

“TASDIQLAYMAN”

“Agrobank” ATB

Boshqaruv raisi o'rinbosari v.b.



F.B.Nasriyev

2026 yil “31” iyul

Falcongaze SecureTower dasturiy ta'minoti uchun litsenziyalarni xarid qilish hamda texnik qo'llab-quvvatlash xizmatini uzaytirish bo'yicha

TEXNIK TOPSHIRIQ

Toshkent – 2026y.

Umumiy ma'lumotlar

«Agrobank» ATB ehtiyojlari uchun tovarlar va xizmatlarni xarid qilish doirasida Yetkazib beruvchi mazkur texnik topshiriqda belgilangan quyidagi texnik talablarga muvofiq Falcongaze SecureTower dasturiy ta'minoti uchun litsenziyalarni xarid qilish hamda texnik qo'llab-quvvatlash xizmatini uzaytirish bo'yicha xizmatlarni ko'rsatishi lozim.

1.1. Xizmatning to'liq nomi

Falcongaze SecureTower dasturiy ta'minoti uchun litsenziyalarni xarid qilish hamda texnik qo'llab-quvvatlash xizmatini uzaytirish.

Ijrochi: Ijrochi tashkilot nomi (bundan buyon matnda – Ijrochi).

Buyurtmachi: Buyurtmachi tashkilot nomi – «Agrobank» ATB (Toshkent shahri, Shayxontohur tumani, B. Zokirov ko'chasi, 2A-uy).

1.2. Tizimni joriy etishdan maqsad

Tizimni joriy etishdan maqsad maxfiy axborot va bank sirining sizib chiqishini oldini olish, korporativ aloqa kanallari orqali ma'lumotlar uzatilishini nazorat qilish, ichki tahdidlarni aniqlash, axborot xavfsizligi talablari hamda amaldagi qonunchilikka rioya etilishini ta'minlash, shuningdek axborotning komprometatsiya qilinishi bilan bog'liq moliyaviy, operatsion va reputatsion xatarlarni kamaytirishdan iborat.

1.3. Tizimni amalga oshirish uchun asos

Mazkur texnik topshiriqni ishlab chiqish uchun asos bo'lib O'zbekiston Respublikasi Markaziy banki Boshqaruvining 2025-yil 1-avgustdagi 19/1-son qarori hamda O'zbekiston Respublikasi Adliya vazirligi tomonidan 2025-yil 18-avgustda 3669-son bilan davlat ro'yxatidan o'tkazilgan «O'zbekiston Respublikasi tijorat banklarining axborot xavfsizligi va kiberxavfsizligiga qo'yiladigan minimal talablar to'g'risidagi nizomni tasdiqlash haqida»gi hujjat hisoblanadi.

Mazkur hujjat tijorat banklarining axborot xavfsizligi hodisalarini monitoring qilish jarayonlarini tashkil etish, kiberxavfsizlik insidentlarini aniqlash va ularga javob qaytarish, shuningdek axborot tizimlarining himoyalanganlik holatini nazorat qilish bo'yicha talablarni belgilaydi.

1.4. Ishtirokchiga qo'yiladigan talablar

Ijrochi quyidagi ma'lumotlarni majburiy tartibda taqdim etishi shart:

1.4.1. Ushbu loyiha bo'yicha tanlovda ishtirok etish uchun taklif etilayotgan uskunalar ishlab chiqaruvchisining mintaqaviy tarkibiy bo'linmalari tomonidan berilgan avtorizatsiya (MAF) hujjatlarining mavjudligi.

1.4.2. Kafolatli xizmat ko'rsatishni ta'minlash maqsadida O'zbekiston

Respublikasi hududida ishlab chiqaruvchi tomonidan vakolat berilgan servis markazlari va/yoki ehtiyot qismlar omborlari mavjudligi to'g'risidagi ma'lumot.

1.4.3. Buyurtmachining obyektlarida tizimni joriy etish jarayonida axborot sizib chiqishining oldini olish hamda o'z xodimlari uchun mehnat va texnika xavfsizligini ta'minlash bo'yicha barcha zarur choralarni ko'rishi.

1.4.4. Yetkazib berilayotgan yechim kiberxavfsizlik talablari bo'yicha sertifikatlangan yoki sertifikatlashdan o'tishga tayyor ekanligini kafolatlashi.

1.4.5. Ishtirokchi har bir texnik talablar bandlariga muvofiqlikni namoyish etuvchi texnik taklifni taqdim etishi lozim.

2.1. DLP SecureTower tizimining funksional imkoniyatlariga qo'yiladigan talablar

500 nafar foydalanuvchi uchun **Falcongaze SecureTower** dasturiy ta'minotining yangilanishlaridan (yangi versiyalaridan) foydalanish litsenziyasi.

Dasturiy ta'minot litsenziyasi — dasturiy ta'minotning funksional imkoniyatlaridan foydalanish uchun beriladigan **eksklyuziv bo'lmagan foydalanish huquqi** bo'lib, u mutlaq (eksklyuziv) huquq amal qiladigan muddat davomida (muddatsiz litsenziya) taqdim etiladi.

Xarid qilinayotgan dasturiy ta'minot kamida **12 oy** kafolatli texnik qo'llab-quvvatlash xizmatiga ega bo'lishi lozim.

Taklif etilayotgan dasturiy ta'minot mazkur Texnik topshiriq talablariga to'liq mos kelishi shart.

Agent yordamida ma'lumotlarni tutib olish

2.2. Agent orqali HTTP/HTTPS trafikni nazorat qilish bo'yicha talablar

Tizim HTTP protokoli va uning shifrlangan HTTPS analogi orqali uzatilayotgan kiruvchi hamda chiquvchi axborotni nazorat qilish imkoniyatiga ega bo'lishi va quyidagi funksiyalarni ta'minlashi lozim:

1. Muayyan chiquvchi va kiruvchi ma'lumotlarni tutib olishdan istisno qilish maqsadida HTTP so'rov parametrlariga asoslangan oldindan belgilangan hamda foydalanuvchi tomonidan yaratilgan qoidalar bo'yicha filtrlarni yaratish va moslashuvchan sozlash imkoniyati.

2. Oldindan belgilangan hamda foydalanuvchi tomonidan yaratilgan qoidalarga muvofiq **MIME turlari** bo'yicha ma'lumotlarni tutib olishni filtrlash imkoniyati.

3. Uzatilayotgan ma'lumotlarni nazorat qilishda HTTP metodlari tanlanganda **GET/POST/PUT** so'rovlarini tutib olish, tahlil qilish, filtrlash va bloklash imkoniyati.

4. Bloglar, forumlar, fayl almashish servislari va boshqa veb-xizmatlarga yuborilgan xabarlar hamda fayllarni tutib olish va tahlil qilish.

5. Foydalanuvchining qidiruv so'rovlarini tutib olish va tahlil qilish.

6. Foydalanuvchi tashrif buyurgan barcha veb-sahifalar manzillarini saqlash.

7. Quyidagi veb-resurslarda amalga oshirilgan veb-kommunikatsiyalarning (chat yozishmalari, statuslar, izohlar va boshqalar) kiruvchi hamda chiquvchi ma'lumotlarini tutib olish: Facebook, Twitter, VKontakte, Odnoklassniki.

8. Veb-pochta xizmatlari (**Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex, Zimbra** va boshqalar) orqali yuborilgan yoki qabul qilingan elektron xatlar hamda ularning ilovalarini tutib olish.

9. Quyidagi messenjerlarning veb-mijozlari orqali uzatilgan xabarlar va fayllarni tutib olish: Skype, Telegram, WhatsApp, Discord, Microsoft Teams, Slack, ICQ, Google Hangouts, Rocket.Chat.

10. Belgilangan axborot xavfsizligi siyosatlari asosida muayyan axborotni o'z ichiga olgan xabarlar va fayllarni avtomatik aniqlash hamda bunday ma'lumot aniqlanganda axborot xavfsizligi uchun mas'ul shaxsga avtomatik bildirishnoma yuborish.

11. HTTP(S) protokoli orqali uzatilgan xabarlar va fayllarni ularning matni hamda atributlari bo'yicha qidirish imkoniyati.

12. Quyidagi mezonlar asosida veb-resurslarga tashrif buyurishni, chiquvchi xabarlar va fayllarni bloklash imkoniyati:

- kontent bo'yicha;
- atributlar to'plami bo'yicha;
- maxfiylik belgisi mavjudligi bo'yicha;
- yuborilayotgan faylning xesh-summasi bo'yicha.

13. Qidiruv lug'atlari va raqamli izlar (digital fingerprints) asosida veb-resurslarga tashrif buyurishni, chiquvchi xabarlar va fayllarni bloklash imkoniyati.

14. HTTP(S) trafikini bloklash to'g'risidagi foydalanuvchi xabarini sozlash imkoniyati, jumladan:

- barcha bloklash qoidalari uchun umumiy xabarni;
- alohida bloklash qoidasi uchun individual xabarni sozlash.

2.3. Agent orqali FTP/FTPS trafikini nazorat qilish bo'yicha talablar

Tizim **FTP protokoli** va uning shifrlangan analogi orqali uzatiladigan kiruvchi hamda chiquvchi fayllarni nazorat qilish imkoniyatiga ega bo'lishi hamda quyidagi funksiyalarni ta'minlashi lozim:

1. FTP ulanishi, shuningdek **SSL** bilan shifrlangan ulanish orqali uzatilayotgan kiruvchi va chiquvchi fayllarni tutib olish.

2. Tutib olinadigan fayllarning maksimal hajmini cheklashni sozlash imkoniyati.

3. Belgilangan axborot xavfsizligi siyosatlari asosida muayyan axborotni o'z ichiga olgan fayllarni avtomatik aniqlash hamda bunday axborot aniqlanganda axborot xavfsizligi uchun mas'ul shaxsga avtomatik bildirishnoma yuborish.

4. FTP(S) protokoli orqali uzatilgan fayllarni ularning matni va atributlari bo'yicha, jumladan shablonlardan foydalangan holda qidirish imkoniyati.

5. FTP protokoli orqali fayllarni yuborishni bloklash imkoniyati.

2.4. Agent orqali elektron pochta trafikini nazorat qilish bo'yicha talablar

Tizim kiruvchi va chiquvchi elektron pochta xabarlarini hamda ularning ilovalarini nazorat qilish imkoniyatiga ega bo'lishi va quyidagi funksiyalarni ta'minlashi lozim:

1. **IMAP, POP3, SMTP, MAPI** protokollari, shuningdek ularning shifrlangan analoglari orqali uzatiladigan elektron pochta xabarlarini tutib olish.

2. Muayyan kontaktlarning elektron pochta xabarlarini tutib olishdan istisno qilishni sozlash imkoniyati.

3. **S/MIME** himoyalangan elektron pochta standartini qo'llab-quvvatlovchi pochta dasturlari orqali yuborilgan elektron pochta xabarlarini agent yordamida tutib olish hamda xat mazmunini avtomatik shifrdan chiqarishni ta'minlash.

4. **Microsoft Outlook** bilan integratsiya orqali elektron pochta xabarlarini tutib olish.

5. **HTTP(S)** protokoli orqali ishlovchi veb-pochta xizmatlari (**Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex, Zimbra** va boshqalar) yordamida yuborilgan yoki qabul qilingan elektron pochta xabarlarini tutib olish va tahlil qilish.

6. Elektron pochta xabarlariga biriktirilgan fayllarni tutib olish va tahlil qilish.

7. Belgilangan axborot xavfsizligi siyosatlari asosida muayyan axborotni o'z ichiga olgan elektron pochta xabarlarini va ularning ilovalarini avtomatik aniqlash

hamda bunday axborot aniqlanganda axborot xavfsizligi uchun mas'ul shaxsga avtomatik bildirishnoma yuborish.

8. Belgilangan axborot xavfsizligi siyosatlariga muvofiq agent moduli tomonidan **SMTP(S)**, **HTTP(S)** va **MAPI** protokollari orqali yuborilayotgan elektron pochta xabarlarini bloklash imkoniyati. Bloklash xabarlarining kontenti va atributlarini tahlil qilish, jumladan qo'shimcha atributlar, xat sarlavhasining ixtiyoriy maydonlari hamda yuborilayotgan fayllarning xesh-summalari asosida amalga oshirilishi lozim.

9. Agent moduli tomonidan **SMTP(S)**, **HTTP(S)** va **MAPI** protokollari orqali yuborilayotgan elektron pochta xabarlarini qidiruv lug'atlari va raqamli izlar (**digital fingerprints**) asosida bloklash imkoniyati.

10. Elektron pochta xabarlarini **HTML** formatida hamda **Microsoft Outlook** bilan mos keluvchi formatda saqlash imkoniyati.

11. Elektron pochta xabarlari va ularga biriktirilgan fayllarni matni va atributlari bo'yicha, jumladan shablonlardan foydalangan holda qidirish imkoniyati.

2.5. Messenjerlardagi yozishmalarni nazorat qilish bo'yicha talablar

Tizim foydalanuvchilarning yozishmalari, yuborilayotgan fayllar hamda messenjer dasturlari orqali amalga oshirilayotgan suhbatlarni nazorat qilish imkoniyatiga ega bo'lishi va quyidagi funksiyalarni ta'minlashi lozim:

1. Quyidagi messenjerlarda matnli xabarlarini tutib olish:

- Viber;
- Telegram (veb-versiyasi bilan birga);
- WhatsApp (veb-versiyasi bilan birga);
- Skype (veb-versiyasi bilan birga);
- Microsoft Lync;
- Microsoft Teams (veb-versiyasi bilan birga);
- Discord (veb-versiyasi bilan birga);
- Hangouts;
- Slack (veb-versiyasi bilan birga);
- WeChat;
- Signal;
- Express;
- Vk Teams;
- TrueConf;

- Agent Mail.ru;
- ICQ10;
- ICQ;
- Rocket.Chat;
- shuningdek **SIP, OSCAR, XMPP (jumladan HTTP orqali XMPP)** va **YMSG** protokollaridan foydalanuvchi messenjerlarda.

2. Quyidagi messenjerlar orqali uzatilayotgan fayllarni tutib olish:

- Viber;
- Telegram;
- WhatsApp (veb-versiyasi bilan birga);
- Skype (veb-versiyasi bilan birga);
- Microsoft Lync;
- Rocket.Chat;
- Microsoft Teams (veb-versiyasi bilan birga);
- Discord (veb-versiyasi bilan birga);
- Slack (veb-versiyasi bilan birga);
- Signal;
- Express;
- Vk Teams;
- TrueConf.

3. Quyidagi platformalar orqali amalga oshirilgan ovozli suhbatlarni tutib olish va ularni **MP3** formatidagi fayllar ko‘rinishida saqlash:

- Skype (jumladan Skype-to-Skype va Skype-to-Phone qo‘ng‘iroqlari);
- Microsoft Lync;
- Viber;
- Zoom;
- Telegram;
- WhatsApp;
- Signal;
- Express;
- Vk Teams;
- TrueConf;
- SIP protokoli.

4. Microsoft Lync, Skype, Viber, Zoom, Telegram, WhatsApp, Signal, Express, Vk Teams, TrueConf va SIP orqali amalga oshirilgan ovozli suhbatlarni

avtomatik ravishda matn ko‘rinishiga o‘tkazish (nutqni matnga aylantirish) imkoniyati.

5. Saqlangan Microsoft Lync, Skype, Viber, Zoom, Telegram, WhatsApp, Signal, Express, Vk Teams, TrueConf va SIP suhbatlarini qayta tinglash imkoniyati.

6. Alohida foydalanuvchi hisoblari bo‘yicha ma’lumotlarni tutib olishni cheklash imkoniyati.

7. Belgilangan axborot xavfsizligi siyosatlariga muvofiq muayyan axborotni o‘z ichiga olgan xabarlar va fayllarni avtomatik aniqlash hamda bunday holat aniqlanganda axborot xavfsizligi uchun mas’ul shaxsga avtomatik bildirishnoma yuborish.

8. Messenjerlar orqali uzatilgan xabarlar va fayllarni ularning matni va atributlari bo‘yicha, jumladan shablonlardan foydalangan holda qidirish imkoniyati.

9. Quyidagi messenjerlarning veb-mijozlari orqali uzatilgan xabarlar va fayllarni tutib olish:

- Skype;
- Telegram;
- WhatsApp;
- Discord;
- Microsoft Teams;
- Slack;
- ICQ;
- Google Hangouts.

10. **Facebook** va **LinkedIn** platformalaridagi yozishmalar hamda postlarni nazorat qilish.

11. **Instagram** platformasidagi yozishmalarni nazorat qilish.

12. **Bitrix24** CMS tizimidagi yozishmalar, elektron pochta va fayllarni nazorat qilish.

13. Messenjerlarga yuborilayotgan fayllarni ularning atributlari to‘plami hamda mazmuni asosida bloklash imkoniyati.

14. **WhatsApp** messenjerining veb va desktop versiyalarida yuborilgan ovozli xabarlar va fayllarni tutib olish imkoniyati.

2.6. Chop etishni nazorat qilish bo‘yicha talablar

Tizim tarmoq, lokal va virtual printerlarga yuborilayotgan hujjatlarni nazorat qilishi hamda quyidagi funksiyalarni ta’minlashi lozim:

1. Foydalanuvchilarning ishchi stansiyalariga o'rnatilgan agentlar orqali chop etishga yuborilgan hujjatlarni tutib olish.
2. Tarmoq, virtual va lokal printerlarga (jumladan **COM** va **LPT** portlari orqali ulangan printerlarga) yuborilgan hujjatlarni tutib olish imkoniyati.
3. **XPS** formatida chop etishni tutib olish imkoniyati.
4. Muayyan printerlar uchun tutib olishdan istisnolarni sozlash imkoniyati.
5. Chop etishni tutib olishni sahifalar soni va hujjat hajmi bo'yicha cheklash imkoniyati.
6. Printerlarda chop etishni tutib olish modulidan ayrim jarayonlarni (process) istisno qilish imkoniyati.
7. Chop etishga yuborilgan hujjatlardan matnni ajratib olish va tahlil qilish.
8. Belgilangan axborot xavfsizligi siyosatlariga muvofiq muayyan axborotni o'z ichiga olgan hujjatlarni avtomatik aniqlash hamda bunday holat aniqlanganda axborot xavfsizligi uchun mas'ul shaxsga avtomatik bildirishnoma yuborish.
9. Chop etishni hujjat nomi, hujjatning matnli mazmuni yoki printer nomi asosida bloklash imkoniyati.
10. Chop etishga yuborilgan fayllarni ularning matni va atributlari bo'yicha, jumladan shablonlardan foydalangan holda qidirish imkoniyati.
11. Hujjatlarni **PDF** va **XPS** formatlarida saqlash imkoniyati.
12. Chop etishga yuborilayotgan hujjatlarni ularning atributlari to'plami hamda mazmuni asosida bloklash imkoniyati.
13. Chop etishga yuborilayotgan hujjatlarni qidiruv lug'atlari va raqamli izlar (**digital fingerprints**) asosida bloklash imkoniyati.

2.7. Tashqi qurilmalar va ma'lumot saqlash qurilmalarini nazorat qilish bo'yicha talablar

Tizim foydalanuvchilar tomonidan tashqi qurilmalar va ma'lumot saqlash vositalaridan foydalanishni nazorat qilish imkoniyatiga ega bo'lishi hamda quyidagi funksiyalarni ta'minlashi lozim:

1. Tashqi qurilmalarning ulanishi bo'yicha auditni yuritish.
2. Tashqi ma'lumot saqlash qurilmalariga (olinadigan qattiq disklar, USB flesh-xotiralar, xotira kartalari, olinadigan saqlash qurilmalari, CD/DVD va floppy disklar va boshqalar) yozilayotgan fayllarning soya nusxalarini (shadow copy) yaratish.
3. Tashqi ma'lumot saqlash qurilmalariga fayllarni nusxalash hodisalari bo'yicha auditni yuritish. Auditda fayl nomi, foydalanuvchi, sana, vaqt va qurilma ma'lumotlari qayd etilishi lozim.

4. Fayl hajmi va kengaytmasi (extension) bo'yicha soya nusxalash va auditdan istisnolarni sozlash imkoniyati.

5. Katta hajmdagi fayllar uchun soya nusxaning qisman saqlanishini sozlash imkoniyati (masalan, faqat dastlabki **100 MB** qismini saqlash).

6. Tashqi ma'lumot saqlash qurilmalariga yozilayotgan fayllarning soya nusxalarini ma'lumotlar serverga yuborilishidan oldin nazorat qilinayotgan kompyuterlarning lokal xotirasida saqlash.

7. Nazorat qilinayotgan kompyuterlarda soya nusxalarni saqlash ombori hajmini sozlash imkoniyati.

8. Uzatilayotgan axborot mazmuni va boshqa atributlar asosida olinadigan ma'lumot tashuvchilarga fayllarni yozishni bloklash imkoniyati.

9. Muayyan tashqi ma'lumot saqlash qurilmalari uchun (qurilma turi, identifikatori, ishlab chiqaruvchisi, nomi, seriya raqami va boshqalar bo'yicha) soya nusxalash va auditdan istisnolarni sozlash, shuningdek parametr qiymatlari niqoblarini kiritishda "*" va "?" almashtirish belgilaridan foydalanish imkoniyati.

10. Tashqi ma'lumot saqlash qurilmalariga kirishni nazorat qilish hamda belgilangan parametrlarga (ishlab chiqaruvchi identifikatori va nomi, mahsulot identifikatori va nomi, seriya raqami, qurilma turi va boshqalar) ega qurilmalardan foydalanishni taqiqlash imkoniyati. Parametr niqoblarini kiritishda "*" va "?" belgilaridan foydalanish imkoniyati ta'minlanishi lozim.

11. Tashqi ma'lumot saqlash qurilmalariga yozish huquqlarini boshqarish, jumladan:

- muayyan qurilmalarga (ishlab chiqaruvchi identifikatori va nomi, mahsulot identifikatori va nomi, seriya raqami, qurilma turi bo'yicha) yozishni taqiqlash;
- parametr niqoblari uchun "*" va "?" belgilaridan foydalanish;
- ma'lum kengaytmaga ega fayllarni yozishni taqiqlash.

12. Axborotni tashqi ma'lumot saqlash qurilmalariga nusxalashni ham lokal, ham terminal foydalanuvchi sessiyalarida nazorat qilish imkoniyati.

13. Ayrim jarayonlarni nazorat, audit va soya nusxalash protseduralaridan istisno qilish imkoniyati.

14. Qo'llab-quvvatlanadigan quyidagi turdagi tashqi qurilmalardan foydalanishni nazorat qilish va auditini yuritish:

- USB Bus Devices (hub va host controllerlar);
- CD/DVD qurilmalari;
- audio qurilmalar;
- tarmoq adapterlari;

- ketma-ket va parallel portlar;
- SCSI va RAID kontrollerlari;
- floppy disk yuritmalari;
- kameralar va skanerlar;
- Windows Portable Devices (WPD);
- Universal Cameras.

Nazorat ishchi stansiyaga ulangan qurilmalar bo'yicha amalga oshirilishi hamda quyidagi parametrlar asosida filtrlash imkoniyatini ta'minlashi lozim:

- qurilma nomi;
- qurilma identifikatori;
- ishlab chiqaruvchi identifikatori;
- mahsulot identifikatori;
- ishlab chiqaruvchi nomi;
- seriya raqami;
- qurilma turi.

15. Nazorat qilinayotgan ishchi stansiyalarga ulangan qurilmalarni istisnolar filtri ro'yxatiga qo'shish imkoniyati.

16. Belgilangan axborot xavfsizligi siyosatlariga muvofiq ko'rsatilgan parametrlarga ega tashqi qurilmalardan foydalanish holatlarini avtomatik aniqlash hamda bunday holat aniqlanganda axborot xavfsizligi uchun mas'ul shaxsga avtomatik bildirishnoma yuborish.

17. Tashqi ma'lumot saqlash qurilmalariga fayllar uzatilishini, jumladan belgilangan axborotni o'z ichiga olgan fayllar uzatilishini avtomatik aniqlash va bunday holat aniqlanganda axborot xavfsizligi uchun mas'ul shaxsga avtomatik bildirishnoma yuborish.

18. Tashqi ma'lumot saqlash qurilmalariga yozilgan fayllarni ularning matni va atributlari bo'yicha, jumladan shablonlardan foydalangan holda qidirish imkoniyati.

19. Ma'lumot saqlash qurilmasiga yozilayotgan fayllarni atributlari to'plami hamda mazmuni asosida bloklash imkoniyati.

20. Ma'lumot saqlash qurilmasiga yozilayotgan fayllarni ularning xesh-summasi (hash) asosida bloklash imkoniyati.

21. Ma'lumot saqlash qurilmasiga yozilayotgan fayllarni qidiruv lug'atlari va raqamli izlar (**digital fingerprints**) asosida bloklash imkoniyati.

2.8. Bulutli ma'lumot saqlash xizmatlarini nazorat qilish bo'yicha talablar

Tizim bulutli ma'lumot saqlash xizmatlarining **desktop ilovalari (iCloud, Dropbox, Google Drive, OneDrive, Mail.ru Cloud, Yandex Disk)** ustidan quyidagi nazorat imkoniyatlarini ta'minlashi lozim:

1. Bulutli ma'lumot saqlash xizmatlariga fayllar yuborilishi hodisalari bo'yicha auditni yuritish. Auditda fayl nomi, foydalanuvchi nomi, sana, vaqt va bulutli saqlash xizmati nomi qayd etilishi lozim.

2. Foydalanuvchi yoki jarayon (process) tomonidan bulutli ma'lumot saqlash xizmatlariga yuborilayotgan fayllarning soya nusxalarini (shadow copy) yaratish.

3. Audit va soya nusxalashni faqat chiquvchi, faqat kiruvchi yoki barcha fayllar uchun alohida sozlash imkoniyati.

4. Katta hajmdagi fayllar uchun soya nusxaning qisman saqlanishini sozlash imkoniyati (masalan, faqat dastlabki **100 MB** qismini saqlash).

5. Bulutli ma'lumot saqlash xizmatiga yozilgan fayllarning soya nusxalarini serverga yuborilishidan oldin nazorat qilinayotgan kompyuterlarning lokal xotirasida saqlash.

6. Foydalanuvchilarning lokal kompyuterlarida soya nusxalarni saqlash ombori hajmini sozlash imkoniyati.

7. Alohida bulutli ma'lumot saqlash xizmatlariga kirishni nazorat qilish va muayyan foydalanuvchilar uchun ulardan foydalanishni taqiqlash imkoniyati.

8. Alohida bulutli ma'lumot saqlash xizmatlariga kirishni nazorat qilish hamda muayyan foydalanuvchilar uchun **"faqat o'qish" (Read Only)** rejimini sozlash imkoniyati.

9. Bulutli ma'lumot saqlash xizmatlariga ma'lumot uzatish huquqlarini boshqarish, jumladan muayyan formatdagi fayllarni yuborishni taqiqlash imkoniyati.

10. Fayl kengaytmalari bo'yicha audit, soya nusxalash va kirishni nazorat qilishdan istisnolarni sozlash imkoniyati.

11. Belgilangan axborot xavfsizligi siyosatlariga muvofiq bulutli ma'lumot saqlash xizmatlariga yuborilgan va muayyan axborotni o'z ichiga olgan fayllarni avtomatik aniqlash hamda bunday holat aniqlanganda axborot xavfsizligi uchun mas'ul shaxsga avtomatik bildirishnoma yuborish.

12. Bulutli ma'lumot saqlash xizmatlariga yuborilgan fayllarni ularning matni va atributlari bo'yicha, jumladan shablonlardan foydalangan holda qidirish imkoniyati.

Bulutli ma'lumot saqlash xizmatlarining veb-versiyalarini nazorat qilish bo'yicha talablar

Tizim bulutli ma'lumot saqlash xizmatlarining **veb-versiyalari (iCloud, Dropbox, Google Drive, OneDrive, Mail.ru Cloud, Yandex Disk, ownCloud)** ustidan quyidagi nazorat imkoniyatlarini ta'minlashi lozim:

1. Bulutli ma'lumot saqlash xizmatlariga fayllar yuborilishi hodisalari bo'yicha auditni yuritish. Auditda fayl nomi, foydalanuvchi nomi, sana, vaqt va bulutli saqlash xizmati nomi qayd etilishi lozim.

2. Foydalanuvchi yoki jarayon (process) tomonidan bulutli ma'lumot saqlash xizmatlariga yuborilayotgan fayllarning soya nusxalarini (shadow copy) yaratish.

3. Bulutli ma'lumot saqlash xizmatiga yozilgan fayllarning soya nusxalarini serverga yuborilishidan oldin nazorat qilinayotgan kompyuterlarning lokal xotirasida saqlash.

4. Belgilangan axborot xavfsizligi siyosatlariga muvofiq bulutli ma'lumot saqlash xizmatlariga yuborilgan va muayyan axborotni o'z ichiga olgan fayllarni avtomatik aniqlash hamda bunday holat aniqlanganda axborot xavfsizligi uchun mas'ul shaxsga avtomatik bildirishnoma yuborish.

5. Bulutli ma'lumot saqlash xizmatlariga yuborilgan fayllarni ularning matni va atributlari bo'yicha, jumladan shablonlardan foydalangan holda qidirish imkoniyati.

2.9. Tarmoq resurslarini nazorat qilish bo'yicha talablar

Tizim foydalanuvchilar tomonidan tarmoq resurslaridan foydalanishni nazorat qilish imkoniyatiga ega bo'lishi hamda quyidagi funksiyalarni ta'minlashi lozim:

1. Lokal tarmoq resurslariga fayllarni nusxalash hodisalari bo'yicha auditni yuritish. Auditda fayl nomi, foydalanuvchi, sana, vaqt hamda tarmoq resursining tarmoq yo'li (network path) qayd etilishi lozim.

2. Tarmoq resurslariga yuborilayotgan fayllarning soya nusxalarini (shadow copy) yaratish.

3. Fayl kengaytmalari bo'yicha audit va soya nusxalashdan istisnolarni sozlash imkoniyati.

4. Muayyan tarmoq resurslarini audit va soya nusxalashdan istisno qilish imkoniyati.

5. Katta hajmdagi fayllar uchun soya nusxaning qisman saqlanishini sozlash imkoniyati (masalan, faqat dastlabki 100 MB qismini saqlash).

6. Tarmoq resurslariga yozilgan fayllarning soya nusxalarini serverga yuborilishidan oldin nazorat qilinayotgan kompyuterlarning lokal xotirasida saqlash.

7. Foydalanuvchilarning lokal kompyuterlarida soya nusxalarni saqlash ombori hajmini sozlash imkoniyati.
8. Terminal serverlarining tarmoq resurslariga uzatilayotgan fayllarning soya nusxalarini yaratish imkoniyati.
9. Tarmoq resurslariga kirishni nazorat qilish hamda muayyan tarmoq resurslariga kirishni taqiqlash imkoniyati.
10. Tarmoq resurslariga yozish huquqlarini boshqarish, jumladan muayyan formatdagi fayllarni yozishni taqiqlash imkoniyati.
11. Ayrim jarayonlarni (process) nazorat, audit va soya nusxalash protseduralaridan istisno qilish imkoniyati.
12. Belgilangan axborot xavfsizligi siyosatlariga muvofiq tarmoq resurslariga uzatilgan hamda muayyan axborotni o'z ichiga olgan fayllarni avtomatik aniqlash va bunday holat aniqlanganda axborot xavfsizligi uchun mas'ul shaxsga avtomatik bildirishnoma yuborish.
13. Tarmoq resurslariga yuborilgan fayllarni ularning matni va atributlari bo'yicha, jumladan shablonlardan foydalangan holda qidirish imkoniyati.

2.10. Ekran suratlari (skrinshot) funksiyasiga qo'yiladigan talablar

Tizim foydalanuvchining ish stoli faolligini ekran suratlarini olish orqali nazorat qilish imkonini berishi hamda quyidagi funksional imkoniyatlarga ega bo'lishi lozim:

1. belgilangan vaqt oralig'ida, soniya aniqligigacha sozlanadigan interval bilan skrinshotlarni olish imkoniyati;
2. faol oyna almashganda skrinshot olish imkoniyati;
3. brauzer yorlig'i (tab) almashganda skrinshot olish imkoniyati;
4. jarayon (protsess) ishga tushirilganda skrinshot olish imkoniyati;
5. bloklash qoidasi ishga tushganda skrinshot olish imkoniyati;
6. **Print Screen** tugmasi bosilganda skrinshot olish imkoniyati;
7. ishchi stansiya bo'sh turgan vaqtda skrinshot olishni o'chirib qo'yish imkoniyati;
8. skrinshot sifatini, jumladan, ularni oq-qora formatda saqlashni sozlash imkoniyati;
9. skrinshot o'lchamini (asl nusxaga nisbatan foiz hisobida) sozlash imkoniyati;
10. skrinshot formatini (JPEG, PNG) tanlash imkoniyati;
11. skrinshotni olishning imkoni bo'lmagan hollarda (foydalanuvchi seansi uzilgan, bloklangan va hokazo) maxsus belgi saqlanishi;

12. skrinshot olingan paytdagi faol jarayon (protsess) to'g'risidagi ma'lumotni saqlash;

13. skrinshot olingan paytdagi brauzerning faol yorlig'i (tabi) to'g'risidagi ma'lumotni saqlash;

14. brauzerda belgilangan veb-saytlarga tashrif buyurilganda skrinshot olishni o'chirib qo'yish imkoniyati;

15. faqat belgilangan faol jarayonlar (protsesslar) uchun skrinshot olish imkoniyati;

16. skrinshotlarni interaktiv tuzilma elementlari qo'llab-quvvatlanadigan va ushlangan ma'lumotlarni veb-brauzer orqali ko'rish imkonini beruvchi tashqi HTML faylga eksport qilish imkoniyati;

17. alohida foydalanuvchining bir kunlik (yoki tanlangan vaqt oralig'idagi) skrinshotlarini grafik fayllar to'plami yoki bitta PDF yoki videofayl ko'rinishida saqlash imkoniyati;

18. PK foydalanuvchisi tomonidan skrinshot olishni (Print Screen tugmasi orqali ham, uchinchi tomon vositalari yordamida ham) bloklash imkoniyati.

2.11. Veb-kamera suratlari funksiyasiga qo'yiladigan talablar

Tizim veb-kamera suratlarni olish orqali kompyuter oldida ishlayotgan xodimni identifikatsiya qilish imkonini berishi hamda quyidagi funksional imkoniyatlarga ega bo'lishi lozim:

1. lokal seans boshlanganda veb-kamera suratini olish imkoniyati;

2. masofaviy seans boshlanganda veb-kamera suratini olish imkoniyati;

3. seans qayta tiklanganda veb-kamera suratini olish imkoniyati;

4. bo'sh turish (idle) davri boshlanganda veb-kamera suratini olish imkoniyati;

5. bo'sh turish (idle) davri yakunlanganda veb-kamera suratini olish imkoniyati;

6. alohida foydalanuvchining bir kunlik (yoki tanlangan vaqt oralig'idagi) veb-kamera suratlarni grafik fayllar to'plami yoki bitta PDF yoki videofayl ko'rinishida saqlash imkoniyati;

7. kompyuter oldida ishlayotgan foydalanuvchini avtomatik identifikatsiya qilish (yuzni tanib olish) hamda begona shaxs aniqlanganda xavfsizlik qoidalarini qo'llash va seansni bloklashni sozlash imkoniyati.

2.12. Videomonitoring funksiyasiga qo'yiladigan talablar

Tizim foydalanuvchi faolligini ish stoli videosi hamda veb-kamera videosini yozib olish orqali nazorat qilish imkonini berishi hamda quyidagi funksional imkoniyatlarga ega bo'lishi lozim:

1. foydalanuvchi kompyuteri monitoriga ulanib, ish stoli videosini real vaqt rejimida ko'rish imkoniyati;
2. bir vaqtning o'zida bir nechta foydalanuvchilarning ish stollarini monitoring qilish imkoniyati;
3. ko'rish oynasini alohida ekranga chiqarish imkoniyati;
4. jadval (reja) asosida ish stoli videosi va ulangan veb-kameradan olingan videoni avtomatik yozib olish imkoniyati;
5. ish stoli videosini qo'lda yozib olish imkoniyati;
6. video yozuv sifatini sozlash imkoniyati;
7. videoni rangli yoki oq-qora formatda yozib olish imkoniyati;
8. bir vaqtning o'zida bir nechta foydalanuvchining video yozuvlarini saqlash imkoniyati;
9. yozuv fayllarini tizim vositalari hamda istalgan media pleyer orqali ijro etish imkoniyati.

2.13. Audiomonitoring funksiyasiga qo'yiladigan talablar

Tizim foydalanuvchi faolligini mikrofondan yozib olinadigan audio hamda ishchi stansiya karnaylariga uzatilayotgan audio orqali nazorat qilish imkonini berishi hamda quyidagi funksional imkoniyatlarga ega bo'lishi lozim:

1. nazorat qilinayotgan ishchi stansiyalar mikrofonlariga ulanib, audio oqimini real vaqt rejimida tinglash imkoniyati;
2. bir vaqtning o'zida bir nechta foydalanuvchining mikrofonlarini tinglash imkoniyati;
3. jadval (reja) asosida mikrofondan kelayotgan audio oqimi va kompyuterning tizim tovushlarini avtomatik yozib olish imkoniyati;
4. audioni qo'lda yozib olish imkoniyati;
5. bir vaqtning o'zida bir nechta foydalanuvchining audio yozuvlarini saqlash imkoniyati;
6. yozuv fayllarini tizim vositalari hamda istalgan media pleyer orqali ijro etish imkoniyati;
7. yozib olingan video va audio fayllarda ovoz yo'lagini (audio trekni) aks ettirish imkoniyati.

2.14. Foydalanuvchi faolligini monitoring qilish funksiyasiga qo'yiladigan talablar

Tizim foydalanuvchining ish joyidagi faolligini nazorat qilish imkonini berishi hamda quyidagi funksional imkoniyatlarga ega bo'lishi lozim:

1. faol ish vaqti hamda bo'sh turish (foydalanuvchi tomonidan hech qanday harakat bajarilmagan vaqt) bo'yicha statistikani yuritish, shuningdek bo'sh turish boshlanishidan oldingi faollik bo'lmagan davrni sozlash imkoniyati;

2. foydalanuvchining ilovalarda ishlash vaqti bo'yicha statistikani yuritish va to'plangan ma'lumotlarni taqdim etish, bunda ilovaning umumiy ishlash vaqti emas, balki foydalanuvchi faol oynada ishlagan vaqt hisobga olinishi;

3. alohida jarayonlarni (protsesslarni) monitoringdan chiqarib tashlash imkoniyati;

4. to'plangan statistikani avtomatik tahlil qilish orqali muayyan hodisalarni (masalan, ruxsat etilmagan ilovalarning ishga tushirilishi), foydalanuvchilarning muayyan ilovalarda ishlash davomiyligini hamda kompyuterning ish va bo'sh turish davrlarini nazorat qilish va bu haqda mas'ul shaxsga tegishli bildirishnoma yuborish imkoniyati;

5. alohida ilovalarning ishga tushirilishini bloklash imkoniyati;

6. tanlangan vaqt oralig'i uchun alohida foydalanuvchi yoki bir nechta foydalanuvchilar bo'yicha faollik hisobotlarini (PKdagi foydalanuvchi faolligi, ilovalar faolligi, hodisalar xronologiyasi) saqlash imkoniyati;

7. turli ilovalarda sarflangan vaqtni avtomatik ravishda **samarali**, **samarasiz** va **neytral** toifalarga ajratish imkoniyati.

2.15. Brauzer faolligini monitoring qilish funksiyasiga qo'yiladigan talablar

Brauzer faolligini monitoring qilish funksiyasi nazorat qilinayotgan foydalanuvchilarning **Internet Explorer, Google Chrome, Mozilla Firefox, Opera, Tor, Yandex Browser, Rambler, Amigo, Chromium** va **Microsoft Edge** brauzerlaridagi faolligi bo'yicha kompleks statistikani yuritish imkonini berishi hamda quyidagi funksional imkoniyatlarga ega bo'lishi lozim:

1. brauzer orqali veb-saytlarga tashrif buyurish vaqtini nazorat qilish, bunda faqat faol brauzer yorlig'idagi (tabdagi) ishlash vaqti hisobga olinishi, veb-sayt sahifalari o'rtasidagi o'tishlar qayd etilishi hamda turli veb-resurslarda o'tkazilgan vaqt bo'yicha kompleks statistika yuritilishi;

2. brauzer faolligini monitoring qilish jarayonidan alohida veb-saytlarni chiqarib tashlash (istisno qilish) imkoniyati;

3. tanlangan vaqt oralig'i uchun alohida foydalanuvchi yoki bir nechta foydalanuvchilar bo'yicha brauzer faolligi haqidagi turli hisobotlarni (kun davomida

tashrif buyirilgan saytlar reytingi, hodisalar xronologiyasi) **PDF** fayl ko‘rinishida saqlash imkoniyati;

4. foydalanuvchining brauzerdagi faollik vaqti bo‘yicha belgilangan miqdoriy ko‘rsatkichlarga erishilganda avtomatik bildirishnomalarni sozlash imkoniyati (masalan: **"Foydalanuvchining muayyan veb-saytda brauzer orqali bo‘lish vaqti bir kun davomida 1 soatdan oshdi"** va hokazo);

5. turli veb-saytlarda o‘tkazilgan vaqtni avtomatik ravishda **samarali, samarasiz** va **neytral** toifalarga ajratish imkoniyati.

2.16. Almashish buferini nazorat qilish funksiyasiga qo‘yiladigan talablar

Tizim foydalanuvchilar tomonidan almashish buferidan (Clipboard) foydalanishni nazorat qilish imkonini berishi hamda quyidagi funksional imkoniyatlarga ega bo‘lishi lozim:

1. almashish buferiga joylashtirilgan matnli ma’lumotlarning soyali nusxasini (shadow copy) yaratish, bunda ushbu ma’lumot qaysi ilovadan almashish buferiga joylashtirilgani va hodisa vaqti qayd etilishi;

2. almashish buferiga joylashtirilgan fayllar auditini yuritish;

3. almashish buferiga joylashtirilgan grafik ma’lumotlarning soyali nusxasini yaratish;

4. almashish buferiga joylashtirilgan fayllarning soyali nusxasini yaratish;

5. almashish buferidan ushlab olinadigan ma’lumotlarning maksimal hajmini cheklash imkoniyati;

6. almashish buferi monitoringidan alohida jarayonlarni (protsesslarni) chiqarib tashlash yoki faqat belgilangan jarayonlarni monitoring qilish imkoniyati;

7. almashish buferi monitoringidan alohida fayllarni chiqarib tashlash yoki faqat belgilangan fayllarni monitoring qilish imkoniyati;

8. almashish buferiga joylashtirilgan ma’lum turdagi axborotni (belgilangan axborot xavfsizligi siyosatlari asosida) avtomatik aniqlash hamda bunday axborot aniqlanganda axborot xavfsizligi uchun mas’ul shaxsga bildirishnoma yuborish imkoniyati;

9. sozlangan xavfsizlik qoidalariga muvofiq fayllarni nusxalashni ham, joylashtirishni (Paste) ham mazmuniga qarab bloklash imkoniyati;

10. foydalanuvchilar tomonidan almashish buferiga joylashtirilgan matn bo‘yicha, jumladan shablonlardan foydalangan holda qidiruvni amalga oshirish imkoniyati;

11. almashish buferiga nusxalangan axborotni va almashish buferidan joylashtirilayotgan axborotni alohida aniqlashni sozlash imkoniyati;

12. almashish buferida faqat fayllarni, faqat matnni yoki faqat tasvirlarni aniqlashni sozlash imkoniyati.

2.17. Klaviaturadan kiritishni nazorat qilish funksiyasiga qo'yiladigan talablar

Tizim foydalanuvchi tomonidan klaviaturadan kiritilayotgan ma'lumotlarni nazorat qilish imkonini berishi hamda quyidagi funksional imkoniyatlarga ega bo'lishi lozim:

1. foydalanuvchi tomonidan klaviaturada bosilgan tugmalarni qayd etish, bunda ma'lumot qaysi ilovada kiritilgani va hodisa vaqti qayd etilishi, shuningdek xizmat tugmalari (**Shift**, **Enter**, **Backspace** va boshqalar) bosilishini ko'rsatish yoki yashirish imkoniyati;

2. belgilangan ilovalarda klaviatura kirituvlarini ushlab qolishni istisno qilish yoki faqat muayyan ilovalarda ushlab qolishni amalga oshirish imkoniyati;

3. brauzerdagi faol sahifa manzili bo'yicha klaviatura kirituvlarini ushlab qolishni istisno qilish yoki faqat muayyan faol sahifalarda ushlab qolishni amalga oshirish imkoniyati;

4. foydalanuvchi tomonidan klaviatura orqali kiritilayotgan ma'lum turdagi axborotni (belgilangan axborot xavfsizligi siyosatlari asosida) avtomatik aniqlash hamda bunday axborot aniqlanganda axborot xavfsizligi uchun mas'ul shaxsga bildirishnoma yuborish imkoniyati;

5. foydalanuvchilar tomonidan klaviatura orqali kiritilgan matn bo'yicha, jumladan shablonlardan foydalangan holda qidiruvni amalga oshirish imkoniyati.

2.18. Fayl tizimini nazorat qilish funksiyasiga qo'yiladigan talablar

Tizim ishchi stansiya fayl tizimida saqlanayotgan fayllarni nazorat qilish imkonini berishi hamda quyidagi funksional imkoniyatlarga ega bo'lishi lozim:

1. nazorat qilinayotgan ishchi stansiyalar fayl tizimlarini maxfiy maqomga ega bo'lgan yoki axborot xavfsizligini ta'minlash nuqtai nazaridan ahamiyatga ega hujjatlar mavjudligini aniqlash maqsadida avtomatik skanerlash;

2. skanerlash jarayonida qidirilishi lozim bo'lgan maxfiy hujjatlar bazasini shakllantirish;

3. **TXT** va **CSV** formatidagi fayllardan oldindan tayyorlangan xesh-funksiyalarni maxfiy hujjatlar bazasiga avtomatik import qilish imkoniyati;

4. fayl tizimlari nazorat qilinadigan ishchi stansiyalar va foydalanuvchilarni tanlash imkoniyati;

5. avtomatik tekshiruvdan o'tkaziladigan fayllar va papkalarni tanlash qoidalarini moslashuvchan sozlash imkoniyati;

6. sozlanadigan hajmdagi fayllarni skanerlashdan chiqarib tashlash imkoniyati;

7. fayl tizimini jadval (reja) asosida tekshirish imkoniyati;

8. alohida foydalanuvchilar va ishchi stansiyalar uchun, jumladan shablonlardan foydalangan holda, fayl tizimi tarkibini nazorat qilishning individual siyosatlarini yaratish imkoniyati;

9. nazorat qilinayotgan ishchi stansiyalar fayl tizimlarida hujjatlarni fayl atributlari va ularning xesh-funksiyalari qiymatlari bo'yicha qidirish imkoniyati.

2.19. Fayl operatsiyalari auditiga qo'yiladigan talablar

Tizim ishchi stansiyadagi, shuningdek tarmoq papkalaridagi fayllar va papkalar bilan bajariladigan operatsiyalar auditini yuritish imkonini berishi lozim.

Fayllar bilan quyidagi operatsiyalar nazorat qilinishi kerak:

1. yaratish;
2. o'qish;
3. yozish;
4. o'chirish;
5. nomini o'zgartirish;
6. ochish;
7. kirish huquqlarini o'zgartirish.

Papkalar bilan quyidagi operatsiyalar nazorat qilinishi kerak:

1. yaratish;
2. o'chirish;
3. nomini o'zgartirish;
4. ochish;
5. kirish huquqlarini o'zgartirish.

Shuningdek, quyidagi qo'shimcha imkoniyatlar nazarda tutilishi lozim:

1. auditdan muayyan fayllar, papkalar va jarayonlarni (protsesslarni) chiqarib tashlash yoki faqat belgilangan fayllar, papkalar va jarayonlar bo'yicha audit yuritish imkoniyati;

2. audit uchun istisnolar ro'yxatini XML formatiga eksport qilish hamda ushbu ro'yxatni import qilish imkoniyati.

2.20. Uskunalarini nazorat qilish moduliga qo'yiladigan talablar

Tizim kompyuterlar va ularga ulangan uskunalarini nazorat qilish imkonini berishi hamda quyidagi funksional imkoniyatlarga ega bo'lishi lozim:

1. kompyuter uskunalarini konfiguratsiyasini belgilash imkoniyatini taqdim etish;
2. aniqlangan ulangan qurilmalar tarkibining belgilangan kompyuter konfiguratsiyasiga muvofiqligini kuzatish;
3. konfiguratsiyaga kirmaydigan qurilmalar aniqlanganda, kompyuter konfiguratsiyasidan chetlanishlarni avtomatik ravishda aniqlash va aks ettirish;
4. konfiguratsiyada mavjud bo'lgan biror qurilma ishga tushmaganligi aniqlanganda, kompyuter konfiguratsiyasidan chetlanishlarni avtomatik ravishda aniqlash va aks ettirish;
5. muayyan uskuna uchun mas'ul xodimni biriktirish;
6. ofis xonalari xaritasida uskunalarini (kompyuterlar va boshqa qurilmalarni) joylashtirish, bunda o'z xonalar sxemasini yuklash imkoniyati;
7. har biri o'z xonalar sxemasi va unda joylashtirilgan kompyuterlar hamda boshqa uskunalar to'plamiga ega bo'lgan bir nechta ofis xaritalarini yaratish imkoniyati, ular ofisning haqiqiy joylashuviga mos bo'lishi kerak;
8. tanlangan kompyuterda ayni paytda faol ishlayotgan foydalanuvchilarni aks ettirish;
9. oxirgi seans davomida tanlangan kompyuterda aniqlangan foydalanuvchilarni aks ettirish;
10. ofis xaritasini **.xlsx** va **.pdf** formatlarida saqlash imkoniyati.

Shuningdek, tizim ishchi stansiyalardagi agentlardan olingan kompyuterlarga ulangan qurilmalar haqidagi ma'lumotlar asosida tashkilotning aniqlangan kompyuterlari va qurilmalari uchun hisob kartochkalarini avtomatik ravishda shakllantirish imkoniyatiga ega bo'lishi lozim.

2.21. Ma'lumotlarni saqlash va qayta ishlashga qo'yiladigan talablar

Sozlamalar turli **MBBT (Ma'lumotlar bazasini boshqarish tizimlari)** boshqaruvidagi ma'lumotlar omborlarini ulash, ma'lumotlarni replikasiya qilish orqali hududiy taqsimlangan tashkilotlarda boshqarish, ma'lum turdagi ma'lumotlarni belgilangan omborlarda saqlash qoidalarini yaratish hamda ma'lumotlar bazalarining rotatsiya guruhlarini shakllantirish imkonini berishi lozim.

Ma'lumotlarni saqlash va qayta ishlash quyidagi funksional imkoniyatlarga ega bo'lishi kerak:

1. tizim tomonidan yig'iladigan barcha ma'lumotlarni **Microsoft SQL Server, Oracle, PostgreSQL 9.3** va undan yuqori, **MySQL 5.7.09** va undan yuqori yoki **SQLite** MBBTlarida (tanlov asosida) saqlash imkoniyati;
2. yetkazib berish to'plamida o'rnatilgan **SQLite** MBBT mavjud bo'lishi;
3. xavfsizlik siyosatlari ishga tushgan yoki tushmaganidan qat'i nazar, ushlab olingan barcha ma'lumotlarni saqlash;
4. turli serverlarda joylashgan ma'lumotlar bazalari bilan ishlashni qo'llab-quvvatlash;
5. fayllarni ma'lumotlar bazasida emas, balki server diskida saqlash imkoniyati, bunda kichik hajmdagi fayllarni diskka saqlamaslikni sozlash hamda ma'lumotlar bazasida faqat fayllarning nisbiy yo'llarini saqlash;
6. alohida ma'lumotlar bazalari uchun tasvirlarni, muhrlarni va nutqni tanib olish funksiyalarini yoqish yoki o'chirish imkoniyati;
7. rotatsiya guruhidagi ma'lumotlar bazalarida ma'lumotlarni saqlash muddatini sozlash imkoniyati;
8. ma'lumotlar bazasini Administrator konsoli orqali qo'lda o'chirib qo'yish imkoniyati, bunda bazadagi ma'lumotlar saqlanib qolishi;
9. Administrator konsoli orqali ma'lumotlar bazasi tarkibini qo'lda tozalash imkoniyati;
10. ma'lumotlar bazalarini arxivlash hamda keyinchalik ulash orqali ularda saqlangan muhim ma'lumotlar bo'yicha retrospektiv qidiruvni amalga oshirish imkoniyati;
11. foydalanuvchi tomonidan ushlab olingan ma'lumotlarni tanlab o'chirish imkoniyati;
12. alohida ma'lumotlar bazalarini bazalarning halqasimon (ring) rotatsiyasini qo'llab-quvvatlovchi guruhlariga birlashtirish imkoniyati, bunda qidiruv barcha bazalar bo'yicha amalga oshiriladi, yozish esa faqat faol bazaga bajariladi;
13. ma'lumotlar bazalari rotatsiyasi uchun bir nechta shartlarni sozlash imkoniyati: ma'lumotlarning umumiy hajmi, ma'lumotlar bazasi hajmi, qidiruv indeksleri hajmi, diskdagi fayllar hajmi, vaqt oralig'i va yozuvlar soni, shuningdek rotatsiya jarayonini ma'lum vaqt oralig'ida ishga tushirishni sozlash;
14. rotatsiya jarayoni boshlanishidan oldin, yakunlangandan keyin va rotatsiya xatosi yuz berganda skriptlarni bajarishni sozlash imkoniyati, bunda **CMD, PowerShell, Script Host** va **Python** skriptlarini bajarish qo'llab-quvvatlanishi;
15. **Round Robin** algoritmi asosida ikki yoki undan ortiq ma'lumotlar bazasi guruhlari yoki ma'lumotlar bazalari o'rtasida yuklamani muvozanatlash

imkoniyati, bunda tizimga kelayotgan barcha ma'lumotlar ma'lumotlar bazalariga navbatma-navbat yozib boriladi.

2.22. Ma'lumotlarni tahlil qilishga qo'yiladigan talablar

Tizim ushlab olingan ma'lumotlarni tahlil qilishning keng funksional imkoniyatlariga ega bo'lishi lozim, jumladan:

1. kontent tahlili;
2. atributiv tahlil;
3. tasvirlarni tanib olish;
4. muhrlarni tanib olish;
5. nutqni tanib olish;
6. statistik tahlil;
7. hodisalar tahlili;
8. xulq-atvor (behavioural) tahlili;
9. ilovalarni toifalash;
10. veb-saytlarni toifalash;
11. veb-saytlar va ilovalarning samaradorligini hisobga olish.

2.23. Tizimning ishga layoqatliligini monitoring qilishga qo'yiladigan talablar

Ishga layoqatlilik monitoringi tizim holatini real vaqt rejimida nazorat qilish imkonini berishi hamda quyidagi funksional imkoniyatlarni ta'minlashi lozim:

1. tizim ishga layoqatliligi monitoringi paneli mavjud bo'lishi, unda tizimning barcha asosiy komponentlari faoliyati hamda uskuna resurslaridan foydalanish to'g'risidagi asosiy ma'lumotlar aks ettirilishi;
2. tizimning server komponentlari hodisalari jurnalini yuritish;
3. Administrator konsolida hodisalar jurnalini, shuningdek har bir hodisa bo'yicha batafsil ma'lumot va tavsiyalarni ko'rish imkoniyati;
4. hodisalar jurnalini sana, hodisa darajasi (axborot, ogohlantirish, xato), server komponenti va hodisa manbasi bo'yicha filtrlash imkoniyati;
5. monitoring uchun hodisalar manbai sifatida muayyan serverlarni tanlash imkoniyati;
6. hodisalar jurnalini hodisalarni saqlash muddati va ularning darajasiga qarab avtomatik tozalash imkoniyati;
7. hodisalar jurnalini **PDF, XPS, CSV, XLS, XLSX, HTML, RTF va TXT** formatlariga eksport qilish imkoniyati;
8. hodisalar jurnalini chop etish imkoniyati;

9. tizim administratorini server komponentlarida yuzaga kelgan yangi hodisalar haqida elektron pochta orqali avtomatik xabardor qilish imkoniyati;

10. elektron pochta orqali bildirishnomalarni yuborish qoidalarini sozlash imkoniyati (qabul qiluvchini, server komponentini, hodisa darajasini yoki muayyan hodisalarni tanlash).

2.24. Axborotni qidirish funksiyasiga qo'yiladigan talablar

Axborotni qidirish vositalari yuqori darajada batafsil qidiruv so'rovlarini yaratish imkonini berishi lozim. Tizim quyidagi funksional imkoniyatlarni taqdim etishi kerak:

1. ushlab olingan ma'lumotlar bo'yicha barcha mavjud tahlil vositalaridan foydalangan holda qidiruvni amalga oshirish: kontent tahlili, atributiv tahlil, tanib olingan tasvirlar, muhrlar va nutq bo'yicha qidiruv, shuningdek hodisalar tahlili;

2. **Active Directory** guruhlarini bo'yicha axborotni qidirish;

3. veb-saytlar va ilovalar toifalari bo'yicha qidiruv;

4. raqamli izlar (digital fingerprint) bo'yicha qidiruv, ishga tushish chegarasini (threshold) sozlash imkoniyati bilan;

5. lug'atlar bo'yicha qidiruv, bunda ishga tushish chegarasi va morfologiyani hisobga olish imkoniyati;

6. xesh-summalar bo'yicha qidiruv, oldindan sozlangan xesh-summalar bazalari bo'yicha qidiruvni qo'llab-quvvatlash bilan;

7. muayyan maxfiylik belgilari (yorliqlari) mavjud bo'lgan axborotni qidirish;

8. bir nechta oddiy qidiruv shartlarini **"VA"**, **"YOKI"**, **"EMAS"** mantiqiy operatorlari yordamida birlashtirish, shuningdek qidiruv shartlarini guruhlariga birlashtirish imkoniyati;

9. qidiruv shablonlarini yaratish va ulardan foydalanish imkoniyati, ya'ni boshqa murakkab qidiruv so'rovlarida foydalanish mumkin bo'lgan qidiruv shartlari to'plamini yaratish;

10. keyinchalik foydalanish uchun qidiruv shartlarini **Tanlanganlar (Favorites)** bo'limiga qo'shish imkoniyati;

11. qidiruv shartlarini import va eksport qilish imkoniyati;

12. qidiruv natijalari sonini cheklash imkoniyati;

13. qidiruv natijalarini turli parametrlar (kolleksiya, foydalanuvchi va boshqalar) bo'yicha guruhlash imkoniyati;

14. qidiruv natijalarini bir vaqtning o'zida turli yorliqlarda (tablarda) ochish hamda zarurat tug'ilganda avval tanlangan qidiruv shartlarini o'zgartirish imkoniyati.

2.25. Hisobotlar moduliga qo'yiladigan talablar

Tizimning hisobotlar moduli quyidagi funksional imkoniyatlarga ega bo'lishi lozim:

1. ixtiyoriy tanlangan foydalanuvchilar, foydalanuvchilar guruhlar yoki **Active Directory** guruhlar bo'yicha hisobotlarni shakllantirish;
2. hisobotlarni butun davr bo'yicha ham, belgilangan vaqt oralig'i bo'yicha ham shakllantirish;
3. hisobot imkoniyatlarining qisqacha tavsifiga ega hisobot yaratish ustasi (Wizard) mavjud bo'lishi;
4. oldindan tayyorlangan (standart) hisobotlar mavjud bo'lishi;
5. kamida **20 ta iyerarxiya darajasiga** ega guruhlar va kichik guruhlar yaratish imkoniyati;
6. hisobotlarni oddiy **"drag-and-drop"** (sichqoncha yordamida sudrab o'tkazish) usuli bilan bir guruhdan boshqasiga ko'chirish imkoniyati;
7. kichik guruhlar oddiy **"drag-and-drop"** usuli bilan bir guruhdan boshqasiga ko'chirish imkoniyati;
8. turli turdagi hisobotlarga kirish huquqlarini sozlash imkoniyati;
9. hisobotlarni shakllantirish jadvalini (rejasini) sozlash hamda ularni yuborish uchun elektron pochta manzillarini tanlash imkoniyati.

Tizim tomonidan ushlab olingan barcha ma'lumotlar quyidagi turdagi hisobotlar ko'rinishida taqdim etilishi lozim:

1. **"Foydalanuvchilar faolligi"** hisoboti;
2. foydalanuvchilar bo'yicha hisobot;
3. foydalanuvchilar bo'yicha **TOP** hisobot;
4. axborot xavfsizligi siyosatlari bo'yicha hisobot;
5. foydalanuvchilar bo'yicha umumlashtirilgan hisobot;
6. ish vaqti tabeli hisoboti;
7. ilovalar faolligi bo'yicha hisobot;
8. brauzer faolligi bo'yicha hisobot;
9. foydalanuvchining umumiy faolligi bo'yicha hisobot.

2.26. Xavfsizlik buzilishlarini tergov qilish funksionaliga qo'yiladigan talablar

Tizim axborot xavfsizligi hodisalarini tergov qilish doirasida hujjatlar bilan ishlashni tashkil etish imkonini beruvchi funksionalga ega bo'lishi hamda quyidagi imkoniyatlarni ta'minlashi lozim:

1. xavfsizlik hodisalari bo'yicha dalillarni **tergov ishi (case)** yaratish orqali to'plash, bunda tergov ishi quyidagilarni o'z ichiga olishi kerak:

- ishning nomi va tavsifi;
- ish yaratilgan sana;
- hodisa (insident) to'g'risidagi ma'lumotlar;
- jalb qilingan shaxslar va ularning rekvizitlari ro'yxati;
- hodisani tergov qilish bo'yicha o'tkazilayotgan yoki o'tkazilgan tadbirlar hamda ularning natijalari;
- tergov natijalari bo'yicha xulosalar;
- tergov materiallari: hujjatlar, tizim tomonidan ushlab olingan hodisalar hamda ishga yuklangan tashqi hujjatlar;
- ichki hujjatlar rekvizitlari: ma'lumot turi, lokal foydalanuvchi, masofaviy foydalanuvchi, ushlab olingan sana va hujjat hajmi;
- tergov materiallari sifatida tashqi hujjatlar;
- tizimning boshqa modullaridan hujjatlarni tergov ishiga biriktirish imkoniyati.

2. Bir vaqtning o'zida bir nechta axborot xavfsizligi mutaxassislari (Security Officer) tomonidan tergov olib borilishini ta'minlash maqsadida tizim quyidagi imkoniyatlarga ega bo'lishi lozim:

- tergov ishlariga kirish huquqlarini chegaralash, ya'ni to'liq kirish, faqat o'qish huquqi yoki kirishni taqiqlash huquqlarini belgilash;
- alohida tergov ishlari va kichik guruhlar uchun ota guruhdan kirish huquqlarini meros qilib olish;
- har bir tergov ishi uchun mas'ul shaxsni tayinlash;
- **"Menga biriktirilgan"** tergov ishlarini filtrlash imkoniyati.

2.27. Xatarlarni tahlil qilish funksionaliga qo'yiladigan talablar

Tizim tashkilot uchun anomal va potensial xavfli bo'lgan xodimlar xatti-harakatlaridagi o'zgarishlarni kuzatish imkonini beruvchi nazorat-tahlil mexanizmlarini ta'minlashi hamda quyidagi funksional imkoniyatlarga ega bo'lishi lozim:

1. xodimlarning xatti-harakatlari modellarini shakllantirish va ularga tegishli xavf darajasini belgilash;

2. xavfsizlik bo'limi mutaxassislari xavf darajasi, xodimlarning xatti-harakatlari hamda xavf darajasining o'zgarishiga sabab bo'lgan axborot xavfsizligi siyosati hodisalari to'g'risida xabardor qilish;

3. xodimlar xatti-harakatlaridagi o'zgarishlarni real vaqt rejimida miqdoriy ko'rsatkichlar va grafiklar yordamida kuzatish;

4. ko‘rib chiqilmagan hodisalar hamda barcha hodisalar bo‘yicha xavf darajasidagi o‘zgarishlarni ko‘rish imkoniyati;

5. foydalanuvchilarning xavf darajasi bo‘yicha jadval ko‘rinishidagi hisobotni saqlash va chop etish imkoniyati.

2.28. Tizimni masshtablashga qo‘yiladigan talablar

1. Tizimning barcha komponentlari bitta serverga o‘rnatilishi yoki bir nechta serverlarga taqsimlangan holda joylashtirilishi mumkin bo‘lishi, bu esa bir vaqtning o‘zida ko‘p sonli xodimlarni nazorat qilish uchun zarur masshtablanuvchanlikni ta‘minlashi lozim.

2. Tarmoq konfiguratsiyasi, qayta ishlanayotgan ushlab olingan ma‘lumotlar hajmi va boshqa parametrlarga qarab tizim yirik va murakkab tashkil etilgan tarmoqlarni nazorat qilish hamda tarmoq va apparat resurslari yuklamasini taqsimlash uchun moslashuvchan tarzda masshtablanishi lozim.

3. Bir nechta ma‘lumotlarni ushlab olish serverlarini o‘rnatish imkoniyati, internetga chiqishning bir nechta nazorat qilinadigan kanallari bo‘yicha ma‘lumotlarni parallel ushlab olishni ta‘minlash uchun.

4. Tarmoqning turli segmentlari yoki kompyuterlarning turli guruhlarini nazorat qilish uchun bir nechta agentlarni boshqarish serverlarini o‘rnatish imkoniyati.

5. Tarmoq yuklamasini muvozanatlash uchun bir nechta oraliq agent serverlarini o‘rnatish imkoniyati.

6. Katta yuklamalarni ko‘plab serverlar o‘rtasida gorizontal masshtablash maqsadida klasterni tashkil etish imkoniyati.

7. Server va ma‘lumotlar bazasi yuklamasini optimallashtirish hamda taqsimlash uchun bir nechta indeksatsiya serverlarini o‘rnatish imkoniyati.

8. Bir vaqtning o‘zida bir nechta pochta serverlari (**MS Exchange**, **IBM Lotus Domino** va boshqalar) bilan ishlashni qo‘llab-quvvatlash.

Tizim ko‘p yadroli va ko‘p protsessorli tizimlarda yuklamani to‘liq taqsimlashni qo‘llab-quvvatlashi lozim.

2.29. Tizimni ma‘muriy boshqarishga qo‘yiladigan talablar

Tizim quyidagi funksional imkoniyatlarni ta‘minlashi lozim:

1. tizimning barcha komponentlarini ikkita konsol orqali markazlashtirilgan boshqarish: yagona administrator konsoli va yagona foydalanuvchi (axborot xavfsizligi xizmati xodimi) konsoli;

2. konsollar va server o‘rtasidagi trafikni shifrlash imkoniyatini ta‘minlash;

3. tizimning barcha server komponentlari uchun axborot omborlarini markazlashtirilgan tarzda ulash va sozlash;
4. tizimning ichki brendmauerini (Firewall) avtomatik boshqarishni o‘chirib qo‘yish imkoniyati;
5. agentlar uchun profillarni sozlashda kompyuterni agentlar sxemasi orqali profilga qo‘shish, shuningdek obyektlarni profillar o‘rtasida nusxalash yoki ko‘chirish imkoniyati;
6. axborot xavfsizligi siyosati qoidalari ishga tushganda dasturlar va skriptlarni avtomatik ishga tushirishni sozlash imkoniyati;
7. tizimning barcha server komponentlari va servislarining holatini real vaqt rejimida kuzatish, ularning har biri bo‘yicha asosiy statistikani aks ettirish hamda tizim orqali server komponentlari va servislarini ishga tushirish va boshqarish imkoniyati;
8. administrator konsolida bir nechta foydalanuvchining bir vaqtning o‘zida ishlashini qo‘llab-quvvatlash;
9. tizim serverlarini avtomatik va qo‘lda avtorizatsiya qilish imkoniyati;
10. eksport qilinadigan hujjatlardagi tizim logotipini foydalanuvchi logotipiga almashtirish imkoniyati;
11. boshqa vaqt mintaqalaridan olingan ma’lumotlarni qulay ko‘rish maqsadida vaqt mintaqasini o‘zgartirish imkoniyati;
12. boshqaruv konsolining turli modullarini bir vaqtning o‘zida turli monitorlarda ochish imkoniyati;
13. boshqaruv konsoli ishga tushirilganda tizimning oldindan belgilangan modullar to‘plamini avtomatik ochish imkoniyati;
14. boshqaruv konsolida yangi versiyalar chiqarilgani va ularga kiritilgan o‘zgarishlarning batafsil tavsifi haqidagi bildirishnomalarni aks ettirish imkoniyati;
15. tizimni yangilash bo‘yicha so‘rovni to‘g‘ridan-to‘g‘ri boshqaruv konsoli orqali yuborish imkoniyati;
16. texnik qo‘llab-quvvatlash muddati tugagan taqdirda uni uzaytirish bo‘yicha so‘rovni to‘g‘ridan-to‘g‘ri boshqaruv konsoli orqali yuborish imkoniyati.

2.30. Foydalanuvchilarni avtorizatsiya qilishga qo‘yladigan talablar

Tizim foydalanuvchilarni avtorizatsiya qilishning bir nechta usullarini taqdim etishi lozim:

1. **Windows** hisob yozuvlari asosida;
2. ichki autentifikatsiya tizimi asosida.

Tizim quyidagi funksional imkoniyatlarga ega bo‘lishi lozim:

1. parolning amal qilish muddatini (kunlarda) cheklash imkoniyati, ushbu muddat tugagandan so'ng tizimga kirishni bloklash;

2. ketma-ket **3 ta** muvaffaqiyatsiz kirish urinishidan so'ng foydalanuvchini bloklash imkoniyati;

3. avtorizatsiya qilishga oid barcha urinishlar haqidagi ma'lumotlarni jurnalda saqlash imkoniyati;

4. Administrator konsoli sozlamalarini o'zgartirish uchun qo'shimcha parolni belgilash imkoniyati;

5. belgilangan bo'sh turish (idle) vaqti oshib ketganda konsollardan avtomatik chiqish imkoniyati;

6. belgilangan seans davomiyligi tugagandan so'ng konsoldan avtomatik chiqish imkoniyati.

Tizim o'z faoliyati davomida Buyurtmachining amaliy axborot tizimlari faoliyatiga salbiy ta'sir ko'rsatmasligi lozim.

Kelishildi:

A.R.Ibodov



S.R.Mamasiddikov



X.T.Abdurazzoqov



A.F.Iskandarov

