TEXNIK TOPSHIRIQNOMA

«TASDIQLAYMAN»
“Biznesni rivojlantirish banki” ATB
Boshqaruv raisi o'rinbosari v.b:
B.Bobojonov

«2» iyul 2026 y.
№ 445

“Biznesni rivojlantirish banki” ATB ning DLP tizimi uchun qo‘shimcha litsenziyalar yetkazib berish va texnik-qo‘llab-quvvatlash bo‘yicha

Toshkent – 2026

1. Umumiy qoidalar

1.1. Buyurtmachi ma’lumotlari

Nomi	AKB «Biznes rivojlantirish banki»
Manzil	O‘zbekiston Respublikasi, Toshkent shahri, 100011, Navoiy ko‘chasi 18A
Telefon	(998-78) 150 00 55 (1254)
MFO / INN	01037 / 206 916 313
Elektron pochta	headoffice@brb.uz

1.2 Tizim umumiy tavsifi

Axborotni himoya qilish dasturiy ta’minoti (keyingi o‘rinda – Tizim) hisoblash tarmoqlari segmentlari chegarasidan tashqariga maxfiy axborot uzatish jarayonini nazorat qilishni ta’minlashi kerak. Tizim ish stantsiyalari darajasida (Endpoint), tarmoq darajasida (tarmoq uskunasi yoki proksi-serverdan trafik soya nusxasini olish) va uchinchi tomon tizimlari bilan integratsiya darajasida (masalan, SMTP, ICAP, API texnologiyalari) ishlashni qo‘llab-quvvatlashi kerak. Tizim bir yoki bir nechta sanab o‘tilgan rejimlarda bir vaqtning o‘zida ishlash imkoniyatini ta’minlashi kerak.

Tizim mijoz-server arxitekturasi asosida qurilishi kerak, bunda server ma'muriyat, qayta ishlash, saqlash va ma’lumotlarni tahlil qilish rollarini, mijoz esa foydalanuvchi interfeysi rolini bajaradi. Foydalanuvchi ish stantsiyalari darajasida maxfiy axborot uzatish jarayonini nazorat qiluvchi Tizimning mijoz qismi dasturiy Agent ko‘rinishida taqdim etilishi kerak.

Tizim Agentlari kamida quyidagi Windows oiladagi operatsion tizimlarda ishlashni qo‘llab-quvvatlashi kerak: Windows 8, 8.1 x32/x64, Windows 10 x32/x64, Windows 11 x64, Windows Server 2016, Windows Server 2019, Windows Server 2022.

Tizim Agentlari kamida quyidagi Linux oiladagi operatsion tizimlarda ishlashni qo‘llab-quvvatlashi kerak: Alt Linux 8 SP x64, 9 x64, 10 x64; CentOS 8 x64; RedOS 7.3 x64; Ubuntu 20.04 x64, 22.04 x64, 24.04 x64.

Tizim Agentlari kamida quyidagi MacOS oiladagi operatsion tizimlarda ishlashni qo‘llab-quvvatlashi kerak: Monterey 12.1, Ventura 13.3, Sonoma 14.0, Sequoia 15.0.

Windows, Linux, MacOS operatsion tizimlarining arxitekturalari o‘rtasidagi muhim farq sababli, Windows, Linux va MacOS OT uchun, shuningdek Linux OT ning turli yadrolar yoki versiyalari uchun amalga oshirilgan Agent funksiyalari o‘rtasidagi farqqa yo‘l qo‘yiladi.

Tizimning barcha server funksiyalari yagona yechim, ma’lumotlarni arxivlash uchun yagona MBBT doirasida bajarilishi va OT ning bitta qator doirasida ishlashi kerak. Istisnoni Tizim integratsiya imkoniyatiga ega uchinchi tomon xizmatlari tashkil etadi.

Tizim yopiq konturda, ya'ni Buyurtmachining mahalliy tarmog‘ida internet tarmog‘iga chiqmasdan ishlashni qo‘llab-quvvatlashi kerak. Istisnoni standart bo‘yicha o‘chirilgan va faqat Buyurtmachi xohishiga ko‘ra faollashtiriluvchi alohida ixtiyoriy funksiyalar tashkil etadi (masalan, Agentlar tomonidan Internet orqali ma’lumot uzatish, bulutli korporativ xizmatlarga ulanish va internet-ulanishni talab qiladigan boshqa funksiyalar).

Barcha tarmoq ulanishlari, aloqa protokollari va ulanish yo‘nalishlari Tizimning texnik hujjatlarida ko‘rsatilishi kerak.

Tizim agent yoki mijoz komponentlari tomonidan aloqa liniyalari orqali uzatiladigan ma’lumotlarni himoya qilishni ta’minlashi kerak.

2. Litsenzion dasturiy vositalarni yetkazib berish talablari

2.1. Dasturiy ta'minot distributivi elektron yoki bosma ko‘rinishda hujjatlar bilan birga yetkazib berilishi kerak. Hujjatlar litsenzion dasturiy ta'minotni o‘rnatish va foydalanish qoidalarini o‘z ichiga olishi kerak.

2.2. Ijrochi Buyurtmachiga 12 (o‘n ikki) oy davomida dasturiy ta'minotni yangilash va qo‘llab-quvvatlash (kafolat hamrohligi) huquqlarini tasdiqlovchi litsenzion (sublitsenzion) kelishuvlarni taqdim etishi kerak.

2.3. Kontent tahlili va qaror qabul qilish quyi tizimlari birliklar bo‘yicha litsenziyalanishi kerak (har bir quyi tizim uchun bitta litsenziya).

2.4. Nazorat quyi tizimi modullari oxirgi foydalanuvchilar bo‘yicha litsenziyalanishi kerak: ya'ni bir litsenziya Tizim tomonidan himoyalanadigan bitta domen yoki mahalliy hisob yozuvi uchun talab etiladi. Bundan istisno fayllar audit moduli bo‘lib, u ish stantsiyalari soni bo‘yicha litsenziyalanadi (mijoz versiyali operatsion tizimlarda Tizim Agentidan foydalanilganda) yoki skanerlangan ma'lumotlar hajmi bo‘yicha (tarmoq skanerlash yoki server versiyali operatsion tizimlarda Agentdan foydalanilganda).

2.5. Nazorat quyi tizimi modullari litsenziyalari raqobatbardosh bo‘lishi kerak — ya'ni bitta litsenziya turli davrlarda turli foydalanuvchilarni (hisob yozuvlarini) / ish stantsiyalarini nazorat qilish uchun ishlatilishi mumkin.

2.6. Barcha litsenziyalar muddatsiz foydalanish uchun berilishi kerak — 36 (o‘ttiz olti) oylik yangilash va kafolat muddati tugagandan so‘ng ham mahsulotlar keyingi yangilash paketlari va texnik qo‘llab-quvvatlash sotib olinishidan qat’i nazar, kontragent tomonidan ishlatilishda davom etadi.

2.7. Axborot xavfsizligini ta'minlash tizimida ishlatiladigan dasturiy-texnik himoya vositalari litsenziyalangan va sertifikatlangan bo‘lishi kerak (O‘zbekiston Respublikasi tijorat banklarining axborot xavfsizligi va kiberxavfsizligiga doir minimal talablar to‘g'risidagi 2025-yil 18-avgustdagi № 3669-sonli Nizomning 33-bandi).

3. Dasturiy ta’minot quyidagi modullar va quyi tizimlarni o‘z ichiga olishi kerak

№	Nomi	Litsenziyalar soni
1	**Nazorat quyi tizimi, quyidagilardan iborat:**	
1.1	Elektron pochta nazorat moduli (MailController)	2 400
1.2	Tezkor xabar almashish xizmatlari nazorat moduli (IMController)	2 400
1.3	FTP-ulanishlarni nazorat moduli (FTPController)	2 400
1.4	HTTP-trafikni nazorat moduli, POST- va GET-so‘rovlar (HTTPController)	2 400
1.5	Chop etishni nazorat moduli (PrintController)	2 400
1.6	Olinadigan qurilmalarga kirishni nazorat va boshqarish moduli (DeviceController)	2 400
1.7	Monitor hodisalari va xodimlar harakatlarini nazorat moduli (MonitorController)	2 400
1.8	Xodimlar suhbatlarini nazorat moduli (MicrophoneController)	2 400
1.9	Foydalanuvchilar va ilovalar faolligini nazorat moduli (ProgramController)	2 400
1.10	Bulutli ma’lumotlar saqlash nazorat moduli (CloudController)	2 400
1.11	Fayllar audit moduli (FileAuditor)	200

Litsenziyalash turi – muddatsiz litsenziyalar.

Ishlab chiqaruvchi/huquq egasining butun dasturiy kompleksga kafolat qo‘llab-quvvatlashi – litsenziyalarni topshirish dalolatnomasini imzolagan sanadan boshlab 1 kalendar yil.

3.1. Tizimga umumiy talablar

Tizim ushbu texnik topshiriqda tavsiflangan kanallar doirasida maxfiy axborot uzatishni nazorat qilishni va himoya qilishni, shuningdek ushbu texnik topshiriqda ko‘rsatilgan texnologiyalar doirasida uning avtomatlashtirilgan tahlilini qo‘llab-quvvatlashi kerak.

Tizim yuqorida sanab o‘tilgan ma’lumot uzatish kanallari uchun nazorat modullarini tanlangan tartibda faollashtirish imkoniyatini ko‘zda tutishi kerak.

Tizim axborot arxivi, xavfsizlik siyosatlari va Tizim sozlamalariga kirish huquqlarini chegaralashni ta’minlashi kerak.

Tizim ish stantsiyalari darajasida, ICAP protokoli bo‘yicha proksi-serverlar bilan integratsiya darajasida va tarmoq shlyuzlaridan trafik soya nusxasini uzatish (SPAN) darajasida veb-trafik nazoratini ta’minlashi kerak.

Tizim ham ish stantsiyalari darajasida, ham korporativ pochta serveri bilan integratsiya darajasida pochta trafigi nazoratini ta’minlashi kerak.

Tizim «tor» ma’lumot uzatish kanali bo‘lgan hududiy ajratilgan tarmoqlardagi resurslarga yuklamani optimallashtirish imkoniyatiga ega bo‘lishi kerak: ma’lumotlarni dastlabki siqish, jadval sozlash, uzatish marshrutlari va uzatish tezligini cheklash, shuningdek oraliq qayta ishlash va vaqtinchalik saqlash serverlarini jalb etish hisobiga.

Tizim ish stantsiyalarida sozlanuvchi atributga bog‘liq qoidalarga muvofiq HTTP(S)-trafikni bloklashni ta’minlashi kerak. Bloklangan HTTP(S) resursining tematik toifasi ham atribut sifatida bo‘lishi kerak.

Tizim yuqorida ko‘rsatilgan barcha operatsion tizimlar uchun Windows OT terminal serverlarida ishlovchi foydalanuvchilarning to‘laqonli nazoratini ta’minlashi kerak.

Windows OT bilan ish stantsiyalari darajasida nazorat amalga oshiruvchi Tizim Agenti raqamli imzo bilan imzolangan bo‘lishi kerak.

Kontent tahlili quyi tizimi quyidagi imkoniyatlarni ta’minlashi kerak:

- tekshirish qoidalarini o‘zgartirish imkoniyatini hisobga olgan holda axborot arxivini retrospektiv tahlil qilish;
- foydalanuvchilar faolligi va axborot xavfsizligi siyosatlarini buzish bilan bog‘liq hodisalar bo‘yicha hisobotlar generatsiya qilish;
- real vaqt rejimida foydalanuvchilar faolligini ko‘rish.

Qaror qabul qilish quyi tizimi ushlab olingan obyekt bo‘yicha avtomatik ravishda hukm chiqarish imkoniyatlarini ta’minlashi kerak – mavjud qoidalarni buzadi yoki buzmaydi.

Elektron pochta nazorat moduli elektron pochta xabarlarini nazorat qilishni ta’minlashi kerak (SMTP/ESMTP/SMTPS, POP3/POP3S, IMAP, MAPI protokollari), shuningdek oxirgi stantsiyalarda ushbu modul tomonidan qayd etilgan hodisa yuzaga kelgan taqdirda xabar yuborishni avtomatik ravishda to‘xtatishning ulanadigan funksiyasiga ega bo‘lishi kerak.

Tezkor xabar almashish xizmatlari nazorat moduli mashhur internet-messenjerlar yordamida uzatilgan xabarlar va fayllar nazoratini ta’minlashi kerak. Xususan, Microsoft Teams, Viber Desktop, Telegram Desktop va Zoom Chat kommunikatsion mijozlarining chatlari, qo‘ng‘iroqlari va fayllarini nazorat qilishni ta’minlashi kerak.

FTP-ulanishlar nazorat moduli kiruvchi va chiquvchi FTP-trafik nazoratini ta’minlashi kerak. Ish stantsiyalari darajasida nazorat qilish holatida SSL orqali FTP (FTPS) qo‘llab-quvvatlanishi ham zarur.

HTTP-trafik nazorat moduli Buyurtmachi foydalanuvchilari internet-xizmatlardan foydalanganda POST- va GET-so‘rovlar nazoratini ta’minlashi kerak, shuningdek ushbu modul tomonidan qayd etilgan hodisa yuzaga kelgan taqdirda trafikni avtomatik ravishda to‘xtatishning ulanadigan funksiyasiga ega bo‘lishi kerak.

Chop etish nazorat moduli tarmoq yoki mahalliy printerlar yordamida chop etishga yuborilgan hujjatlar nazoratini ta’minlashi kerak.

Olinadigan qurilmalarga kirish nazorat va boshqarish moduli USB-qurilmalar, CD-/DVD-matritsalar va boshqa turdagi olinadigan qurilmalarga yoziladigan fayllar nazoratini ta’minlashi kerak.

Monitor hodisalari va xodimlar harakatlari nazorat moduli foydalanuvchilar ekranidagi tasvirlar nazoratini ta’minlashi, harakatlarni video yozib olish, suratlar va veb-kamera orqali video yozib olish imkoniyatini ta’minlashi, shuningdek monitorlar mazmuni va foydalanuvchilar harakatlarini real vaqt rejimida ko‘rish imkoniyatini ta’minlashi kerak. Modul klaviaturadan kiritiladigan ma’lumotlar nazoratini, har qanday ilovalarda tugmachalar bosishlarini (tizim tugmachalar va ularning kombinatsiyalarini bosishlarni ham o‘z ichiga olgan holda) jurnalga yozishni amalga oshirishi kerak. Maxfiylikni ta’minlash maqsadida modul, texnik imkoniyat mavjud bo‘lgan hollarda, parol kiritishini aniqlab, parollarni auditdan chiqarish imkoniyatini ta’minlashi kerak. Texnik imkoniyat va amalga oshirish metodikasi Tizim Ishlab chiqaruvchisi tomonidan belgilanadi.

Xodimlar suhbatlari nazorat moduli ish stantsiyasiga ulangan mikrofon yordamida suhbatlar audio yozuvini ta’minlashi kerak. Uchinchi tomon maxfiyligini ta’minlash maqsadida modul xodim ofisda va ofisdan tashqarida bo‘lgan hollar uchun turli ishlash sozlamalarini tanlash imkoniyatini ta’minlashi muhimdir.

Foydalanuvchilar va ilovalar faolligi nazorat moduli ish kuni davomida foydalanuvchilar faolligi va ular tomonidan ishga tushirilgan jarayonlarni davomiyligini hisobga olgan holda monitoring qilishni ta’minlashi kerak.

Bulutli ma’lumotlar saqlash nazorat moduli bulutli xizmatlarning (Google Drive, OneDrive, Office 365, Dropbox, Evernote, Yandex Disk, cloud.mail.ru va boshq.) kiruvchi va chiquvchi ma’lumotlar nazorati imkoniyatlarini ta’minlashi, shuningdek masofaviy kirish dasturlarida (TeamViewer, RealVNC, Radmin, LiteManager) uzatiladigan fayllarni nazorat qilish imkoniyatini berishi kerak.

Fayllar audit moduli ish stantsiyasidagi hamda tarmoq papkalaridagi fayllar va papkalar bilan operatsiyalar auditini ta’minlashi kerak. Quyidagi fayl operatsiyalari kuzatilishi kerak: yaratish, o‘qish, yozish, o‘chirish, nomini o‘zgartirish, ochish, kirish huquqlarini o‘zgartirish. Papkalar bilan quyidagi operatsiyalar kuzatilishi kerak: yaratish, o‘chirish, nomini o‘zgartirish, ochish, kirish huquqlarini o‘zgartirish.

Tizimda Tizim konfiguratsiya sozlamalarini boshqarishni va Tizimning me'yoriy ishlashini avtomatlashtirilgan nazorat qilishni ta’minlovchi funksiyalar amalga oshirilishi kerak. Boshqarish deganda Buyurtmachi xodimlari tashqi mutaxassislarni jalb etmasdan Tizim sozlamalarini mustaqil o‘zgartirish imkoniyatini beruvchi chora-tadbirlar majmui tushuniladi. Avtomatlashtirilgan nazorat deganda Tizimning barcha komponentlarining me'yoriy ishlashini monitoring qilish va favqulodda vaziyatlar yuzaga kelganda administratorni avtomatik xabardor qilish tushuniladi.

3.3. Axborot almashish uchun aloqa usullari va vositalariga talablar

Tizim Buyurtmachining axborot-hisoblash tarmog‘i tarkibida faoliyat ko‘rsatishi kerak.

Ish stantsiyasi darajasidagi nazorat modullari ulanishni himoya qilish uchun ma’lumotlarni Tizim serveriga uzatishda HTTPS dan va/yoki uzatiladigan ma’lumotlarni shifrlashning muqobil algoritmlarini ishlatish imkoniyatiga ega bo‘lishi kerak.

Tizim domen tarmog‘ida to‘g‘ri ishlashi kerak.

Tizim virtual infratuzilmada ishlashni qo‘llab-quvvatlashi kerak. Tizim tomonidan qo‘llab-quvvatlanadigan virtualizatsiya muhitlari, amaliy dasturiy ta’minot va ularning versiyalari ro‘yxati Ijrochi tomonidan texnik hujjatlar tarkibida taqdim etilishi kerak.

Tizim komponentlari o‘rtasida axborot almashish uchun faqat TCP/IP oilasining standart protokollari va interfeyslari (Ethernet/Fast Ethernet/Gigabit Ethernet) va/yoki simsiz tarmoq ulanishlari ishlatilishi kerak.

Tizim va korporativ pochta tizimi o‘rtasida axborot almashish uchun SMTP protokoli ishlatilishi kerak.

Tizim Active Directory bilan integratsiya orqali axborot yuborgan kompaniya xodimining quyidagi ma’lumotlarini aniq belgilash imkoniyatini ta’minlashi kerak:

- foydalanuvchi hisob yozuvi;
- ishlatiladigan ish stantsiyasi haqidagi ma’lumot (nomi, IP- va MAC-manzili).

3.4. Tizim ishlash rejimlariga talablar

Tizim quyidagi rejimlarda ishlash imkoniyatini ta’minlashi kerak:

- me'yoriy rejim (asosiy ishlash rejimi – Tizimning barcha funksiyalarini uzluksiz tinimsiz bajarishni ta’minlovchi administrator boshqaruvida avtomatlashtirilgan ishlashni ko‘zda tutadi);
- servis rejimi (komponentlarni texnik xizmat ko‘rsatish, qayta konfiguratsiya qilish va modernizatsiya qilish uchun ishlatiladi);
- avtonom rejim (Tizim komponentlari o‘rtasida yoki tashqi tarmoqlar bilan aloqa bo‘lmagan taqdirda konfiguratsiya va arxiv axborotiga kirish uchun ishlatiladi).

3.5. Tizimni diagnostika qilish talablari

Tizim xizmat hodisalari va nosozliklar bo‘yicha axborotni audit jurnallariga yozib olish imkoniyatini ta’minlashi kerak. Jurnallardagi yozuvlar nosozlik sababini aniqlash uchun yetarli ma’lumotni o‘z ichiga olishi kerak.

Tizimning har bir moduli me'yoriy va kengaytirilgan jurnal yozib olish rejimiga ega bo‘lishi kerak. Dasturiy nosozliklar holatida tizim jurnallariga majburiy yozib olishning nosozlik bartaraf etish rejimi ko‘zda tutilishi kerak. Nosozlik bartaraf etish rejimi dasturiy nosozlik yuzaga kelganda foydalanuvchi ishtirokisiz avtomatik ravishda yoqilishi kerak.

Ko‘p foydalanuvchili ish holatida modul har bir foydalanuvchi uchun avtomatik ravishda alohida jurnallar yaratishi kerak.

3.6. Ijrochi xodimlarining soni va malakasiga talablar

Tizimni yetkazib berish va foydalanishga topshirishni ta’minlash uchun Ijrochi xodimlar tarkibida kamida bitta texnik qo‘llab-quvvatlash muhandisi bo‘lishi kerak.

Texnik qo‘llab-quvvatlash muhandisi Buyurtmchi tomonida Tizimga me’yoriy texnik va favqulodda xizmat ko‘rsatishni bajarish uchun zarur hajmdagi bilimlarga ega bo‘lishi kerak.

3.7. Tizimni rivojlantirish va modernizatsiya qilish istiqbollari

Tizim texnik vositalar xususiyatlarini yaxshilash hisobiga unumdorlikni oshirishga yo‘l qo‘yishi kerak.

Tizim texnik va/yoki dasturiy ta’minotni almashtirish yo‘li bilan modernizatsiya qilish imkoniyatini ta’minlashi kerak.

Ijrochi Tizimni joriy etishni rejalashtirish vaqtida minimal yetarli yoki tavsiya etilgan uskunalar bo‘yicha Buyurtmachining konsultatsiyalari uchun jalb etilishi mumkin. Konsultatsiyalar rasmiylashtirilib, Buyurtmachini standart so‘rovnoma asosida so‘roq qilish tartibida olib borilishi kerak.

3.8. Tizimning maqsadli vazifasi saqlanadigan xususiyatlarga talablar

Tizimning maqsadli vazifasi butun ekspluatatsiya muddati davomida saqlanishi kerak. Tizimning ekspluatatsiya muddati hisoblash komplekslarining texnik vositalarining barqaror ishlash muddati, texnik vositalarni o‘z vaqtida almashtirish (yangilash), Tizim dasturiy ta’minotini (kafolat va kafolatdan keyingi xizmat ko‘rsatish doirasida) hamrohlik qilish va yangilash, modernizatsiya qilish ishlari bilan belgilanadi.

Tizimning maqsadli vazifasi butun ekspluatatsiya muddati davomida oldindan kelishilgan IT muhiti uchun saqlanishi kerak. Alohida Ijrochi bilan kelishilmagan va kelajakda chiqadigan tizim yoki amaliy dasturiy ta’minotning yangi versiyalarini qo‘llab-quvvatlash kafolatlanmasligi mumkin.

3.9. Ma'muriyat funksiyalariga talablar

Administrator interfeysi Tizim ishlash qobiliyatini nazorat qilish imkoniyatini ta’minlashi kerak.

Administrator interfeysi Agentlar ishlash statistikasini, ish stantsiyalaridan ma’lumotlarni ushlab olish server quyi tizimlarini, indekslash serverini, pochta yozishmalarini nazorat xizmatlarini (korporativ pochta serveri bilan integratsiya darajasida), pochta bloklash xizmatini, MS SQL Server va PostgreSQL MBBT ni, grafik tasvirlar va audio fayllarni tanib olish xizmatlarini, operatsion tizimni ko‘rsatish imkoniyatini ta’minlashi kerak. Ko‘rsatilgan barcha statistik ma’lumotlar uchun zaxira nusxa olish imkoniyati ta’minlangan bo‘lishi kerak.

Administrator interfeysi quyi tizimlar xizmatlarini boshqarish imkoniyatini ta’minlashi kerak.

Administrator interfeysi axborot nazorat modullari ma’lumotlar bazasini boshqarish imkoniyatini ta’minlashi kerak.

Administrator interfeysi Tizim serverlaridagi disk maydonini monitoring qilish imkoniyatini ta’minlashi kerak.

Administrator interfeysi muhim hodisalar haqida avtomatik xabarnoma berish imkoniyatini ta’minlashi kerak (ishlash nosozliklari, bo‘sh joy yetishmasligi, litsenziyalar sonidan oshib ketish va boshqalar).

Administrator interfeysi bir yoki bir nechta Active Directory domeni bilan sinxronizatsiya imkoniyatini ta’minlashi kerak.

Administrator interfeysi ish guruhlari foydalanuvchilari bilan ishlash imkoniyatini ta’minlashi kerak.

Administrator interfeysi xavfsizlik xizmati xodimlarining quyi tizimlar konsollarining funksiyalariga va ma'lum foydalanuvchilar, foydalanuvchilar guruhlari hamda ma’lumot manbalariga oid ma’lumotlarga kirish huquqlarini chegaralash imkoniyatini ta’minlashi kerak. Ma’lumotlar deganda qaror qabul qilish quyi tizimi tomonidan qayd etilgan hodisalar, shuningdek kontent tahlili quyi tizimida ko‘rib chiqish uchun mavjud bo‘lgan karantinga tushgan hujjatlar va pochta xabarlarining mazmuni tushuniladi.

Administrator interfeysi ma’lumotlar bazalariga ulanish sozlamalarini ko‘rsatish imkoniyatini ta’minlashi kerak (ular ishlatiladigan hollarda), keyinchalik ularni standart sifatida ishlatish mumkin bo‘lishi kerak.

Administrator interfeysi «eski» ma’lumotlar bazalari, indekslar, xotiralarni yangi saqlash joyiga avtomatik ko‘chirish (tez disklar yukini kamaytirish maqsadida), shuningdek ma’lumotlar bazalari, indekslar, xotiralarni keyingi tiklash imkoniyati bilan avtomatik arxivlashni ta’minlashi kerak.

3.10. Ma’lumotlarni saqlash talablari

Katta hajmdagi ma’lumotlar bilan samarali ishlash uchun Tizim, texnik jihatdan mumkin bo‘lganda, soya nusxa fayllarining originallarini Tizim bilan moslashtirilgan va optimallashtrilgan maxsus fayl xotirasida saqlashi kerak. Texnik imkoniyat Tizim Ishlab chiqaruvchisi tomonidan belgilanadi.

Tizim matnli va atributiv ma’lumotlarni qidiruv tanlovlarini tezlashtirish uchun ixtisoslashtirilgan indekslarda saqlash opsiyasiga ega bo‘lishi kerak. Ma’lumotlar indeksda mavjud bo‘lgan taqdirda, bunday ma’lumotlar bo‘yicha har qanday qidiruv so‘rovi ham avval indeks bo‘yicha bajarilishi kerak.

Tizim ma’lumotlarni tuzilgan jadval ko‘rinishida saqlash va ularni uchinchi tomon tahlil tizimlarida qayta ishlash uchun Microsoft SQL Server 2012 SP4 va undan yuqori, shuningdek, PostgreSQL 14 va undan yuqori versiyalar bilan muvofiq bo‘lishi kerak.

Tizim faqat hodisalar qayd etilgan obyektlarni emas, balki barcha ushlab olingan obyektlarni arxivlashi kerak.

3.11. Ishonchlilik talablari

Tizimning barcha serverlarida RAID massivi bo‘lishi ko‘zda tutilishi kerak.

Tizim nosozliklari holatida ishlash qobiliyatini tiklash bo‘yicha namunaviy yo‘riqnoma ko‘zda tutilishi kerak. Tizim ishlash qobiliyatini tiklash protsedurasi Tizimga tegishli ekspluatatsiya hujjatlarida tavsiflangan va hujjatlashtirilgan bo‘lishi kerak.

Tizim shunday amalga oshirilishi kerakki va/yoki xodimlar kuchlari bilan nosozliklar yuzaga kelganda uning ishlash qobiliyati va ma’lumotlarini tiklashni ta’minlovchi chora-tadbirlar majmui belgilanishi kerak.

Tizimning texnik yoki dasturiy ta’minoti nosozligi yuzaga kelgan taqdirda uning ma’lumotlari va sozlamalarini tiklash imkoniyati ta’minlanishi kerak.

4. Tizim tomonidan bajariluvchi funksiyalarga (vazifalar) talablar

4.1. Kontent tahlili quyi tizimiga talablar

Kontent tahlili quyi tizimi nazorat quyi tizimi modullaridan olinadigan ma’lumotlar bilan ishlashga mo‘ljallangan bo‘lishi kerak.

Quyi tizim barcha ushlab olingan yoki qayd etilgan obyektlar bo‘yicha retrospektiv tahlil o‘tkazish imkoniyatini ta’minlashi kerak. Ma’lumotlar indekslash sozlangan obyektlar uchun quyidagi qidiruv imkoniyatlari qo‘llab-quvvatlanishi kerak:

- ushlab olingan hujjatlar bazalarida kalit so‘zlar va iboralar bo‘yicha qidirish;
- ushlab olingan ma’lumotlarni sana, foydalanuvchining domen nomi, elektron pochta manzillari va xostlari, kompyuterlar, printerlar nomlari va boshqa atributlar bo‘yicha saralash;
- izlanayotganga mazmun yoki tarkibi jihatdan o‘xshash matn namunasi bo‘yicha qidirish. Ushbu qidiruv turi qidiruv mexanizmi sozlamalarini manipulyatsiya qilish va qo‘shimcha lug‘atlarni ulashni nazarda tutmasligi kerak – faqat hujjatlar relevanlik (o‘xshashlik) foizini belgilash talab etiladi;
- so‘zlar to‘plami (lug‘at) bo‘yicha qidirish, ma'lum miqdordagi yoki foizli so‘zlarni o‘z ichiga olgan hujjatlarni topish imkonini beruvchi. So‘zlar to‘plami qo‘lda kiritilishi, bufer almashuvidan joylashtirilishi yoki tashqi matn faylidan yuklanishi mumkin. Lug‘atdagi har bir so‘zni shakllantirish mantiqiy operatorlarni ishlatmasdan amalga oshirilishi kerak.

Matniy mazmunni tahlil qilish morfologik xususiyatlar va sinonimlarni hisobga olgan holda amalga oshirilishi kerak. Bunda so‘z shakllari mantiqiy operatorlar va maxsus belgilardan foydalanmasdan hosil qilinishi kerak.

Quyi tizim har bir ushlab olingan obyekt bo‘yicha batafsil ma’lumotni ko‘rish, jumladan, foydalanuvchilar ekranlaridagi harakatlar yozuvini o‘rnatilgan video pleyerda ko‘rish, shuningdek video yozuvni ilovalar faolligi va tugmachalar bosishlari bilan solishtirish imkoniyatini ta’minlashi kerak.

Quyi tizim ushlab olingan hujjatning kontent marshrutini ko‘rish imkoniyatini ta’minlashi kerak.

Quyi tizim ushlab olingan ma’lumotlar tanlovini eksport qilish (to‘liq ro‘yxat yoki mundarija bilan fayllar to‘plami) imkoniyatini ta’minlashi kerak.

Quyi tizim «Foydalanuvchi kartochkasi»ni shakllantirish va ko‘rsatish imkoniyatini ta’minlashi kerak, u quyidagilarni o‘z ichiga olishi kerak: tanlangan foydalanuvchi bo‘yicha umumiy ma’lumot (qo‘shimcha maydonlar qo‘shish imkoniyati bilan), uning Active Directory hisob yozuvlari, aloqa

ma’lumotlari (e-mail manzillari va boshqa IM-mijozlar), shuningdek ko‘rsatilgan vaqt davri uchun joriy foydalanuvchining aloqalari haqidagi ma’lumot.

Quyi tizim foydalanuvchi faolligi toifalari bo‘yicha filtrlash imkoniyati bilan real vaqt rejimida xodimlar faolligini ko‘rish imkoniyatini ta’minlashi kerak.

Quyi tizim real vaqt rejimida foydalanuvchilar ish joylarida bo‘layotgan voqealar ustidan tezkor nazorat o‘rnatish imkoniyatini ta’minlashi kerak: monitorlar ekranlarida bo‘layotgan narsalarni ko‘rish, xodimlar nutqini tinglash, jadvalga muvofiq ulangan veb-kamera orqali kompyuter oldida bo‘layotgan voqealarni ko‘rish.

Quyi tizim mavjud asosiy shablonlar (kamida 30 ta) bo‘yicha hisobotlar generatsiya qilish, shuningdek foydalanuvchi shablonlarini qo‘shish imkoniyatini ta’minlashi kerak.

Quyi tizim hisobotlarni jadval, diagramma, vaqt grafigi, shuningdek aloqalar grafi ko‘rinishida taqdim etishni qo‘llab-quvvatlashi kerak.

Quyi tizim foydalanuvchilar faolligi va axborot xavfsizligi siyosatlarini buzish bilan bog‘liq hodisalar bo‘yicha statistika yig‘ish va hisobotlar generatsiya qilishni amalga oshirishi kerak.

Quyi tizim ish kuni davomida foydalanuvchilarning ishga tushirilgan ilovalardagi faolligini ko‘rsatishi kerak. Xodimlar tomonidan kompaniyada belgilangan mehnat tartibini buzish (kech kelish, erta ketish, yetarli faollik bo‘lmasligi; ish faoliyati bilan bog‘liq bo‘lmagan ilovalarda uzoq vaqt ishlash) holatlarida ushbu haqda axborot xavfsizligi xizmati xodimining elektron manziliga bildirishnoma shakllantirish va yuborish imkoniyati ko‘zda tutilishi kerak.

Quyi tizim tanlangan vaqt davri uchun foydalanuvchilar ish unumdorligi bo‘yicha qisqa va batafsil hisobotlar generatsiya qilishi kerak.

Quyi tizim dasturlar bo‘yicha hisobotlar generatsiya qilishi kerak: dasturlarni o‘rnatish va o‘chirish soni, agentlarni o‘rnatish/o‘chirish, belgilangan dasturlari o‘rnatilgan/(o‘rnatilmagan) kompyuterlar ro‘yxati va kompyuterlardagi ularning o‘zgarish tarixi.

Quyi tizim qurilmalar bo‘yicha hisobotlar generatsiya qilishi kerak: foydalanuvchilar kompyuterlarida o‘rnatilgan uskunalar ro‘yxati va qurilmalar (komplektlovchilar) o‘zgarishlari bo‘yicha hisobot.

Quyi tizim quyidagilarni ko‘rsatuvchi tizim hisobotlarini generatsiya qilishi kerak:

- har qanday yoki ko‘rsatilgan foydalanuvchi tomonidan agentlar/protokollar bilan amalga oshirilgan operatsiyalar;
- ishlamayotgan agentlari bo‘lgan kompyuterlar ro‘yxati;
- agentsiz kompyuterlar ro‘yxati;
- belgilangan vaqt oralig‘i uchun tanlangan kompyuterlar bo‘yicha xabarlar miqdori haqida ma’lumot.

Quyi tizim topilgan hujjatlarni qidirish va ko‘rishga tez o‘tish imkoniyatini ta’minlashi kerak.

Quyi tizim bog‘liq hisobotlar bo‘yicha o‘tishlar imkoniyatini ta’minlashi kerak.

Quyi tizim tanlangan foydalanuvchi yoki bir nechta foydalanuvchilarning muloqot doirasi haqida ko‘rgazmali tasavvur olish, ushbu foydalanuvchilar uchun umumiy kontaktlarni, shuningdek tashqi adresatlarning kompaniya xodimlari bilan kontaktlarini aniqlash maqsadida ichki va tashqi adresatlar o‘rtasidagi aloqalarni interaktiv graf ko‘rinishida ko‘rsatishni ko‘zda tutishi kerak.

Quyi tizim tanlangan foydalanuvchi xabar yuborgan yoki u xabar olgan manzillar haqida ko‘rgazmali tasavvur olish imkoniyatini ta’minlashi kerak.

Quyi tizim generatsiya qilingan hisobotlarni PDF-faylga konvertatsiya qilish, shuningdek ularni chop etishga chiqarish imkoniyatini ko‘zda tutishi kerak.

Quyi tizim auditorlarga xavfsizlik hodisalarini tekshirish imkoniyatini ta’minlovchi funksional imkoniyatni ta’minlashi kerak: ularga qo‘shilgan qidiruv natijalari va fayllar bilan vazifalar yaratish, mas'ul auditorni tayinlash, shuningdek vazifalar prioriteti va bajarish muddatini belgilash.

4.2. Qaror qabul qilish quyi tizimiga talablar

Quyi tizim xavfsizlik siyosatlari va hodisalarni boshqarish uchun mijoz konsolidan foydalanishi kerak. Konsol uchun ajratilgan kirish huquqlarini chegaralash ishlashi kerak.

Quyi tizim har bir ushlab olingan obyekt uchun yagona hukm chiqarishi kerak (hodisa / hodisa emas).

Quyi tizim ma’lumot uzatish kanallari, protokollar, foydalanuvchilar, tekshirish qoidalari bo‘yicha rubrikatsiya imkoniyati bilan hodisalar jurnalini yuritish imkoniyatini ta’minlashi kerak.

Quyi tizim mas'ul shaxslarga hodisalar haqida elektron pochta orqali bildirishnoma berish imkoniyatini ta’minlashi kerak.

Quyi tizim obyekt bo‘yicha avtomatik hukm chiqarish qoidalarini (hodisa / hodisa emas) belgilash imkoniyatlarini ta’minlashi kerak. Avtomatik hukm chiqarish qoidalarini quyidagilarga asosan qo‘llash imkoniyati ta’minlanishi kerak:

- ushlab olingan obyektning rasmiy belgilari (domen nomi, yuboruvchi, oluvchi, xost, hajmi, fayl kengaytmasi, ma’lumot uzatish kanali, protokol va boshq.);
- parol bilan himoyalangan arxivlar;
- ushlab olingan obyektlardan ajratib olingan matnni kontent tahlili natijalari (so‘zlar va matn namunalari bo‘yicha, tematik lug‘atlar bo‘yicha, etalon hujjatlar bazasi bilan solishtirish yo‘li bilan, mazmun yoki tarkibi jihatdan etalonaga yaqin matnlarni qidirish, alifboli-raqamli obyektlarni qidirish, shuningdek muntazam ifodalar yordamida qidirish).

Quyi tizim mavjud avtomatik hukm chiqarish qoidalarini (tekshirish qoidalari) o‘zgartirish va yangilarini qo‘llash imkoniyatlarini ta’minlashi kerak.

Quyi tizim foydalanuvchi xavfsizlik siyosati shablonlarini (tekshirish qoidalarini) qo‘llash imkoniyatini ko‘zda tutishi kerak.

Quyi tizim yangilangan tekshirish qoidalarini hisobga olgan holda ushlab olingan hujjatlarni retrospektiv nazorat qilishni o‘tkazish imkoniyatini ta’minlashi kerak.

Quyi tizim xavfsizlik siyosatlarini (tekshirish qoidalarini) guruhlarga birlashtirish imkoniyatini ko‘zda tutishi kerak.

Quyi tizim har bir xavfsizlik siyosatlari guruhi uchun individual sozlamalar belgilash imkoniyatini ta’minlashi kerak: so‘rov o‘tkaziladigan ma’lumot manbalari ro‘yxati, tekshirish jadvali, hodisalar haqida bildirishnomalar oluvchilar ro‘yxati, istisnolar ro‘yxati.

Quyi tizim «oq» istisnolar ro‘yxatlaridan (tekshiruvlardan chiqarilgan foydalanuvchilar hujjatlari ro‘yxati) va «qora» istisnolar ro‘yxatlaridan (faqat hujjatlari bo‘yicha tekshiruv o‘tkaziladigan foydalanuvchilar ro‘yxati) foydalanish imkoniyatlarini ta’minlashi kerak.

Quyi tizim sozlamalar strukturasini (xavfsizlik siyosatlari, qidiruv mezonlari, istisnolar ro‘yxatlari va boshq.) eksport/import qilish imkoniyatini ta’minlashi kerak.

Quyi tizim foydalanuvchilarni qo‘shish va ularga muayyan xavfsizlik siyosatlari hamda istisnolar ro‘yxatlarini ko‘rish va tahrirlash huquqlarini berish, jumladan ushbu amallarga taqiq belgilash imkoniyatini ta’minlashi kerak.

Quyi tizim aniqlangan hodisalarni protokollash imkoniyatlarini ta’minlashi kerak.

Quyi tizim rang belgilar yordamida hodisalarni kategoriyalash imkoniyatini qo‘llab-quvvatlashi kerak.

Quyi tizim syslog orqali hodisalar va voqealar haqidagi ma’lumotlarni eksport qilish imkoniyatini qo‘llab-quvvatlashi kerak.

Quyi tizim parol bilan himoyalangan ushlab olingan arxivlar uchun parollarni tanlash imkoniyatlarini ta’minlashi kerak. Parollarni tanlash uchun baza (lug‘at) klaviatura ma’lumotlari nazorat moduli ma’lumotlari asosida avtomatik ravishda generatsiya qilinadi.

Quyi tizim quyidagi turdagi obyektlar bo‘yicha qaror qabul qilish imkoniyatlarini ta’minlashi kerak:

- Tizim tomonidan qo‘llab-quvvatlanadigan kanallar va protokollar orqali uzatilgan xabarlar;
- quyidagi formatlardagi fayllar: MS Office (doc, docx, dot, xls, xlsx, xlsb, xlsm, xlt, xltx, xltm, ppt, pptx, rtf, pot, vsd, vst, vsdx), Open Office (sxw, stw, odt, ods), HTML-fayllar (htm, html, shtml, mht, css, js, maff), pochta xabarlari fayllari (eml, msg), ma’lumotlar bazalari (mdb), qo‘shimcha hujjat formatlari (txt, xml, pdf, djvu, csv, lst, log, bat, ini, wri);
- bmp, jpg, jpeg, png, tif, tiff, gif formatdagi grafik fayllardagi tanib olingan va tahlil qilingan matnlar;
- siqilgan fayllarga joylashtirilgan hujjatlar: rar, zip, 7z, jar, tar, arj, gz, gzip, cab, iso, chm, hlp, 001.

Quyi tizim muhim ma’lumotlarni aniqlashning quyidagi imkoniyatlarini ta’minlashi kerak:

- kalit so‘zlar bo‘yicha, jumladan izlanayotgan so‘zlarning o‘zaro joylashishiga cheklovlar qo‘yish imkoniyati;
- mazmun yoki tarkibi jihatdan izlanayotganga o‘xshash namuna asosida o‘xshash hujjatlarni aniqlash imkoniyati;
- xabarlar va fayllarning rasmiy belgilari bo‘yicha (domen foydalanuvchisi, kompyuter nomi, yuboruvchi, oluvchi, hajmi, fayl nomi, formati va boshq.), jumladan matni ajratib olib bo‘lmaydigan fayllar uchun ham;
- ma'lum turdagi hujjatlarni (rezyume, moliyaviy va buxgalteriya hisobotlari) aniqlash maqsadida oldindan belgilangan lug‘at bo‘yicha;
- bir nechta mezonlarni (iborali qidiruv, paragraflar va butun hujjatlar hamda atributlar bo‘yicha qidiruv) AND, OR, NOT mantiqiy operatorlari bilan birlashtirishni o‘z ichiga olgan kompleks qidiruv so‘rovlarini yaratish imkoniyati;
- PCRE muntazam ifodalari bo‘yicha – murakkab alifboli-raqamli obyektlarni qidirish (pasport raqamlari, soliq to‘lovchilarning individual raqamlari, kredit kartalari raqamlari, shartnamalar yoki hisoblar raqamlari, klassifikatorlar kodlari va boshq.), murakkab muntazam ifodalar yaratish imkoniyati bilan (bir nechta oddiylardan iborat), muntazam ifodalalarning umumiy miqdori bo‘yicha ishga tushirish ostonasini, hujjatdagi muntazam ifoda kirishlarining sonini va muntazam ifodalar o‘rtasidagi oraliq belgilar sonini belgilash imkoniyati bilan, distribu-tivga kiritilgan standart ifodalar va foydalanuvchi tomonidan yaratilganlarini qo‘llash imkoniyati bilan, shuningdek olingan natijalarni tekshirish imkoniyati bilan;
- maxfiy hujjatlarning raqamli izlari bo‘yicha, ishga tushirish ostonasini ko‘rsatish imkoniyati bilan;
- atributlar qiymatlari bo‘yicha (ham umumiy atributlar, ham aloqa kanallarining alohida atributlari);
- statistik so‘rovlarning miqdoriy ko‘rsatkichlari bo‘yicha (yuborilgan xatlar/chop etilgan sahifalar, Viber, IM va boshqalardagi xabarlar soni);
- qo‘shimcha qidiruv so‘rovi (topilgan bo‘yicha filtrlar) orqali qidiruv natijalarini toraytirish imkoniyati.

Quyi tizim ma’lumotlarni quyidagi turdagi manipulyatsiyalarga chidamliligini ta’minlashi kerak:

- maxfiy axborot fragmentini maxfiy bo‘lmagan hujjatlarga import qilish;
- so‘zlar tartibini o‘zgartirish;
- so‘zlar orasidagi masofalarni o‘zgartirish;
- hujjat formatlashtirishini o‘zgartirish;
- so‘z shakllarini o‘zgartirish;
- harflarni boshqa alifbo belgilariga almashtirish;

- harflar o‘rnida raqamlardan foydalanish;
- fayl kengaytmalarini o‘zgartirish.

Quyi tizim har bir hodisa bo‘yicha batafsil ma’lumotni ko‘rish imkoniyatlarini ta’minlashi kerak.

4.3. Nazorat quyi tizimiga talablar

4.3.1. Windows OT uchun Agent funksiyalariga umumiy talablar

4.3.1.1. Elektron pochta nazorat moduliga talablar

Modul pochta mijozlari yoki brauzerlar yordamida SMTP, POP3, IMAP, MAPI, HTTP protokollari (veb-pochta: ham chiquvchi, ham kiruvchi) bo‘yicha uzatiladigan xabarlar va ilovalarni nazorat qilish imkoniyatlarini ta’minlashi kerak. Modul kontent va/yoki kontekst tahlili asosida SMTP va HTTP protokollari bo‘yicha chiquvchi pochta xabarlarini, shuningdek IMAP va MAPI protokollari bo‘yicha Outlook pochta mijozi yordamida uzatiladigan chiquvchi elektron xabarlarni avtomatik to‘xtatishning ulanadigan funksiyasiga ega bo‘lishi kerak.

Modul kontent va/yoki kontekst mezonlari bo‘yicha chiquvchi pochtani bloklash imkoniyatini ta’minlashi kerak.

Modul ushlab olingan hujjatlarga atributlar belgilashni ta’minlashi kerak: domen hisob yozuvlari, yuboruvchi va oluvchilarning manzillari, xat mavzusi va boshqalar.

4.3.1.2. Tezkor xabar almashish xizmatlari nazorat moduliga talablar

Modul quyidagilarni nazorat qilishni ta’minlashi kerak:

- Facebook, LinkedIn, VKontakte, Odnoklassniki.ru va boshqa ijtimoiy tarmoqlarda (Tizim Ishlab chiqaruvchisi xohishiga ko‘ra) HTTP protokoli bo‘yicha kiruvchi va chiquvchi xabarlar;
- Teams, Viber, Telegram, WhatsApp, Rocket.chat, Mattermost messenjerlarining desktop-versiyalari yordamida uzatilgan chatlar va fayllar;
- Telegram (web.telegram.org), WhatsApp (web.whatsapp.com), Rocket.chat, Mattermost, Teams, Bitrix24 messenjerlarining veb-versiyalari chatlar va fayllar;
- Zoom Chat, TrueConf Client yordamida uzatilgan chatlar, qo‘ng‘iroqlar va fayllar, shuningdek Zoom konferensiyalari;
- Instagram, LINE, Output Messenger fayl uzatish tarixi va chatlari;
- slack.com resursi xabarlari va fayllari.

Modul HTTP protokoli bo‘yicha ijtimoiy tarmoqlarda, Slack, Zoom Chat, Telegram orqali uzatiladigan xabarlar va fayllarni belgilangan kontent va/yoki kontekstga muvofiq bloklash, shuningdek WhatsApp Desktop, WhatsApp Web orqali uzatiladigan fayllarni bloklash va Telegram Web ga kirishni to‘liq bloklash imkoniyatini ta’minlashi kerak.

Modul matnli va ovozli aloqa seanslarini (jumladan, telefon raqamlariga qo‘ng‘iroqlar va video aloqa seanslarining ovozli yozuvlari), fayllarni nazorat qilishni amalga oshirishi kerak.

Modul Microsoft Teams, Viber va Telegram kommunikatsion dasturlari-mijozlarining kiruvchi/chiquvchi xabarlari, qo‘ng‘iroqlari va fayllarini nazorat qilishni ta’minlashi kerak.

Modul foydalanuvchi tomonidan HTTP-tunnellash qo‘llangan holda uzatilgan tezkor xabar almashish xizmatlari trafigini nazorat qilishni ta’minlashi kerak.

Modul ushlab olingan hujjatlarga atributlar belgilashni ta’minlashi kerak: domen hisob yozuvlari, yuboruvchi va oluvchilarning UIN lari, xabarlar soni va boshqalar.

4.3.1.3. FTP-ulanishlar nazorat moduliga talablar

Modul SSL-shifrlashdan foydalanishni o‘z ichiga olgan holda FTP-ulanishlar orqali yuklangan yoki uzatilgan hujjatlarni nazorat qilishni ta’minlashi kerak.

Modul ushlab olingan hujjatlarga atributlar belgilashni ta’minlashi kerak: domen hisob yozuvlari, maqsadli URL-manzillar, FTP-serverlar foydalanuvchilarining nomlari va boshqalar.

Modul ushlab olingan hujjatlarni maxsus fayl xotirasiga joylashtirishni ta’minlashi kerak.

4.3.1.4. HTTP-trafik nazorat moduliga talablar

Modul POST-so‘rovlar (xabarlar va fayllar) nazorat qilish imkoniyatlarini ta’minlashi kerak.

Modul zamonaviy brauzerlar, jumladan Internet Explorer, Mozilla Firefox, Opera, Google Chrome tomonidan generatsiya qilinadigan so‘rovlarni filtrlashni qo‘llab-quvvatlashi kerak.

Modul foydalanuvchilar tomonidan mashhur qidiruv tizimlariga, jumladan Google, Yandex ga yuborilgan GET-so‘rovlarni nazorat qilishni qo‘llab-quvvatlashi kerak.

Modul mashhur blog xizmatlari, veb-chatlar va mashhur forum dvigatellari (vBulletin, Invision Power Board, phpBB) tomonidan generatsiya qilinadigan so‘rovlarni filtrlashni qo‘llab-quvvatlashi kerak.

Modul faqat belgilar to‘plami ma'noli axborot tashuvchi ushlab olingan POST-so‘rovlarning qidiruv natijalarini ko‘rsatish imkoniyatini ko‘zda tutishi kerak.

Modul ular terilgan ilovalar va brauzerlar bo‘yicha filtrlash bilan tugmachalar bosishlarini nazorat qilishni ta’minlashi kerak.

Modul HTTP(S) bo‘yicha taqiqlangan internet-resurslarni tashrif buyurishni bloklash, «oq» va «qora» istisnolar ro‘yxatlarini yaratish, shuningdek internet-resurslarni bloklash va/yoki tashrif buyurishga ruxsat berish uchun sayt toifalaridan foydalanish imkoniyatini ko‘zda tutishi kerak; taqiqlangan internet-resursga kirishni bloklashda ko‘rsatiladigan bildirishnomani sozlash imkoniyatini ko‘zda tutishi kerak.

Modul belgilangan kontent va/yoki kontekstga muvofiq xabarlar va fayllarni uzatishni bloklash imkoniyatini ta’minlashi kerak.

Modul ushlab olingan hujjatlarga atributlar belgilashni ta’minlashi kerak: domen hisob yozuvlari, so‘rov tanasi, xost nomi va boshqalar.

4.3.1.5. Chop etish nazorat moduliga talablar

Modul mahalliy va tarmoq printerlari yordamida chop etishga yuborilgan hujjatlarni nazorat qilishni amalga oshirishi kerak.

Modul chop etishga yuborilgan hujjatlarning grafik tasviri va matnini ham nazorat qilishni amalga oshirishi kerak.

Modul ushlab olingan hujjatlarga atributlar belgilashni ta’minlashi kerak: domen hisob yozuvlari, printerlar nomlari, chop etilgan sahifalar soni va boshqalar.

Modul alohida printerlarni (shu jumladan ularning tavsifi va joylashuvi bo‘yicha), foydalanuvchilarni, hujjatlarni (nomlar bo‘yicha) va jarayonlarni nazoratdan chiqarish imkoniyatini qo‘llab-quvvatlashi kerak.

Modul belgilangan kontent va/yoki kontekstga muvofiq fayllarni chop etishni bloklash imkoniyatini ta’minlashi kerak.

Modul nazorat qilingan hujjatlarni chop etish mumkin bo‘lmagan PostScript/PCL printerlar uchun Escape-funksiyalarini bloklash imkoniyatini ta’minlashi kerak.

4.3.1.6. Olinadigan qurilmalar nazorat va boshqarish moduliga talablar

Modul foydalanuvchining tashqi qurilmalarga (CD-/DVD-qurilmalar, USB va FireWire olinadigan xotiralar, USB-qurilmalar) va portlarga (USB, FireWire, COM, LPT, IRDA, SCSI va boshqalar Tizim Ishlab chiqaruvchisi xohishiga ko‘ra) kirish nazorat imkoniyatlarini ta’minlashi kerak.

Modul terminal sessiyasida ishlashni qo‘llab-quvvatlashi kerak.

Modul qurilmalar va portlarning vakolatli foydalanuvchilar guruhlarini aniqlashni ta’minlashi kerak.

Modul tashqi qurilmaga uzatiladigan ma’lumotlarni soya nusxa olish imkoniyatini ta’minlashi kerak.

Modul ulangan tashqi USB-qurilmada saqlanadigan ma’lumotlarni soya nusxa olish imkoniyatini ta’minlashi kerak.

Modul bufer almashuvi, jumladan RDP-sessiyasining bufer almashuvi orqali uzatiladigan ma’lumotlarni soya nusxa olish imkoniyatini ta’minlashi kerak.

Modul audit jurnalida barcha voqealarni qayd etishni ta’minlashi kerak: olinadigan tashuvchida fayllarni yaratish, ochish, o‘qish, yozish, bajarish, nomini o‘zgartirish, formatlash, o‘chirish.

Modul foydalanuvchilarning tashqi qurilmalarga kirish turlarini ko‘zda tutishi kerak: «kirishni taqiqlash», «to‘liq kirish» va «faqat o‘qish».

Modul ulangan tashqi USB-qurilmalarga yozishni fayllarning rasmiy belgilari (fayl nomi, formati), shuningdek uzatiladigan ma’lumotlar mazmuni asosida bloklash imkoniyatini ta’minlashi kerak.

Modul RDP-sessiyasi orqali uzatiladigan ma’lumotlarni nusxa ko‘chirishni taqiqlash imkoniyatini ta’minlashi kerak.

Modul masofaviy ish stantsiyalari yoki serverlarga, shuningdek moduli ishlaydigan ish stantsiyasi yoki serverga RDP-ulanishini cheklash imkoniyatini ta’minlashi kerak.

Modul foydalanuvchi kompyuterida ma'lum jarayonlarning ishga tushirilishini bloklash imkoniyatini ta’minlashi kerak.

Modul foydalanuvchi kompyuteridagi bufer almashuvini nazorat qilish, shuningdek ko‘chiriladigan ma’lumotlar mazmuni bo‘yicha bufer almashuvi orqali ma’lumot uzatishni bloklash imkoniyatini ta’minlashi kerak.

Modul foydalanuvchilarning ma'lum mahalliy papkalarga va/yoki mantiqiy disklarga (tizim disklaridan tashqari) kirishini bloklash imkoniyatini ta’minlashi kerak.

Modul foydalanuvchi keyinchalik cheksiz kirish yoki «faqat o‘qish» kirishiga ega bo‘ladigan qurilmalarning «oq ro‘yxatlaridan», shuningdek kirishga bloklash qilinadigan qurilmalarning «qora ro‘yxatlaridan» foydalanish imkoniyatini ta’minlashi kerak.

Modul ushlab olingan fayllarga atributlar belgilashni ta’minlashi kerak: domen hisob yozuvlari, fayl nomlari, qurilmalarning seriya raqamlari va boshqalar.

4.3.1.7. Monitor hodisalari va xodimlar harakatlari nazorat moduliga talablar

Modul belgilangan jadvalga muvofiq, jumladan berilgan internet-tugun, ish stantsiyasi operatsion tizimining jarayoniga bog‘liq holda va/yoki foydalanuvchi kalit so‘zlarni kiritganda foydalanuvchilar ish stantsiyalari ekranlarining suratlarini olishni ta’minlashi kerak.

Modul ma'lum (oldindan sozlangan) internet-tugunlarni tashrif buyurishda, qo‘ng‘iroq yoki video-konferensiya faollashtirilganda, klaviatura va sichqonchadan faollik bo‘lmaganda, «PrintScreen» tugmasi yoki Win+Shift+S tugmalar birikmasini bosganda skrinshot olish jadvalini sozlash imkoniyatini ta’minlashi kerak.

Modul sozlangan jadvalga yoki voqealarga muvofiq, jumladan berilgan internet-tugun, ish stantsiyasi operatsion tizimining jarayoniga bog‘liq holda va/yoki foydalanuvchi kalit so‘zlarni kiritganda monitorlar ekranlarida bo‘layotgan narsalarni video yozib olishni ta’minlashi kerak.

Modul belgilangan jadvalga muvofiq, jumladan berilgan ish stantsiyasi operatsion tizimining jarayoniga bog‘liq holda, bir nechta veb-kameradan foydalanish imkoniyati bilan ish stantsiyasiga ulangan veb-kamera orqali suratlar olish va video yozib olishni ta’minlashi kerak.

Modul ma'lum (oldindan sozlangan) internet-tugunlarni tashrif buyurishda, operatsion tizimda avtorizatsiya qilinganda, foydalanuvchi sessiyalari bo‘lmaganda surat olish jadvalini sozlash imkoniyatini ta’minlashi kerak.

Modul ekran surati va video yozuv olingan paytda kompyuter operatsion tizimi tomonidan bajariladigan jarayonlarni (fon va faol jarayonlarga bo‘lish bilan) ko‘rish imkoniyatini ko‘zda tutishi kerak.

Modul real vaqt rejimida bir yoki bir nechta foydalanuvchi ekrani faolligini bir vaqtda ko‘rish imkoniyatini ta’minlashi kerak.

Modul veb-kamera orqali foydalanuvchilarning ish stantsiyasidagi harakatlarini ko‘rish imkoniyatini ta’minlashi kerak.

Modul ushlab olingan ekran suratlari va video yozuvlarni alohida papkaga eksport qilish imkoniyatini ta’minlashi kerak.

Modul ishga tushirilgan har qanday ilovalarda, tizim tugmachalarini va ularning birikmasini bosishlarni ham o‘z ichiga olgan holda, tugmachalar bosishlarini nazorat qilishni ta’minlashi kerak.

Modul foydalanuvchi tomonidan bufer almashuviga joylashtirilgan matnli ma’lumotni nazorat qilishni ta’minlashi kerak.

Modul «PrintScreen» tugmasini bosishni bloklash imkoniyatini ta’minlashi kerak.

Modul kiritilgan belgilar parol kiritish bo‘lganda (texnik jihatdan mumkin bo‘lgan barcha holatlarda) ularni auditdan chiqarish imkoniyatini ta’minlashi va belgilashi kerak. Texnik imkoniyat Tizim Ishlab chiqaruvchisi tomonidan belgilanadi.

Modul domen foydalanuvchilari yoki jarayonlarga nisbatan tugmachalar bosishlarini jurnalga yozish qoidalarini belgilash imkoniyatini ta’minlashi kerak.

Modul berilgan foydalanuvchilar, kompyuterlar, ishga tushirilgan jarayonlar nomlari, MAC- va IP-manzillar, ilovada ishlash davomiyligi bo‘yicha ma'lum vaqt davri uchun klaviaturadan kiritilgan yoki bufer almashuviga joylashtirilgan mazmunni qidirish imkoniyatini ta’minlashi kerak.

Modul ushlab olingan tugmachalar bosishlarini alohida papkaga eksport qilish imkoniyatini ta’minlashi kerak.

4.3.1.8. Xodimlar suhbatlari nazorat moduliga talablar

Modul ulangan mikrofon (garnitura, noutbuk, veb-kamera va boshq.) yordamida, shuningdek tovush kartasining chiqishidan audio yozuv qilish imkoniyati bilan ofis ichida ham, ofisdan tashqarida ham bo‘layotgan voqealarning audio yozuvini ta’minlashi kerak.

Modul ovozlarni yozishni jadvalga muvofiq, ma'lum jarayonlar ishga tushirilganda, ofis ichida/tashqarisida (xizmat safarida), operatsion tizimda vakolatli foydalanuvchilar bo‘lmaganda faollashtirish, OT sozlamalarida foydalanuvchilar tomonidan mikrofonni o‘chirib qo‘yganda uni avtomatik faollashtirish, shuningdek yozib olinayotgan ovozli fayl sifatini sozlash imkoniyatini ko‘zda tutishi kerak.

Modul real vaqt rejimida ish stantsiyasiga ulangan mikrofonni tinglash imkoniyatini ta’minlashi kerak.

Modul yozib olingan ovozli fayllarni ma’lumotlar bazasiga joylashtirishni yoki ikkilik ma’lumotlarni saqlash uchun fayl xotirasidan foydalanishni ta’minlashi kerak.

Modul ushlab olingan suhbatlarni alohida papkaga eksport qilish imkoniyatini ta’minlashi kerak.

4.3.1.9. Foydalanuvchilar va ilovalar faolligi nazorat moduliga talablar

Modul xodimlarning ishga tushirilgan ilovalar yoki saytlardagi faolligini nazorat qilishni ta’minlashi kerak.

Modul xodimning kompyuter oldida haqiqiy ishlash vaqtini hisoblashni ta’minlashi kerak.

Modul oldindan yuklangan va muntazam to‘ldirib boriladigan sayt tasniflar bazasidan foydalangan holda tashrif buyurilgan saytlarni tematik guruhlarga avtomatik kategoriyalash imkoniyatini ulash imkoniyatiga ega bo‘lishi kerak.

4.3.1.10. Bulutli ma’lumotlar saqlash nazorat moduliga talablar

Modul Google Drive, Google Docs, OneDrive, SkyDrive, Office 365, DropBox, Evernote, Yandex.Disk, Cloud.mail.ru, Amazon S3, iCloud, DropMeFiles, OwnCloud, Pcloud, OziBox, MediaFire, OpenDrive, 4shared, Box, Syncplicity, CloudMe, MiMedia, My-Files, Nextcloud, Seafile, SharePoint, Acronis File Advanced, Cloudian S3 storage, Disk Bitrix24, Disk-O va boshqa bulutli xizmatlarning (Tizim Ishlab chiqaruvchisi xohishiga ko‘ra) kiruvchi va chiquvchi ma’lumotlarini nazorat qilish imkoniyatlarini ta’minlashi kerak.

Modul TeamViewer, RealVNC, Radmin, LiteManager va boshqa (Tizim Ishlab chiqaruvchisi xohishiga ko‘ra) masofaviy kirish dasturlarida uzatiladigan fayllarni nazorat qilishni ta’minlashi kerak.

Modul ushlab olingan hujjatlarga atributlar belgilashni ta’minlashi kerak: domen hisob yozuvlari, fayl nomi, IP-manzillar va boshqalar.

Modul HTTPS spetsifikatsiyasidan tashqari trafik bundan mustasno, veb-brauzer orqali bulutli xotiralarga belgilangan kontent va/yoki kontekstga muvofiq fayllarni yuborishni bloklash imkoniyatini ta’minlashi kerak.

4.3.1.11. Fayllar audit moduliga talablar

DLP dagi fayl auditi funksiyasi Tizim ish stantsiyasidagi, shuningdek tarmoq papkalaridagi fayllar va papkalar bilan operatsiyalar auditini o‘tkazish imkoniyatini ta’minlashi kerak. Quyidagi fayl operatsiyalari kuzatilishi kerak: yaratish, o‘qish, yozish, o‘chirish, nomini o‘zgartirish, ochish, kirish huquqlarini o‘zgartirish. Quyidagi papka operatsiyalari kuzatilishi kerak: yaratish, o‘chirish, nomini o‘zgartirish, ochish, kirish huquqlarini o‘zgartirish.

4.3.2. Linux OT uchun Agent funksiyalariga umumiy talablar

Linux OT uchun Agent elektron pochta, tezkor xabar almashish xizmatlari, FTP-ulanishlar, HTTP protokoli, bulutli xotiralar xizmatlari orqali uzatiladigan ma’lumotlarni nazorat qilishni, tashqi qurilmalardagi ma’lumotlarga kirishni nazorat qilish va boshqarishni, ma’lumotlarni chop etishni nazorat qilishni, monitordagi voqealar va harakatlarni, xodimlar suhbatlarini va ularning ilovalardagi faolligini, shuningdek xodimlar ish stantsiyalarida statik saqlangan fayllarni nazorat qilishni amalga oshirishi kerak.

4.3.2.1. Elektron pochta nazorat moduliga talablar

Modul har qanday pochta mijozlari yoki brauzerlar yordamida SMTP, POP3, IMAP, MAPI, HTTP protokollari (veb-pochta: ham chiquvchi, ham kiruvchi) bo‘yicha uzatiladigan xabarlar va ilovalarni nazorat qilish imkoniyatlarini ta’minlashi kerak. Kontent va/yoki kontekst tahlili asosida SMTP protokoli bo‘yicha chiquvchi pochta xabarlarini avtomatik to‘xtatishning ulanadigan funksiyasiga ega bo‘lishi kerak.

Modul ushlab olingan hujjatlarga atributlar belgilashni ta’minlashi kerak: domen hisob yozuvlari, yuboruvchi va oluvchilarning manzillari, xat mavzusi va boshqalar.

4.3.2.2. Tezkor xabar almashish xizmatlari nazorat moduliga talablar

Modul quyidagilarni nazorat qilishni ta’minlashi kerak:

- Facebook, LinkedIn, VKontakte, Odnoklassniki.ru, Mamba.ru va boshqa ijtimoiy tarmoqlarda (Tizim Ishlab chiqaruvchisi xohishiga ko‘ra) HTTP(S) protokoli bo‘yicha kiruvchi va chiquvchi xabarlar;

- Telegram desktop-versiyasi yordamida uzatilgan chatlar, qo‘ng‘iroqlar, chiquvchi fayllar;
- Bitrix24 ning veb-versiyasi chatlar va chiquvchi fayllar;
- Telegram (web.telegram.org), WhatsApp (web.whatsapp.com) veb-versiyalari chatlar.

Modul foydalanuvchi tomonidan HTTP-tunnellash qo‘llangan holda uzatilgan tezkor xabar almashish xizmatlari trafigini nazorat qilishni ta’minlashi kerak.

Modul ushlab olingan hujjatlarga atributlar belgilashni ta’minlashi kerak: domen hisob yozuvlari, yuboruvchi va oluvchilarning UIN lari, xabarlar soni va boshqalar.

4.3.2.3. FTP-ulanishlar nazorat moduliga talablar

Modul SSL-shifrlashdan foydalanishni o‘z ichiga olgan holda FTP-ulanishlar orqali yuklangan yoki uzatilgan hujjatlarni nazorat qilishni ta’minlashi kerak.

Modul ushlab olingan hujjatlarga atributlar belgilashni ta’minlashi kerak: domen hisob yozuvlari, maqsadli URL-manzillar, FTP-serverlar foydalanuvchilarining nomlari va boshqalar.

4.3.2.4. HTTP-trafik nazorat moduliga talablar

Modul POST-so‘rovlar (xabarlar va fayllar) nazorat qilish imkoniyatlarini ta’minlashi kerak.

Modul zamonaviy brauzerlar, jumladan Mozilla Firefox, Opera, Google Chrome tomonidan generatsiya qilinadigan so‘rovlarni filtrlashni qo‘llab-quvvatlashi kerak.

Modul foydalanuvchilar tomonidan mashhur qidiruv tizimlariga, jumladan Google, Yandex, Rambler, Yahoo ga yuborilgan GET-so‘rovlarni nazorat qilishni qo‘llab-quvvatlashi kerak.

Modul mashhur blog xizmatlari, veb-chatlar va mashhur forum dvigatellari (vBulletin, Invision Power Board, phpBB) tomonidan generatsiya qilinadigan so‘rovlarni filtrlashni qo‘llab-quvvatlashi kerak.

Modul faqat belgilar to‘plami ma'noli axborot tashuvchi ushlab olingan POST-so‘rovlarning qidiruv natijalarini ko‘rsatish imkoniyatini ko‘zda tutishi kerak.

Modul ushlab olingan hujjatlarga atributlar belgilashni ta’minlashi kerak: domen hisob yozuvlari, so‘rov tanasi, xost nomi va boshqalar.

4.3.2.5. Chop etish nazorat moduliga talablar

Modul mahalliy va tarmoq printerlari yordamida chop etishga yuborilgan hujjatlarni nazorat qilishni amalga oshirishi kerak.

Modul chop etishga yuborilgan hujjatlarning grafik tasviri va matnini ham nazorat qilishni amalga oshirishi kerak.

Modul ushlab olingan hujjatlarga atributlar belgilashni ta’minlashi kerak: domen hisob yozuvlari, printerlar nomlari, chop etilgan sahifalar soni va boshqalar.

Modul alohida printerlarni (shu jumladan ularning tavsifi va joylashuvi bo‘yicha), foydalanuvchilarni nazoratdan chiqarish imkoniyatini qo‘llab-quvvatlashi kerak.

4.3.2.6. Olinadigan qurilmalar nazorat va boshqarish moduliga talablar

Modul foydalanuvchining tashqi qurilmalarga (USB olinadigan xotiralar va tarmoq adapterlar) va portlarga (COM, LPT) kirish nazorat imkoniyatlarini ta’minlashi kerak.

Modul terminal sessiyasida ishlashni qo‘llab-quvvatlashi kerak.

Modul qurilmalar va portlarning vakolatli foydalanuvchilar guruhlarini aniqlashni ta’minlashi kerak.

Modul tashqi USB-qurilmaga yoziladigan ma’lumotlarni soya nusxa olish imkoniyatini ta’minlashi kerak.

Modul audit jurnalida barcha voqealarni qayd etishni ta’minlashi kerak: olinadigan tashuvchida fayllarni yaratish, ochish, o‘qish, yozish, bajarish, nomini o‘zgartirish, formatlash, o‘chirish.

Modul foydalanuvchilarning tashqi qurilmalarga kirish turlarini ko‘zda tutishi kerak: «kirishni taqiqlash», «to‘liq kirish» va «faqat o‘qish».

Modul ushlab olingan fayllarga atributlar belgilashni ta’minlashi kerak: domen hisob yozuvlari, fayl nomlari, qurilmalarning seriya raqamlari va boshqalar.

4.3.2.7. Monitor hodisalari va xodimlar harakatlari nazorat moduliga talablar

Modul belgilangan jadvalga muvofiq, jumladan berilgan internet-tugun, ish stantsiyasi operatsion tizimining jarayoniga bog‘liq holda foydalanuvchilar ish stantsiyalari ekranlarining suratlarini olishni ta’minlashi kerak.

Modul ma'lum (oldindan sozlangan) internet-tugunlarni tashrif buyurishda, ma'lum (oldindan sozlangan) jarayonlar ishga tushirilganda, klaviatura va sichqonchadan faollik bo‘lmaganda, «PrintScreen» tugmasi bosilganda skrinshot olish jadvalini sozlash imkoniyatini ta’minlashi kerak.

Modul monitorlar ekranlarida bo‘layotgan narsalarni video yozib olishni ta’minlashi kerak. Modul ish stantsiyasining klaviaturasi va sichqonchasidan faollik bo‘lmaganda ekranni yozib olishni to‘xtatish imkoniyatini ta’minlashi kerak.

Modul belgilangan jadvalga muvofiq, jumladan foydalanuvchi operatsion tizimga kirganida, bir nechta veb-kameradan foydalanish imkoniyati bilan ish stantsiyasiga ulangan veb-kamera orqali suratlar olishni ta’minlashi kerak.

Modul real vaqt rejimida foydalanuvchi ekrani faolligini ko‘rish imkoniyatini ta’minlashi kerak.

Modul veb-kamera orqali foydalanuvchilarning ish stantsiyasidagi harakatlarini ko‘rish imkoniyatini ta’minlashi kerak.

Modul ekran surati olingan paytda kompyuter operatsion tizimi tomonidan bajariladigan jarayonlarni (fon va faol jarayonlarga bo‘lish bilan) ko‘rish imkoniyatini ko‘zda tutishi kerak.

Modul ishga tushirilgan har qanday ilovalarda, tizim tugmachalarini va ularning birikmasini bosishlarni ham o‘z ichiga olgan holda, tugmachalar bosishlarini nazorat qilishni ta’minlashi kerak.

Modul foydalanuvchi tomonidan bufer almashuviga joylashtirilgan matnli ma’lumotni nazorat qilishni ta’minlashi kerak.

Modul domen foydalanuvchilari yoki jarayonlarga nisbatan tugmachalar bosishlarini jurnalga yozish qoidalarini belgilash imkoniyatini ta’minlashi kerak.

4.3.2.8. Xodimlar suhbatlari nazorat moduliga talablar

Modul ulangan mikrofon (garnitura, noutbuk, veb-kamera va boshq.) yordamida ofis ichida ham, ofisdan tashqarida ham bo‘layotgan voqealarning audio yozuvini ta’minlashi kerak.

Modul real vaqt rejimida ish stantsiyasiga ulangan mikrofonni tinglash imkoniyatini ta’minlashi kerak.

Modul ovozlarni yozishni jadvalga muvofiq, ofis ichida/tashqarisida (xizmat safarida) faollashtirish, shuningdek yozib olinayotgan ovozli fayl sifatini sozlash imkoniyatini ko‘zda tutishi kerak.

4.3.2.9. Foydalanuvchilar va ilovalar faolligi nazorat moduliga talablar

Modul xodimlarning ishga tushirilgan ilovalar yoki saytlardagi faolligini nazorat qilishni ta’minlashi kerak.

Modul xodimning kompyuter oldida haqiqiy ishlash vaqtini hisoblashni ta’minlashi kerak.

4.3.3. MacOS OT uchun Agent funksiyalariga umumiy talablar

MacOS OT uchun Agent monitordagi voqealar va xodimlar harakatlarini, ularning ilovalardagi faolligini nazorat qilishni amalga oshirishi kerak.

4.3.3.1. Monitor hodisalari va xodimlar harakatlari nazorat moduliga talablar

Modul belgilangan jadvalga muvofiq, jumladan berilgan ish stantsiyasi operatsion tizimining jarayoniga bog‘liq holda foydalanuvchilar ish stantsiyalari ekranlarining suratlarini olishni ta’minlashi kerak.

Modul ekran surati olingan paytda kompyuter operatsion tizimi tomonidan bajariladigan jarayonlarni (fon va faol jarayonlarga bo‘lish bilan) ko‘rish imkoniyatini ko‘zda tutishi kerak.

Modul ishga tushirilgan har qanday ilovalarda, tizim tugmachalarini va ularning birikmasini bosishlarni ham o‘z ichiga olgan holda, tugmachalar bosishlarini nazorat qilishni ta’minlashi kerak.

Modul domen foydalanuvchilari yoki jarayonlarga nisbatan tugmachalar bosishlarini jurnalga yozish qoidalarini belgilash imkoniyatini ta’minlashi kerak.

4.3.3.2. Foydalanuvchilar va ilovalar faolligi nazorat moduliga talablar

Modul xodimlarning ishga tushirilgan ilovalardagi faolligini nazorat qilishni ta’minlashi kerak.

Modul xodimning kompyuter oldida haqiqiy ishlash vaqtini hisoblashni ta’minlashi kerak.

4.3.4. Tarmoq ushlab olish darajasida ma’lumotlarni nazorat qilish funksiyalariga talablar (proksi-server bilan integratsiya (ICAP protokoli bo‘yicha) yoki trafik ko‘zgulash (SPAN) orqali tarmoq uskunasi bilan)

4.3.4.1. Elektron pochta nazorat moduliga talablar

Modul pochta mijozlari yoki brauzerlar yordamida SMTP, POP3, IMAP, HTTP protokollari (veb-pochta: ham chiquvchi, ham kiruvchi) bo‘yicha uzatiladigan xabarlar va ilovalarni nazorat qilish imkoniyatlarini ta’minlashi kerak. Bunda shifrlangan bo‘lmagan HTTP trafigi ham ko‘zgulash rejimida, ham proksi-server bilan integratsiya rejimida mavjud. Shifrlangan bo‘lmagan SMTP, POP3 va IMAP trafigi faqat ko‘zgulash rejimida mavjud. Shifrlangan HTTP(S) trafigi faqat sertifikat almashtirish amalga oshiriladigan proksi-server bilan integratsiya rejimida mavjud.

Modul ushlab olingan hujjatlarga atributlar belgilashni ta’minlashi kerak: domen hisob yozuvlari, yuboruvchi va oluvchilarning manzillari, xat mavzusi va boshqalar.

4.3.4.2. Tezkor xabar almashish xizmatlari nazorat moduliga talablar

Modul sertifikat almashtirish amalga oshiriladigan proksi-server bilan integratsiya rejimida nazorat qilishni ta’minlashi kerak:

- Facebook, LinkedIn, VKontakte, Moy Mir@Mail.ru, Odnoklassniki.ru, Mamba.ru va boshqa ijtimoiy tarmoqlarda (Tizim Ishlab chiqaruvchisi xohishiga ko‘ra) HTTP(S) protokoli bo‘yicha kiruvchi va chiquvchi xabarlar;
- Telegram (web.telegram.org), WhatsApp (web.whatsapp.com), Rocket.chat, Mattermost messenjerlarining veb-versiyalari chatlar va fayllar;
- Instagram, VK Teams fayl uzatish tarixi va chatlari;
- slack.com resursi xabarlari va fayllari.

Modul HTTP protokoli bo‘yicha ijtimoiy tarmoqlarda va veb-messenjerlar (Rocket.chat, Mattermost va boshq.) orqali uzatiladigan xabarlar va fayllarni belgilangan kontekstga muvofiq bloklash imkoniyatini ta’minlashi kerak.

Modul foydalanuvchi tomonidan HTTP-tunnellash qo‘llangan holda uzatilgan tezkor xabar almashish xizmatlari trafigini nazorat qilishni ta’minlashi kerak.

Modul ushlab olingan hujjatlarga atributlar belgilashni ta’minlashi kerak: domen hisob yozuvlari, yuboruvchi va oluvchilarning UIN lari, xabarlar soni va boshqalar.

4.3.4.3. FTP-ulanishlar nazorat moduliga talablar

Modul sertifikat almashtirish amalga oshiriladigan proksi-server bilan integratsiya rejimida SSL-shifrlashdan foydalanishni o‘z ichiga olgan holda FTP-ulanishlar orqali yuklangan yoki uzatilgan hujjatlarni nazorat qilishni ta’minlashi kerak.

Modul ushlab olingan hujjatlarga atributlar belgilashni ta’minlashi kerak: domen hisob yozuvlari, maqsadli URL-manzillar, FTP-serverlar foydalanuvchilarining nomlari va boshqalar.

Modul ushlab olingan hujjatlarni maxsus fayl xotirasiga joylashtirishni ta’minlashi kerak.

4.3.4.4. HTTP-trafik nazorat moduliga talablar

Himoyalangan HTTPS trafigini nazorat qilish faqat sertifikat almashtirish amalga oshiriladigan proksi-server bilan integratsiya rejimida mavjud bo‘lishi mumkin.

Himoyalanmagan HTTP trafigini nazorat qilish ham proksi-server bilan integratsiya rejimida, ham trafik ko‘zgulash rejimida mavjud bo‘lishi mumkin.

Modul POST-so‘rovlar (xabarlar va fayllar) nazorat qilish imkoniyatlarini ta’minlashi kerak.

Modul zamonaviy brauzerlar, jumladan Internet Explorer, Mozilla Firefox, Opera, Google Chrome tomonidan generatsiya qilinadigan so‘rovlarni filtrlashni qo‘llab-quvvatlashi kerak.

Modul foydalanuvchilar tomonidan mashhur qidiruv tizimlariga, jumladan Google, Yandex, Rambler, Yahoo ga yuborilgan GET-so‘rovlarni nazorat qilishni qo‘llab-quvvatlashi kerak.

Modul mashhur blog xizmatlari, veb-chatlar va mashhur forum dvigatellari (vBulletin, Invision Power Board, phpBB) tomonidan generatsiya qilinadigan so‘rovlarni filtrlashni qo‘llab-quvvatlashi kerak.

Modul faqat belgilar to‘plami ma'noli axborot tashuvchi ushlab olingan POST-so‘rovlarning qidiruv natijalarini ko‘rsatish imkoniyatini ko‘zda tutishi kerak.

Modul HTTP(S) bo‘yicha taqiqlangan internet-resurslarni tashrif buyurishni bloklash, «oq» va «qora» istisnolar ro‘yxatlarini yaratish, shuningdek internet-resurslarni bloklash va/yoki tashrif buyurishga ruxsat berish uchun sayt toifalaridan foydalanish imkoniyatini ko‘zda tutishi kerak; taqiqlangan internet-resursga kirishni bloklashda ko‘rsatiladigan bildirishnomani sozlash imkoniyatini ko‘zda tutishi kerak.

Modul belgilangan kontekstga muvofiq so‘rovlarni uzatishni bloklash imkoniyatini ta’minlashi kerak.

Modul ushlab olingan hujjatlarga atributlar belgilashni ta’minlashi kerak: domen hisob yozuvlari, so‘rov tanasi, xost nomi va boshqalar.

5. Barcha dasturiy ta’minotga boshqa talablar

5.1. O‘rnatish va sozlash xizmatlariga talablar

Ta’minotchi sotib olingan yechimning har bir tarkibiy qismini yetkazib berish sanasidan boshlab 30 (o‘ttiz) kun ichida o‘rnatishi kerak. Xizmatlar “to‘liq yakunlangan” shartlarida ko‘rsatiladi.

5.2. Qo‘shimcha talablar

Tanlov ishtirokchisining taklifiga barcha dasturiy mahsulotlar bo‘yicha vakolatli o‘qitish – kamida 2 nafar xodim uchun kiritilishi kerak.

Barcha tizimlarni “Mutlaq foydalanishga tayyor” shartlarida joriy etish va kafolat muddati davomida qo‘llab-quvvatlash.

Bank axborot tizimida amalda mavjud bo‘lgan 200 ta litsenziyaning texnik qo‘llab-quvvatlash muddati yakunlangandan so‘ng yangi sotib olingan litsenziyalar uchun amal qiluvchi texnik qo‘llab-quvvatlash doirasida davom ettirilishi ko‘zda tutilgan bo‘lishi kerak (amaldagi litsenziya uchun texnik qo‘llab quvvatlash muddati 3-dekabr 2026-yilgacha).

6. Texnik qo‘llab-quvvatlash shartlari

Ijrochi quyidagi shartlarda texnik qo‘llab-quvvatlash xizmatini ko‘rsatishi shart:

- Xizmat ko‘rsatish muddati: litsenziyalar topshirilgan sanadan boshlab 12 (o‘n ikki) kalendar oy;
- Texnik qo‘llab-quvvatlash doirasida dasturiy ta’minotning yangi versiyalari va yangilanishlaridan foydalanish huquqi taqdim etiladi;
- Texnik yordam masofaviy ko‘rinishda, zarur hollarda esa Buyurtmachi ofisida ko‘rsatiladi;
- Ijrochi tarkibida kamida 2 (ikki) nafar sertifikatlangan texnik qo‘llab-quvvatlash muhandisi bo‘lishi shart.

Xizmat ko‘rsatish darajasi (SLA) quyidagi ko‘rsatkichlardan kam bo‘lmasligi lozim:

Muhimlik darajasi	Qo‘llab-quvvatlash xizmati mutaxassisining reaksiya vaqti	Vaqtinchalik yechim taqdim etish muddati	Muammoni hal qilish yechimini taqdim etish muddati
Juda shoshilinch	Ish kuni davomida xizmat ko‘rsatish so‘rovi joylashtirilgan vaqtdan boshlab 4 soat	2 ish kunidan ko‘p bo‘lmagan muddat	Xizmat ko‘rsatish so‘rovi joylashtirilgan vaqtdan boshlab 20 ish kunidan ko‘p bo‘lmagan muddat
Shoshilinch	Ish kuni davomida xizmat ko‘rsatish so‘rovi joylashtirilgan vaqtdan boshlab 8 soat	5 ish kunidan ko‘p bo‘lmagan muddat	Xizmat ko‘rsatish so‘rovi joylashtirilgan vaqtdan boshlab 30 ish kunidan ko‘p bo‘lmagan muddat
Muhim	Xizmat ko‘rsatish so‘rovi joylashtirilgan vaqtdan boshlab 2 ish kuni	15 ish kunidan ko‘p bo‘lmagan muddat	Xizmat ko‘rsatish so‘rovi joylashtirilgan vaqtdan boshlab 50 ish kunidan ko‘p bo‘lmagan muddat
Kritik bo‘lmagan	Xizmat ko‘rsatish so‘rovi joylashtirilgan vaqtdan boshlab 3 ish kuni	30 ish kunidan ko‘p bo‘lmagan muddat	Xizmat ko‘rsatish so‘rovi joylashtirilgan vaqtdan boshlab 90 ish kunidan ko‘p bo‘lmagan muddat

7. Xodimlarni o‘qitish shartlari

7.1. O‘qitish hajmi va yo‘nalishlari

Ijrochi Buyurtmachining kamida 2 (ikki) nafar xodimini DLP tizimi bo‘yicha o‘qitishni ta’minlashi shart. O‘quv mashg’ulotlari uchun minimal mavzular quyidagicha tashlil etiladi:

Kurs turi	Mavzular
DLP tizimi administratorligi (1 nafar xodim)	• DLP tizimlarini o‘rnatish • Server komponentlarini sozlash va boshqarish • Agentlarni tarqatish va boshqarish • Tizim arxitekturasi va integratsiya masalalari • Ma’lumotlar bazasini boshqarish • Zaxiralash va avariyadan tiklash jarayonlari • Tizim monitoringi va nosozliklarni bartaraf etish

DLP tizim analitikasi yoki tizimni joriy qilish amaliyoti (1 nafar xodim)	• Axborot xavfsizligi siyosatlarini yaratish va sozlash • DLP hodisalarini monitoring qilish va tahlil qilish • AlertCenter va ReportCenter modullari bilan ishlash • Qoidabuzarliklarni aniqlash va tekshirish • FileAuditor modulida ma’lumotlarni klassifikatsiya qilish • Audit va hisobotlarni shakllantirish • Axborot sizib chiqishi bilan bog‘liq insidentlarni tahlil qilish

7.2. Xodimlarni o‘qitishga qo‘yiladigan talablar

- O‘qitish ishlab chiqaruvchi yoki uning rasmiy vakolatli hamkori tomonidan o‘tkazilishi shart;
- O‘qitish tizim joriy etilgandan so‘ng, amaliy mashg‘ulotlarni o‘z ichiga olgan holda o‘tkaziladi;
- O‘qitish yakunida har bir tinglovchiga kursni muvaffaqiyatli tamomlaganligini tasdiqlovchi sertifikat yoki rasmiy guvohnoma berilishi shart;
- O‘qitish xarajatlari (o‘quv materiallari, imtihonlar, sertifikatlash) shartnoma qiymatiga kiritilgan bo‘lishi lozim.
- O‘quv mashg‘ulotlari O‘zbekiston Respublikasi hududida yoki chet el davlatlarida o‘tkazilishi mumkin.

8. Muhim shartlar va muddatlar

Shart	Ko‘rsatkich
Yetkazib berish muddati	Shartnoma tuzilgan sanadan boshlab 10 (o‘n) kalendar kun ichida
To‘lov muddati	Hisob-faktura sanasidan boshlab 10 (o‘n) kalendar kun ichida
To‘lov shartlari	Xizmat ko‘rsatish sertifikati olingandan so‘ng — 100% miqdorda
Litsenziyalar turi	Muddatsiz (perpetual) litsenziyalar
Kafolat qo‘llab-quvvatlash	Dalolatnoma imzolangan sanadan boshlab 12 kalendar oy
O‘qitish muddati	Tizim joriy etilgandan so‘ng kelishilgan muddatda (12-oygacha)
Litsenziya maqomi	Rasmiy, yangi, foydalanish huquqini tasdiqlovchi hujjatlar bilan

kelishuvchilar: B.Shamsiev, Z.Orifkhojayev