdan oldin diskni to'liq shifrlash va zavod sozlamalariga qaytarish yoki maxsus o'chirish vositalaridan foydalanish lozim. Diskni shifrlangan qurilmada shifrlash kalitini yo'q qilish ma'lumotni amalda tiklab bo'lmaydigan holga keltiradi.

3. Parollar va parol menejerlari

3.1. Kuchli parol nima?

Zamonaviy tavsiyalarga (jumladan, AQSh Milliy standartlar va texnologiyalar instituti — NIST SP 800-63B) ko'ra, parolning kuchliligini birinchi navbatda uning **uzunligi** va **noyoblighi** belgilaydi, murakkab belgilar aralashmasi esa ikkinchi darajali. Parolni muntazam majburiy almashtirish o'rniga, u sizib chiqqanda yoki shubha tug'ilganda darhol almashtirish tavsiya etiladi.

- kamida 12-16 belgi; eng yaxshisi — bir nechta tasodifiy so'zdan iborat «parol-ibora» (masalan, *qovun-daftar-yomg'ir-sakkiz*);
- har bir xizmat uchun alohida parol — bitta parolni takror ishlatish eng xavfli odatlardan biri;
- shaxsiy ma'lumotlar (tug'ilgan sana, farzand ismi, telefon raqami) va «123456», «qwerty», «parol» kabi keng tarqalgan birikmalardan foydalanmaslik;
- parolni qog'ozga yozib monitorga yopishtirmaslik, messenger yoki pochta orqali yubormaslik.

O'rtacha foydalanuvchida 80-100 dan ortiq onlayn hisob bo'ladi. Ularning har biri uchun uzun va noyob parolni yodda saqlash amalda imkonsiz. Bu muammoning yechimi — parol menejeri.

3.2. Parol menejeri

Parol menejeri — barcha parollarni shifrlangan «seyf»da saqlaydigan dastur. Foydalanuvchi faqat bitta kuchli **bosh parolni** (master password) eslab qoladi; qolgan parollarni dastur o'zi yaratadi, saqlaydi va saytlarga avtomatik kiritadi. Muhim afzalligi: parol menejeri parolni faqat haqiqiy sayt manziliga kiritadi, shu sababli soxta (fishing) saytni ham bilvosita aniqlashga yordam beradi.

Dastur	Turi	Xususiyati
Bitwarden	Bulutli, ochiq kodli	Bepul tarif mavjud, barcha platformalarda ishlaydi
KeePassXC	Lokal (oflayn), ochiq kodli	Baza faylda saqlanadi, bulutga bog'liq emas
1Password	Bulutli, pullik	Jamoa (yuridik firma) uchun qulay boshqaruv

Dastur	Turi	Xususiyati
Brauzer va OT menejerlari	O'rnatilgan (Google, Apple, Microsoft)	Qulay, ammo hisob xavfsizligiga bog'liq

Parol menejeridan foydalanish tartibi:

- ishonchli parol menejerini rasmiy saytdan o'rnatish va uzun bosh parol-ibora yaratish;
- parol menejeri hisobiga albatta 2FA yoqish;
- tiklash kodlari (recovery kit) ni chop etib, xavfsiz joyda (masalan, seyfa) saqlash;
- avval eng muhim hisoblar — elektron pochta, bank, bulutli saqlash va ish tizimlari parollarini yangi, noyob parollarga almashtirish;
- parol menejeridagi «xavfsizlik hisoboti» yordamida takroriy va kuchsiz parollarni bosqichma-bosqich almashtirish.

Elektron pochta — «asosiy kalit». Deyarli barcha xizmatlarda parolni tiklash pochta orqali amalga oshiriladi. Shu sababli pochta paroli eng kuchli va noyob bo'lishi, unga esa 2FA albatta yoqilishi kerak.

4. Ikki bosqichli autentifikatsiya (2FA)

Autentifikatsiya — foydalanuvchining haqiqatan ham o'zi ekanligini tasdiqlash jarayoni. U uch turdagi omilga asoslanadi:

- **bilim omili** — siz biladigan narsa (parol, PIN-kod);
- **egallik omili** — sizda mavjud narsa (telefon, apparat kaliti, smart-karta);
- **biometrik omil** — sizning o'zingizga xos belgi (barmoq izi, yuz tasviri).

Ikki bosqichli (ikki omilli) autentifikatsiya — tizimga kirishda ikki xil omilni talab qilish. Parol o'g'irlangan taqdirda ham, jinoyatchi ikkinchi omilsiz hisobga kira olmaydi. Microsoft ma'lumotlariga ko'ra, ko'p omilli autentifikatsiya hisoblarni avtomatlashtirilgan buzish urinishlarining 99 foizdan ortig'ini to'xtatadi.

4.1. 2FA usullari va ularning ishonchliligi

Usul	Qanday ishlaydi	Ishonchlilik
SMS-kod	Telefon raqamiga bir martalik kod keladi	Past-o'rta: SIM-kartani almashtirish va SMS ushlab qolish xavfi
Autentifikator ilova (TOTP)	Google Authenticator, Microsoft Authenticator, Aegis, 2FAS — har 30 soniyada yangi kod	Yaxshi; oflayn ishlaydi
Push-tasdiqlash	Telefondagi ilovada «Ha, bu menman» tugmasini bosish	Yaxshi, ammo «charchatish hujumi»dan ehtiyot bo'ling
Apparat kaliti (FIDO2/U2F)	YubiKey kabi USB/NFC kalit	Juda yuqori; fishingga chidamli

Usul	Qanday ishlaydi	Ishonchlilik
Passkey (kirish kaliti)	Parolsiz kirish: qurilma va biometriya orqali tasdiqlash	Juda yuqori; fishingga chidamli

4.2. 2FA ni yoqish tartibi

- hisob sozlamalaridagi «Xavfsizlik» bo'limiga kiring va «Ikki bosqichli tasdiqlash» (2-Step Verification) ni toping;
- imkon bo'lsa SMS o'rniga autentifikator ilovani yoki apparat kalitni tanlang;
- ekrandagi QR-kodni ilova bilan skanerlang va ko'rsatilgan kodni kiriting;
- **zaxira (tiklash) kodlarini** albatta saqlab qo'ying — telefon yo'qolganda hisobga faqat ular orqali kirish mumkin;
- birinchi navbatda 2FA ni elektron pochta, parol menejeri, bulutli saqlash, messenjerlar (Telegram — «Bulutli parol», WhatsApp — «Ikki bosqichli tasdiqlash»), bank va davlat xizmatlari hisoblarida yoqing.

Hech qachon 2FA kodini hech kimga aytmang — na «bank xodimi»ga, na «sud kotibi»ga, na «Telegram qo'llab-quvvatlash xizmati»ga. Haqiqiy tashkilotlar bunday kodni hech qachon so'ramaydi. Kodni so'rash — firibgarlikning aniq belgisi.

5. Zaxira nusxa olish

Zaxira nusxa (backup) — ma'lumotlarning asl nusxasi yo'qolgan, buzilgan yoki shifrlangan holatda ularni tiklash uchun boshqa joyda saqlanadigan nusxasi. Disk ishdan chiqishi, noutbukning o'g'irlanishi, to'lov talab qiluvchi dastur hujumi yoki tasodifan o'chirib yuborish — bularning barchasida yagona najot zaxira nusxa hisoblanadi. Yurist uchun bu ish hujjatlari va protsessual muddatlarni saqlab qolish masalasidir.

5.1. «3-2-1» qoidasi

- **3** — ma'lumotlarning kamida uchta nusxasi (asl nusxa + ikkita zaxira);
- **2** — kamida ikki xil turdagi saqlash vositasida (masalan, kompyuter diski va tashqi disk);
- **1** — bitta nusxa boshqa joyda (ofisdan tashqarida yoki bulutda) saqlanadi.

To'lov talab qiluvchi dasturlar kompyuterga ulangan disklarni ham shifrlashi mumkinligi sababli, zamonaviy amaliyotda bitta nusxani **oflayn** (nusxa olingandan keyin uzib qo'yiladigan disk) yoki o'zgartirib bo'lmaydigan (immutable) holatda saqlash tavsiya etiladi. Bu qoida ba'zan «3-2-1-1-0» deb ham ataladi: oxirgi «0» — tiklash sinovida xatolar soni nol bo'lishi kerakligini bildiradi.

5.2. Zaxira nusxa turlari

Turi	Mazmuni	Afzalligi / kamchiligi
To'liq (full)	Barcha tanlangan ma'lumotlar to'liq nusxalanadi	Tiklash oson; ko'p joy va vaqt talab qiladi

Turi	Mazmuni	Afzalligi / kamchiligi
Inkremental	Oxirgi istalgan zaxiradan keyin o'zgargan fayllar	Tez va ixcham; tiklash zanjiriga bog'liq
Differensial	Oxirgi to'liq zaxiradan keyin o'zgargan fayllar	O'rtacha hajm; tiklash nisbatan oson
Sinxronizatsiya	Papkani bulut bilan doimiy moslashtirish (OneDrive, Google Drive)	Qulay, ammo o'chirish va shifrlash ham sinxronlanadi — to'liq zaxira emas!

5.3. Amaliy vositalar

- **Windows:** «Fayllar tarixi» (File History), «Windows Backup», OneDrive dagi «Versiyalar tarixi»;
- **macOS:** Time Machine (tashqi diskka avtomatik zaxira);
- **Telefon:** iCloud yoki Google hisobi orqali zaxira; WhatsApp va Telegram yozishmalari uchun alohida sozlamalar;
- **Bulut:** tanlangan bulutli xizmatda 2FA yoqilgan bo'lishi va iloji bo'lsa, maxfiy fayllar yuklashdan oldin shifrlanishi kerak.

Eng muhim qoida: **tekshirilmagan zaxira — zaxira emas**. Kamida oyiga bir marta bir nechta faylni zaxiradan tiklab ko'ring. Zaxira jadvalini avtomatlashtiring (masalan, har kuni kechqurun yoki har juma kuni) — qo'lda bajariladigan ishlar albatta unutiladi.

6. Fayl va qurilmalarni shifrlash

Shifrlash — ma'lumotni maxsus algoritm va kalit yordamida begona shaxs o'qiy olmaydigan ko'rinishga keltirish. Kalitga ega bo'lgan shaxsgina uni asl holatiga qaytara oladi. Zamonaviy standart algoritm — AES (Advanced Encryption Standard), odatda 256 bitli kalit bilan qo'llaniladi. To'g'ri sozlangan shifrlashni amaldagi kompyuter quvvati bilan «buzib» bo'lmaydi — shu sababli eng zaif nuqta odatda parol hisoblanadi.

6.1. Shifrlash turlari

- **«Tinch holatdagi» ma'lumotlarni shifrlash (at rest)** — diskdagi, fleshkadagi, bulutdagi fayllar;
- **«Harakatdagi» ma'lumotlarni shifrlash (in transit)** — tarmoq orqali uzatilayotgan ma'lumotlar (HTTPS, VPN);
- **Uchdan-uchgacha shifrlash (end-to-end, E2EE)** — xabarni faqat jo'natuvchi va qabul qiluvchi o'qiy oladi, xizmat ko'rsatuvchi ham o'qiy olmaydi (Signal, WhatsApp; Telegramda faqat «maxfiy chat» rejimida).

6.2. To'liq diskni shifrlash

Platforma	Vosita	Qanday yoqiladi
Windows Pro / Enterprise	BitLocker	Boshqaruv paneli → BitLocker disk shifrlash → Yoqish

Platforma	Vosita	Qanday yoqiladi
Windows Home	Qurilmani shifrlash (Device Encryption)	Sozlamalar → Maxfiylik va xavfsizlik → Qurilmani shifrlash
macOS	FileVault	Tizim sozlamalari → Maxfiylik va xavfsizlik → FileVault
Linux	LUKS	Odatda OT o'rnatish paytida tanlanadi
iPhone / Android	O'rnatilgan shifrlash	Ekran qulfi (PIN-kod yoki parol) o'rnatilganda avtomatik faollashadi

Diskni shifrlash noutbuk yoki telefon yo'qolgan taqdirda undagi ma'lumotlarni himoya qiladi. **Diqqat:** BitLocker yoki FileVault tiklash kalitini (recovery key) albatta xavfsiz joyda saqlang — u yo'qolsa, o'z ma'lumotlaringizga ham kira olmay qolasiz.

6.3. Alohida fayl, arxiv va tashuvchilarni shifrlash

- **VeraCrypt** — bepul, ochiq kodli dastur; shifrlangan «konteyner» (virtual disk) yoki butun fleshkani shifrlash uchun;
- **BitLocker To Go** — Windows da USB-fleshka va tashqi disklarni shifrlash;
- **7-Zip** — arxivni AES-256 bilan parol orqali shifrlash («Fayl nomlarini shifrlash» belgisini qo'yish kerak); mijozga maxfiy fayl yuborishda qulay;
- **PDF va Office hujjatlarini parol bilan himoyalash** — «Hujjatni himoyalash → Parol bilan shifrlash» funksiyasi.

Oltin qoida: shifrlangan fayl va uning paroli hech qachon bitta kanal orqali yuborilmaydi. Masalan, arxiv elektron pochta orqali yuborilsa, parol telefon qo'ng'irog'i yoki SMS orqali alohida xabar qilinadi.

7. Xavfsiz ish muhitini sozlash

Yuqorida ko'rib chiqilgan vositalar bir-birini to'ldirgandagina samarali bo'ladi. Quyida yuristning ish joyini xavfsiz sozlash bo'yicha amaliy chek-list keltirilgan.

7.1. Qurilma darajasida

- OT va barcha dasturlarning avtomatik yangilanishi yoqilgan;
- kirish uchun kuchli parol/PIN va biometriya; ekran 5 daqiqa harakatsizlikdan keyin avtomatik qulflanadi; ish joyidan ketayotganda **Win + L** (macOS: Ctrl + Cmd + Q) bilan qulflash odatiy holga aylangan;
- to'liq disk shifrlash (BitLocker / FileVault) yoqilgan, tiklash kaliti xavfsiz saqlangan;
- antivirus (Microsoft Defender yoki boshqa ishonchli dastur) va tarmoqlararo ekran faol;
- kundalik ish administrator bo'lmagan hisobdan bajariladi;
- «Qurilmamni topish» (Find My Device / Find My) funksiyasi yoqilgan — masofadan qulflash va o'chirish imkoniyati uchun;

- noutbukda ekranga maxfiylik filtri (privacy filter) — ommaviy joylarda ishlash uchun.

7.2. Tarmoq darajasida

- router zavod parolini almashtirish, WPA2/WPA3 shifrlashni yoqish, routerning dasturiy ta'minotini yangilash;
- mehmonlar uchun alohida Wi-Fi tarmog'i;
- ommaviy Wi-Fi (kafe, aeroport, mehmonxona) da maxfiy ishlar bilan shug'ullanmaslik yoki ishonchli VPN dan foydalanish; muqobil — telefon orqali mobil internet;
- brauzer manzil satrida HTTPS va to'g'ri domen nomini tekshirish.

7.3. Hisoblar va ma'lumotlar darajasida

- parol menejeri + barcha muhim hisoblarda 2FA;
- ish va shaxsiy hisoblarni ajratish (alohida pochta, iloji bo'lsa alohida brauzer profili);
- «3-2-1» qoidasi bo'yicha avtomatlashtirilgan zaxira nusxa va uning muntazam tekshiruvi;
- maxfiy hujjatlarni yuborishda shifrlash va adresatni ikki marta tekshirish;
- bulutli hujjatlarga «havola orqali hamma uchun ochiq» ruxsatini bermaslik, ishlar tugagach ruxsatlarni bekor qilish.

7.4. Xulq-atvor darajasida: fishingni tanib olish

- shoshiltiruvchi ohang («24 soat ichida javob bermasangiz...», «hisobingiz bloklanadi»);
- jo'natuvchi manzilidagi g'alati domen (*sud-uz.com*, *lex-uz.net* kabi o'xshatmalar);
- kutilmagan ilova (ayniqsa .zip, .exe, .scr, .js, .html, makroli .docm/.xlsm fayllar);
- pul o'tkazish yoki bank rekvizitlarini o'zgartirish talabi — har doim ma'lum telefon raqami orqali qayta tasdiqlang;
- shubhali xat haqida darhol mas'ul xodim yoki IT mutaxassisiga xabar bering, havolani bosmang.

7.5. Insident yuz berganda

Agar hisob buzilgan, qurilma yo'qolgan yoki zararli dastur yuqtirilgan bo'lsa: (1) qurilmani tarmoqdan uzing; (2) boshqa, toza qurilmadan muhim hisoblar parollarini almashtiring va barcha seanslardan chiqing; (3) yo'qolgan qurilmani masofadan qulflang yoki tozalang; (4) bankni va kerak bo'lsa mijozlarni xabardor qiling; (5) hodisani hujjatlashtiring va qonunchilikda belgilangan hollarda vakolatli organlarga xabar bering; (6) ma'lumotlarni zaxira nusxadan tiklang.

8. Huquqiy jihatlar va yuristning kasbiy majburiyatlari

Kiber-gigiyena yurist uchun nafaqat texnik, balki huquqiy talabdir. O'zbekiston Respublikasida bu sohani tartibga soluvchi asosiy hujjatlar:

- **«Shaxsga doir ma'lumotlar to'g'risida»gi Qonun (2019)** — shaxsga doir ma'lumotlarni qayta ishlovchi shaxsning ularni himoya qilish, maxfiyligini ta'minlash va noqonuniy foydalanishdan saqlash majburiyatlarini belgilaydi;
- **«Kiberxavfsizlik to'g'risida»gi Qonun (2022)** — kiberxavfsizlikni ta'minlash sohasidagi asosiy tushunchalar, subyektlar va kiberhodisalarga javob berish tartibini belgilaydi;
- **«Advokatura to'g'risida»gi Qonun** va advokatlik kasbiy odob qoidalarini — advokatlik sirini saqlash majburiyati; ushbu majburiyat elektron shakldagi ma'lumotlarga ham to'liq tatbiq etiladi;
- **«Elektron hujjat aylanishi to'g'risida»** va **«Elektron raqamli imzo to'g'risida»**gi qonunlar — elektron hujjatlar va ERI kalitlaridan foydalanish tartibi.

Xalqaro amaliyotda ham yuristning texnologik kompetensiyasi kasbiy majburiyat sifatida e'tirof etilgan. Masalan, Amerika advokatlar assotsiatsiyasining (ABA) Model qoidalariga ko'ra, advokat foydalanayotgan texnologiyalarning foyda va xavflaridan xabardor bo'lishi hamda mijoz ma'lumotlarini ruxsatsiz oshkor qilinishining oldini olish uchun oqilona choralar ko'rishi shart.

ERI (elektron raqamli imzo) kaliti — yuristning «raqamli muhri». Uni boshqa shaxsga bermang, kompyuterda ochiq papkada saqlamang va kalit parolini hech kimga aytmang. ERI orqali imzolangan hujjat qog'ozdagi imzo bilan teng yuridik kuchga ega.

Xulosa

Yuristning raqamli ish joyi — bu uning ofisi, arxivi va seyfi. Raqamli xavfsizlikning asosiy qismi qimmat texnologiyalarni emas, balki oddiy, ammo izchil bajariladigan odatlarni talab qiladi:

- tizim va dasturlarni yangilab turish, fayllarni tartibli saqlash;
- har bir hisob uchun noyob parol va ularni parol menejerida saqlash;
- muhim hisoblarda 2FA (iloji bo'lsa — apparat kalit yoki passkey);
- «3-2-1» qoidasi bo'yicha avtomatik va tekshirilgan zaxira nusxa;
- qurilma, tashuvchi va maxfiy fayllarni shifrlash;
- fishing va ijtimoiy muhandislikka nisbatan doimiy hushyorlik.

Bu odatlar mijoz ishonchini, kasbiy obro'ni va yuristning o'zini huquqiy javobgarlikdan himoya qiladi.

Nazorat savollari

- 1 «Yuristning raqamli ish joyi» tushunchasiga qanday elementlar kiradi?
- 2 Nima uchun operatsion tizimni yangilab turish xavfsizlik uchun muhim?
- 3 Fayl kengaytmalarini ko'rsatish qanday xavfdan himoya qiladi?
- 4 Hujjat metama'lumotlari nima va ularni qachon tozalash kerak?
- 5 Kuchli parolning asosiy mezonlari qanday? Parol-ibora nima?
- 6 Parol menejeri qanday ishlaydi va uning afzalliklari nimada?

- 7 Autentifikatsiya omillarining qanday turlari mavjud?
- 8 Nima uchun SMS-kod 2FA ning eng zaif usuli hisoblanadi?
- 9 «3-2-1» qoidasining mazmunini tushuntiring.
- 10 Sinxronizatsiya nega to'liq zaxira nusxa o'rnini bosa olmaydi?
- 11 «Tinch holatdagi» va «harakatdagi» ma'lumotlarni shifrlashning farqi nimada?
- 12 Fishing xatining qanday belgilarini bilasiz?

Amaliy topshiriqlar

- 1 O'z kompyuteringizda fayl kengaytmalarini ko'rinadigan qiling va OT yangilanishlarini tekshiring.
- 2 Bitwarden yoki KeePassXC ni o'rnating, kuchli bosh parol yarating va kamida 5 ta hisobni unga ko'chiring.
- 3 Elektron pochtangiz va Telegram hisobingizda 2FA ni yoqing; tiklash kodlarini xavfsiz joyda saqlang.
- 4 «Ishlar» papkasining namunaviy tuzilmasini yarating va fayllarni nomlash qoidalariga muvofiq qayta nomlang.
- 5 Bitta papkaning zaxira nusxasini tashqi diskka yoki bulutga oling va undan bitta faylni tiklab ko'ring.
- 6 7-Zip yordamida maxfiy faylni AES-256 bilan shifrlang; parolni boshqa kanal orqali «yuborish»ni mashq qiling.

Foydalanilgan va tavsiya etiladigan manbalar

- 1 O'zbekiston Respublikasining «Shaxsga doir ma'lumotlar to'g'risida»gi Qonuni, 2019-yil 2-iyul.
- 2 O'zbekiston Respublikasining «Kiberxavfsizlik to'g'risida»gi Qonuni, 2022-yil 15-aprel.
- 3 O'zbekiston Respublikasining «Advokatura to'g'risida»gi Qonuni.
- 4 O'zbekiston Respublikasining «Elektron raqamli imzo to'g'risida»gi Qonuni.
- 5 NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management.
- 6 CISA (AQSh Kiberxavfsizlik va infratuzilma xavfsizligi agentligi). «Secure Our World» tavsiyalari.
- 7 American Bar Association. Model Rules of Professional Conduct, Rule 1.1 (Comment 8) va Rule 1.6(c).
- 8 Microsoft, Apple, Google rasmiy yo'riqnomalari: BitLocker, FileVault, 2-Step Verification.