“TASDIQLAYMAN”

“Agrobank” ATB

Boshqaruv raisi o'rinbosari v.b.



F.B.Nasriyev

2026 yil “9” noyabr

Group-IB fraud protection (sessiyaviy antifrod)
bir yillik litsenziyasini xarid qilish uchun
TEXNIK TOPSHIRIQ

Toshkent sh. 2026-yil

Atamalar va qisqartmalar

Atama	Tushuncha
Buyurtmachi	«Agrobank» ATB
Tashkilot	Bank yoki to‘lov tashkiloti
JSh MBX	Buyurtmachining jismoniy shaxslarga masofaviy bank xizmatlari ko‘rsatish tizimi (internet-banking, mobil bank)
YSh MBX	Buyurtmachining yuridik shaxslarga masofaviy bank xizmatlari ko‘rsatish tizimi (internet-banking, mobil bank)
P2P	Buyurtmachining kartadan kartaga pul o‘tkazish sahifasi.
3-D Secure	Internetda tovar uchun to‘lovni tasdiqlashga mo‘ljallangan emitent-bank sahifalari
SAT	Group-IB sessiyaviy antifrod tizimi
DT	Dasturiy ta’minot
Obfuskatsiya	Dastur manba matni yoki bajariluvchi kodini uning funksionalligini saqlagan, ammo dekompilyatsiya jarayonida tahlil qilish, ishlash algoritmlarini tushunish va o‘zgartirishni qiyinlashtiradigan shaklga keltirish
Operator	SAT qoidalarini tahlil qiluvchi va sozlovchi SAT foydalanuvchisi.
Foydalanuvchi	12 oy ichida jismoniy yoki yuridik shaxslar masofaviy bank xizmatlari tizimiga kamida bir marta kirgan foydalanuvchi.
Proksi-server	Kompyuter tarmoqlarida foydalanuvchilarga boshqa tarmoq xizmatlariga bilvosita so‘rov yuborish imkonini beruvchi server (dasturlar majmuasi).
Qoida	Anomaliyalarni aniqlash uchun Buyurtmachi foydalanuvchilarining hozirgi xatti-harakatlari va qurilmasi haqidagi ma’lumotlarni avval yig‘ilgan ma’lumotlar bilan nomuvofiqlik belgilariga ko‘ra solishtirishga xizmat qiluvchi, mantiqiy amallar orqali birlashtirilgan bir yoki bir nechta mezonlar to‘plami.
Veb-sensor	JavaScript kodi ko‘rinishida yetkazib beriladigan, firibgarlik yoki avtomatlashtirilgan faollik belgilarini aniqlash uchun axborot yig‘ish maqsadida raqamli xizmat kanalining (internet-banking, P2P, 3-D Secure) veb-sahifasiga o‘rnatiladigan SAT qismi.
Mobil sensor	iOS/Android operatsion tizimlari uchun SDK shaklida yetkazib beriladigan, firibgarlik belgilarini aniqlash va xavfga asoslangan autentifikatsiyaga tayyorlash uchun ma’lumot yig‘ish maqsadida Buyurtmachining mobil ilovasiga o‘rnatiladigan SAT qismi.
HQ	Hisob qaydnomasi.
API	Application Programming Interface – tashqi dasturiy mahsulotlarda foydalanish uchun dasturiy mahsulot taqdim etadigan tayyor sinflar, protseduralar, funksiyalar, tuzilmalar va konstantalar majmuasi.

Atama	Tushuncha
Fishing	Soxta sahifalardan foydalanib foydalanuvchilarning identifikatsiya ma’lumotlarini qo‘lga kiritishga qaratilgan internet-firibgarlik turi.
Vishing	Telefon aloqasi orqali foydalanuvchilarning identifikatsiya ma’lumotlarini yoki ruxsatsiz moliyaviy operatsiyalar uchun zarur ma’lumotlarni qo‘lga kiritishga qaratilgan internet-firibgarlik turi.
Cookie	Sessiya tokeni – veb-server tomonidan yuboriladigan va foydalanuvchi kompyuterida saqlanadigan kichik ma’lumot bo‘lagi.
Proxy	Kompyuter tarmog‘ida internet foydalanuvchisi bilan maqsadli serverlar orasidagi vositachi server.
TOR	Himoyalangan anonim tarmoq ulanishini o‘rnatish imkonini beruvchi proksi-serverlar tizimi. Ma’lumotlarni shifrlangan shaklda uzatadigan virtual tunnellarning anonim tarmog‘i sifatida qaraladi.
Veb-inyeksiyalar	Mijoz tomonida (brauzerda) veb-sahifa tarkibini o‘zgartirish (kod kiritish)

1 Umumiy ma’lumotlar

«Agrobank» ATB ehtiyojlari uchun tovarlar va xizmatlarni xarid qilish doirasida yetkazib beruvchi quyidagi texnik talablarga mos keluvchi, masofaviy xizmat ko‘rsatish kanallarida noqonuniy va firibgarlik operatsiyalarini amalga oshiruvchi botlar faolligini aniqlash, monitoring qilish, anomaliyalarni aniqlash, foydalanuvchilar xatti-harakatlarini profillash va tahlil qilish imkonini beruvchi Group-IB Fraud protection (sessiyaviy antifrod) bir yillik litsenziyasini yetkazib berishi lozim.

Tizimning to‘liq nomi: «Agrobank» ATB uchun Group-IB sessiyaviy antifrod tizimi».

Ushbu hujjatda tizimning qisqartirilgan nomi: SAT.

Ijrochi: Ijrochi tashkilotning nomi (keyingi o‘rinlarda – Ijrochi)

Buyurtmachi: «Agrobank» ATB (Toshkent sh., Shayxontohur tumani, B. Zokirov ko‘chasi, 2A-uy).

Qo‘llanish sohasi

SAT Buyurtmachining raqamli resurslarida (jismoniy shaxslar MBX, yuridik shaxslar MBX, P2P, 3-D Secure) anomaliyalarni aniqlash, foydalanuvchilarning xatti-harakatlarini profillash va tahlil qilish, shuningdek, masofaviy xizmat kanallarida noqonuniy va firibgarlik operatsiyalarini amalga oshiruvchi botlar faoliyatini aniqlash maqsadida sessiya va xulq-atvor ma’lumotlarini yig‘ishi hamda tahlil qilishi kerak. SATdan foydalanish doirasida Buyurtmachi xodimlari va uning tashqi tizimlariga qo‘shimcha tahlil o‘tkazish uchun foydalanuvchilar sessiyalari, qurilmalari va tizim qoidalarining ishga tushish natijalari haqidagi ma’lumotlarga (shu jumladan API orqali) kirish imkoniyati berilishi kerak.

Dasturiy ta’minot ishlab chiqaruvchi tomonidan e’lon qilingan foydalanish maqsadlari va spetsifikatsiyada ko‘rsatilgan funksional imkoniyatlarga mos kelishi kerak. Dasturiy ta’minotda zararli dasturlar bo‘lmasligi lozim. Buyurtmachining ushbu dasturiy ta’minotdan foydalanishi, xususan, uning kompyuter ma’lumotlarini ruxsatsiz yo‘q qilish, bloklash, o‘zgartirish, nusxalash yoki ma’lumotlarni himoyalash vositalarini zararsizlantirishga, shuningdek, Buyurtmachiga boshqa zarar yetkazishga olib kelmasligi kerak.

Tizim joriy etilishiga asos bo‘ladigan hujjatlar ro‘yxati

O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-sonli «Kiberxavfsizlik to‘g‘risida»gi Qonuni;

O‘zbekiston Respublikasi Prezidentining 2023-yil 31-maydagi PQ-167-sonli «O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida»gi qarori;

Prezidentning 2020-yil 15-iyundagi PQ-4751-sonli «O‘zbekiston Respublikasida kiberxavfsizlikni ta’minlash tizimini yanada takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida»gi qarori;

2024-yil 21-mayda 3513-son bilan davlat ro‘yxatidan o‘tkazilgan O‘zbekiston Respublikasi Markaziy bankining qarori bilan tasdiqlangan “To‘lov tizimlari, to‘lov tizimlari operatorlari va to‘lov xizmatlarini ko‘rsatuvchilarning axborot xavfsizligi va kiberxavfsizligini ta’minlash hamda raqamli texnologiyalar orqali sodir etiladigan huquqbuzarliklarning oldini olish choralari to‘g‘risidagi nizomi“;

2026-yil 21-yanvarda 3759-son bilan davlat ro‘yxatidan o‘tkazilgan O‘zbekiston Respublikasi Markaziy bankining qarori bilan tasdiqlangan “Kredit va to‘lov tashkilotlari, to‘lov tizimi operatorlari tomonidan jismoniy shaxslarga masofadan moliyaviy xizmatlar ko‘rsatishda axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda frod holatlarining oldini olish bo‘yicha minimal talablar to‘g‘risidagi nizomi“;

2.Tizimga qo‘yiladigan talablar

Veb-kanalni himoyalash bo‘yicha talablar:

- foydalanuvchi qurilmasining raqamli izini aniqlash (device fingerprinting);
- mijozlarning hisob ma’lumotlaridan ruxsatsiz foydalanish holatlarini aniqlash;
- himoyalanayotgan veb-ilovaga begona kod kiritilishi holatlarini aniqlash;
- mijoz tomonidagi veb-qismga firibgarlik maqsadida kod kiritishni (veb-inyeksiyalarni) aniqlash;
- fishingdan himoyani ta’minlash;
- mijoz qurilmasiga ruxsatsiz masofaviy ulanishlarni aniqlash;
- mijozning TOR, proxy va «anonimayzerlar» orqali ishlashini aniqlash;
- masofaviy boshqaruv vositalari (TeamViewer, AnyDesk, RDP, AmmyAdmin va boshqalar) yordamidagi firibgarlikni aniqlash;
- xosting va kolokatsiya xizmatlarini ko‘rsatuvchi kompaniyalarning buzib kirilgan ajratilgan serverlari yoki qurilmalaridan ulanishni aniqlash;
- qurilmaning asl parametrlarini almashtiruvchi brauzerlardan («antidetect browser») foydalanishni aniqlash;
- navigatsiya, kursor harakati, tugmalarni bosish tezligi va ketma-ketligi, tanaffuslar hamda shakllar bilan o‘zaro ishlash kabi xulq-atvor ma’lumotlari asosida firibgar va qonuniy foydalanuvchi harakatlarini aniqlash;
- Bank serverlariga bevosita tarmoq so‘rovlarini yuboruvchi, headless browser turidagi vositalardan (Selenium, PhantomJS va boshqalar) foydalanuvchi, qonuniy cookie fayllarini qayta ishlatuvchi (cookie stuffing), inson xatti-harakatiga taqlid qiluvchi va boshqa usullardan foydalanadigan botlarning zararli faoliyatini aniqlash va bloklash;

- hisob qaydnomalarini avtomatik buzishga urinishlarni («brute force») yoki boshqa resurslardan o‘g‘irlangan hisob ma’lumotlaridan («credential stuffing») foydalanishni aniqlash va bloklash;

- qurilma parametrlarini almashtiruvchi vositalarni (Sphere, Multilogin va boshqalar) aniqlash;

- veb-kanalda qurilmaning global identifikatori va turli buyurtmachilar o‘rtasidagi korrelyatsiya.

Mobil kanalni himoyalash bo‘yicha:

- mobil qurilmani identifikatsiya qilish;

- signatura va xulq-atvor tahlili yordamida zararli mobil ilovalarni aniqlash;

- ilovaning mobil qurilma emulyatorida yoki mobil platformaning norasmiy versiyasida (root huquqli qurilmada) ishga tushishini aniqlash;

- mijoz qurilmasiga ruxsatsiz masofaviy ulanishlarni (masofaviy boshqaruv vositalaridan foydalanishni) aniqlash;

- mijozlarning hisob ma’lumotlaridan ruxsatsiz foydalanish holatlarini (yangi qurilmadan yoki firibgarlik qurilmasidan kirishni) aniqlash;

- mobil kanalda passiv biometriya yordamida mobil qurilma emulyatorlari/simulyatorlarini aniqlash;

- mijozning TOR, proxy va «anonimayzerlar» orqali ishlashini aniqlash;

- xosting va kolokatsiya xizmatlarini ko‘rsatuvchi kompaniyalarning buzib kirilgan ajratilgan serverlari yoki qurilmalaridan ulanishni aniqlash;

- ilova doirasida bitta foydalanuvchining mobil qurilmalarini identifikatsiya qilish;

- mobil qurilma almashtirilganda foydalanuvchini kuzatib borish;

- Android ilovasi ishga tushirilishidan oldin amalga oshirilgan qo‘ng‘iroqlarni tahlil qilish;

- mobil kanalda qurilmaning global identifikatori va turli buyurtmachilar o‘rtasidagi korrelyatsiya;

- firibgarlik darajasini kamaytirish;

- ijtimoiy muhandislik yordamidagi firibgarlik belgilarini aniqlash;

- botlar faolligini aniqlash;

- axborot xavfsizligi hodisalarini tekshirish samaradorligini oshirish;

- autentifikatsiyada SATdan ikkinchi omil sifatida foydalanish imkoniyati.

3 Yetkazib beriladigan dasturiy ta’minotga talablar

- Dasturiy ta’minot litsenziya kalitlari security@agrobank.uz elektron manziliga yuborilishi orqali yetkazib berilishi lozim;

- Dasturiy ta’minotni joylashtirish uchun hisoblash quvvatlari Ijrochi tomonidan taqdim etiladi.

- Xarid qilinadigan dasturiy ta’minot yetkazib berish vaqtida dolzarb versiyada bo‘lishi kerak;

- Dasturiy ta’minotda foydalanuvchi rollarini ajratish va boshqarish imkoniyati bo‘lishi kerak.

3.1 Kafolat xizmatiga talablar

- Ijrochi yetkazib beriladigan dasturiy ta’minotga kafolat xizmatini ko‘rsatishi shart.

- Xarid qilinadigan dasturiy ta’minot kamida bir yillik kafolat va texnik yordamga ega bo‘lishi kerak;

- Xarid qilinadigan dasturiy ta’minot yetkazib berish bilan bog‘liq barcha bojxona bojlari va boshqa xarajatlardan to‘liq tozalangan bo‘lishi lozim;

3.2 Texnik yordamga talablar

- Texnik yordam doirasida Buyurtmachi nosozliklar va texnik yordam so‘rovlari haqida so‘rovlar soni cheklanmagan holda xabar berish imkoniyatiga ega bo‘lishi kerak.

- Texnik yordam portaliga kirish hisob qaydnomalari soni bilan cheklanmasligi kerak.

- Murojaatlarni ko‘rib chiqish kamida texnik muammolarni hal qilish va tizimni sozlashni o‘z ichiga olishi kerak.

- Yangi ochilgan murojaatga javob berish vaqti 2 ish kunidan oshmasligi kerak.

- Texnik yordam xizmati tizimning amaldagi versiyalari va yangilanishlari, shuningdek, texnik hujjatlar – kamida tizim foydalanuvchisi va administratori qo‘llanmalaridan foydalanish imkoniyatini kafolatlashi kerak.

- Texnik yordam 24/7 rejimida ko‘rsatilishi kerak.

- Ijrochi yordami o‘zbek, ingliz va rus tillarida ko‘rsatiladi.

- Texnik muammo bo‘yicha murojaat kamida ikki aloqa kanali orqali ochilishi kerak: veb-brauzerdan ochiladigan, masofadan murojaat yuborish va uning holatini kuzatish imkonini beruvchi texnik yordam portali hamda elektron pochta.

3.3 Xodimlarni o‘qitishga talablar

- Ijrochi dasturiy ta’minotning vazifasi va funksiyalariga muvofiq undan foydalanish hamda uni qo‘llab-quvvatlash uchun zarur ko‘nikmalarni shakllantirish maqsadida xodimlarni o‘qitish majburiyatini oladi.

- Ijrochi Buyurtmachi xodimlarini dasturiy ta’minotdan foydalanish va uni boshqarish bo‘yicha o‘qitishi kerak.

3.4 Texnik hujjatlarga talablar

- Ijrochi dasturiy ta’minotni o‘rnatish, sozlash va undan foydalanish bo‘yicha to‘liq hujjatlarni taqdim etishi kerak.

- Taqdim etiladigan barcha texnik vositalar to‘liq va dolzarb texnik hujjatlar bilan birga berilishi kerak.

3.5 Xavfsizlikka talablar

Ijrochi joriy etishning barcha bosqichlarida dasturiy ta’minot yaxlitligini nazorat qilishi kerak.

Dasturiy ta’minotni o‘rnatuvchi xodimlar tegishli malaka va tajribaga ega bo‘lishi kerak.

Ijrochi dasturiy ta’minot uchun muntazam yangilanishlar va tuzatishlar, shu jumladan xavfsizlik yangilanishlarini taqdim etishi kerak.

4 Ishtirokchiga talablar

- ishlab chiqaruvchi tomonidan tasdiqlangan vakolatli hamkor maqomiga ega bo‘lish;

- yechim yetkazib beruvchisi yoki ishlab chiqaruvchi vakilida yechimni rus, ingliz va o‘zbek tillarida o‘rnatish hamda sozlash ishlarini bajara oladigan sertifikatlangan mutaxassis (Advanced yoki unga teng daraja) bo‘lishi;

- mutaxassisning ushbu sohada (o‘rnatish, sozlash, qo‘llab-quvvatlash) kamida 2 yillik ish tajribasiga ega bo‘lishi;

- so‘ralgan konfiguratsiyadan to‘liq foydalanishni ta’minlovchi, barcha qismlari bilan jamlangan va ishlaydigan yechimni taqdim etishi;

- loyiha qiymatini oshirish uchun dasturiy yechimni joriy etish muddatlarini sun’iy o‘zgartirmasligi kerak;

5 Tizimga texnik-texnologik talablar

5.1 Veb-xizmatlarda

Quyidagilar amalga oshirilishi kerak:

- parametrlariga ko‘ra foydalanuvchi qurilmasini identifikatsiya qilish (device fingerprinting);

- qurilmani global identifikatsiya qilish;

- mijozlar hisob ma’lumotlaridan ruxsatsiz foydalanish holatlarini aniqlash;

- himoyalanadigan veb-ilovaga begona kod kiritish holatlarini aniqlash;

- server tomonidagi veb-qismga firibgarlik maqsadida kiritmalarni (veb-inyeksiyalarni) aniqlash;

- yechim yakuniy foydalanuvchi tomonida Buyurtmachining veb-ilovasi mijoz qismiga (html, js va boshqalar) kiritmalarni aniqlashi kerak;

- yechim Buyurtmachi veb-ilovasidagi bunday kiritmalarni qo‘lda va avtomatik tasniflashni ta’minlashi kerak;

- yechim dinamik o‘zgaruvchi kiritmalarni tasniflashi kerak;

- yakuniy foydalanuvchi tomonida zararli kiritma aniqlansa, SAT hodisa yaratishi kerak.

- fishingni aniqlash;

- yechim Buyurtmachining veb-ilovasiga o‘tishlar haqida ma’lumot yig‘ishi kerak;

- yechim Buyurtmachining qonuniy veb-ilovasi nusxalanib, zararli maqsadlarda ishlatilishini aniqlashi kerak;

- to‘plangan havolalar avtomatik, shu jumladan mashinali o‘qitish algoritmlari yordamida tasniflanishi kerak; bunda logotip va favicon bilan tasvirlarning o‘xshashligini, sahifa matnini va SSL sertifikatlarini tekshirish kabi usullar qo‘llanadi, biroq ular bilan cheklanilmaydi.

- mijozning TOR, proxy va «anonimayzerlar» orqali ishlashini aniqlash;

- xosting va kolokatsiya xizmatlarini ko‘rsatuvchi kompaniyalarning buzib kirilgan ajratilgan serverlari yoki qurilmalaridan ulanishni aniqlash;

- xavflarni shakllantirish uchun har bir mijoz ishlatadigan brauzerlarni monitoring qilish;

- antidetect brauzeridan foydalanishni aniqlash;

- Dolphin, Incognition, CheBrowser, AdsPower va boshqa antidetect brauzerlarini aniqlash;

- Buyurtmachining veb-resursidagi navigatsiya, kursor harakatlari, tugmalarni bosish tezligi va ketma-ketligi, tanaffuslar va shakllar bilan o‘zaro aloqalar kabi xulq-atvor ma’lumotlari asosida firibgar va qonuniy foydalanuvchining ishini aniqlash;

- hisob qaydnomalarini avtomatik buzishga urinishlarni («brute force») yoki boshqa resurslardan olingan buzib kirilgan hisob qaydnomalaridan («credential stuffing») foydalanishni aniqlash va bloklash;

- Buyurtmachining tashqi tizimlariga, masalan, tranzaksion antifrod tizimiga qo‘shimcha xulosalarni taqdim etish;

- foydalanuvchi Buyurtmachi ilovasidan foydalanayotganda uning harakatlari haqidagi axborotni yuborish;

- quyidagi brauzerlardan axborot olish, shuningdek, foydalanuvchi ko‘rsatilganidan eski versiyalardan foydalansa, ulanishni bloklash:

Chromium 26 va undan yuqori (Google Chrome, Yandex Browser, Opera shu jumladan)

Internet Explorer 9 va undan yuqori

Microsoft Edge 13 va undan yuqori

Mozilla Firefox 4 va undan yuqori

Safari 8 va undan yuqori

- Buyurtmachi tanlagan boshqa qoidalar (bir nechta hisob qaydnomasi, firibgarlik tarmoq segmentlaridan foydalanish va boshqalar) asosida foydalanuvchi va dasturiy ta’minotning zararli faoliyatini aniqlash; bu imkoniyat Buyurtmachining ko‘p sahifali internet-resurslarida ham, Single Page Application texnologiyasidagi resurslarida ham ishlashi kerak;

- maxfiy ma’lumotlarni, shu jumladan shaxsga doir ma’lumotlar va bank sirini tashkil etuvchi ma’lumotlarni yig‘maslik va taqdim etmaslik.

5.2 Mobil ilovalarda

Quyidagilar bajarilishi va SATga uzatilishi kerak:

- mobil qurilmani identifikatsiya qilish;

- qurilmani global identifikatsiya qilish;

- Buyurtmachining mobil ilovasi qalbakilashtirilganini aniqlash (imzoni tekshirish, yaxlitlikni nazorat qilish);

- operatsion tizim versiyasi va root huquqlari mavjudligi haqida SATga ma’lumot taqdim etish, ilovaning mobil qurilma emulyatorida ishga tushishini aniqlash;

- mijoz qurilmasiga masofaviy ulanishlarni (masofadan boshqaruv vositalaridan foydalanishni) aniqlash;

- masofadan kirish va boshqarish dasturlari paydo bo‘lishi va mavjudligiga ko‘ra;

- masofaviy boshqaruvning faol sessiyalari mavjudligiga ko‘ra;

- xulq-atvor belgilariga ko‘ra masofaviy boshqaruvni aniqlash.

- mijoz SIM-kartani almashtirganini aniqlash va SATga uzatish;

- Buyurtmachi ilovasidan foydalanilganda foydalanuvchining teginishlari va surishlari, ilova interfeysi elementlari bilan o‘zaro ishlashi, matn terish tezligi va mobil qurilma sensorlari ma’lumotlari (xususiyatlari) yig‘ilib SATga uzatilishi kerak;

- SATga GPS ma’lumotlari hamda ishlatiladigan ma’lumot uzatish kanallari (Wi-Fi, mobil tarmoq, simli internet) haqida ma’lumot taqdim etish;

- mobil qurilma GPS sensoridan uzunlik, kenglik, balandlik, yo‘nalish, joylashuv/harakat tezligi yig‘ilishi kerak;

- mobil qurilma ayni paytda ulangan uyali aloqa minorasining identifikatsiya ma’lumotlari yig‘ilishi kerak;

- qurilma ulangan Wi-Fi kirish nuqtasi va mobil qurilmaga mavjud boshqa kirish nuqtalarining identifikatorlari yig‘ilishi kerak;

- foydalanuvchi qurilmasida debugger aniqlangani haqidagi ma’lumotni SATga taqdim etish;

- mobil qurilmadagi dasturchi rejimini va mobil ilovaning faol nosozliklarni tuzatish sessiyasini aniqlash;

- foydalanuvchi qurilmalarida Buyurtmachi ilovalari ishlashini sezilarli sekinlashtirmaslik;

- zarur ma’lumotlarni yig‘ish va SATga taqdim etish foydalanuvchi javobini talab qiladigan muloqot oynalari yoki tasdiqlash so‘rovlari hamda bildirishnomalarni keltirib chiqarmasligi kerak;

- foydalanuvchi qurilmasi va Buyurtmachi SATi yoki uning infratuzilmasi o‘rtasidagi tarmoq faolligini sezilarli oshirmaslik;

- mahalliy mobil ilovalarda ham, gibrid ilovalarda ham (WebView komponentlaridan foydalangan holda) ishlash;

- foydalanuvchi harakatlari haqidagi ma’lumotni faqat Buyurtmachi ilovasidan foydalanilgan vaqtda yuborish;

- brauzerlar hamda Android va iOS mobil operatsion tizimlarining standart funksiyalaridan foydalanish;

quyidagi OTlarda ishlash va ma’lumot olish imkoniga ega bo‘lish:

- Android v.5 (API 14) va undan yuqori;
- iOS v.10 va undan yuqori.

- maxfiy ma’lumotlarni, shu jumladan shaxsga doir ma’lumotlar va bank sirini tashkil etuvchi ma’lumotlarni yig‘maslik va taqdim etmaslik.

6 SATga umumiy talablar

6.1 SAT komponentlari ro‘yxati

SAT quyidagi komponentlarni o‘z ichiga olishi kerak

- foydalanuvchi qurilmasidan ma’lumot yig‘ish quyi tizimi (veb va mobil sensorlar);
- tahlil va qayta ishlash quyi tizimi;
- hisobot va vizualizatsiya quyi tizimi;
- axborot almashinuvi quyi tizimi;
- O‘zbekiston Respublikasi Markazlashtirilgan antifrod tizimi bilan axborot almashinuvi quyi tizimi.

6.2 Foydalanuvchi qurilmasidan ma’lumot olish quyi tizimiga talablar

Quyi tizim quyidagilarni bajarishi kerak:

- Buyurtmachi tizimlarining ishlashiga xalaqit bermaslik;

- firibgarning quyi tizim ishlashiga faol qarshilik ko‘rsatishining mumkin bo‘lgan turlarini hisobga olish:

- statik tahlildan himoyaga ega bo‘lish;

- veb-xizmatlar uchun SATning mijoz qismi kodni dinamik obfuskatsiyalashni ta’minlashi kerak;

- SAT mijoz modulidan uzatilayotgan ma’lumotlarning firibgar tomonidan ko‘rib chiqilishidan himoyasini ta’minlash;

- SAT mijoz modulidan uzatilgan ma’lumotlar yaxlitligini nazorat qilish;

- nosozliklarni tuzatish hamda runtime muhitini almashtirish vositalarini aniqlash.

- Buyurtmachi foydalanuvchisi qurilmasi buzilganini ko‘rsatuvchi indikatorlarni aniqlash:

Veb-ilovalar uchun SAT quyidagilarni ta’minlashi kerak:

- yakuniy foydalanuvchi tomonida Buyurtmachi veb-ilovasining mijoz qismiga (html, js va boshqalar) kiritilgan inyeksiyalarni aniqlash;

- Buyurtmachi veb-ilovasidagi bunday inyeksiyalarni qo‘lda va avtomatik tasniflash;

- dinamik o‘zgaruvchi inyeksiyalarni tasniflash;

- internetdagi shubhali yoki firibgarlik resurslariga murojaatlarni aniqlash;

- shakllarning belgilangan maydonlari va sahifaning boshqa elementlariga ruxsatsiz murojaatlarni aniqlash.

Buyurtmachining mobil ilovalari uchun:

- foydalanuvchi yakuniy qurilmasiga o‘rnatilgan zararli dasturiy ta’minotni signatura asosida tahlil qilishni ta’minlash;

- yakuniy foydalanuvchi qurilmasida zararli dasturiy ta’minot mavjudligi va ishlashini xulq-atvor asosida tahlil qilish, jumladan, lekin quyidagilar bilan cheklanmagan holda:

- ilovaga administrator huquqlarini berish

- o‘rnatish manbai

- overlay faoliyatini amalga oshirish

- mobil OT va begona ilovalarda zararli dasturiy ta’minotning avtomatik harakatlari;

- zararli dasturiy ta’minotga xos xavfli yoki odatiy ruxsatlar (permissions) birikmalari mavjudligi;

- tizim sozlamalarini almashtirish

- mijozning TOR, proxy va «anonimayzerlar» orqali ishlashini aniqlash;

- proxy va VPN xizmatlarini ko‘rsatishga mo‘ljallangan tarmoq xizmatlarining ochiq portlarini aniqlash uchun butun IPv4 manzil makonini profillash natijalaridan foydalanish;

- «anonimayzerlar»ni aniqlash uchun domen nomlari va IP-manzillarni profillash natijalaridan foydalanish;

- qurilmadan olingan geolokatsiya bilan IP-manzil orqali aniqlangan geolokatsiya o‘rtasidagi nomuvofiqlikni aniqlash;

- xosting va kolokatsiya xizmatlari ko‘rsatuvchi kompaniyalarning buzib kirilgan ajratilgan serverlari yoki qurilmalaridan ulanishni aniqlash;

- internetdagi tarmoq qurilmalarini profillash bo‘yicha tashqi manbalardan foydalanish;

- avtomatlashtirilgan faoliyatni aniqlash hodisalaridan belgilash uchun foydalanish.

- qurilmalar va SIM-kartalar almashtirilganda bir foydalanuvchining ilova doirasidagi turli mobil qurilmalarini aniqlash;

- qonuniy foydalanuvchi o‘z mobil qurilmasini yangi modelga almashtirgan holatlarni aniqlash

- foydalanuvchi mobil qurilmasida (e)SIM-kartani almashtirgan holatlarni aniqlash.

- xulq-atvor ma’lumotlari asosida firibgar va qonuniy foydalanuvchi harakatlarini aniqlash:

- foydalanuvchining teginish va surish xususiyatlari, ilova interfeysi elementlari bilan aloqasi, matn terish tezligi, mobil qurilma sensorlari ma’lumotlari:

- foydalanuvchining tugmalarni bosish dinamikasini profillash va anomaliyalarni aniqlash;

- foydalanuvchi kursor harakati dinamikasini profillash va anomaliyalarni aniqlash;

- sensorlarni hisobga olgan holda foydalanuvchining mobil qurilma ekrani bilan o‘zaro ishlash xususiyatlarini profillash va anomaliyalarni aniqlash;

- foydalanuvchining veb va mobil ilovalar interfeysidagi odatiy harakatlari hamda xulq-atvor xususiyatlarini profillash va anomaliyalarni aniqlash;

- foydalanuvchi harakatlarining firibgar profiliga o‘xshashligini aniqlash.

- GPS ma’lumotlari va aloqa kanallari turlari haqidagi ma’lumotlar yordamida firibgarlikni aniqlash:

- SAT maydonlaridagi yuqori xavfli hodisalarni hisobga olgan holda geolokatsiyalarni profillash;

- yakuniy foydalanuvchi qurilmasida geolokatsiya almashtirilganini aniqlash.

- Buyurtmachi tanlagan boshqa qoidalar (bir nechta hisob qaydnomasi, firibgarlik tarmoq segmentlari va boshqalar) asosida foydalanuvchi va dasturiy ta’minotning zararli faoliyatini aniqlash:

- debugger yoqilgan mijoz sessiyalarini aniqlash va mijoz harakatlarini tahlil qilishda hisobga olish;

- Buyurtmachining boshqa tizimlariga, masalan, tranzaksion antifrod tizimiga qo‘shimcha xulosalar taqdim etish;

- Tashkilot tanlagan yoki sozlagan boshqa qoidalar (bir nechta hisob qaydnomasi, qurilmalar soni va xususiyatlari, firibgarlik tarmoq segmentlari va boshqalar) asosida zararli faoliyatni aniqlash;

- SAT Buyurtmachining masofaviy bank xizmatlarida mijoz sessiyasi yoki harakatini bloklash/to‘xtatish uchun real vaqt rejimida ma’lumot uzatishni ta’minlashi kerak, jumladan, shaxsiy kabinetga kirish, tranzaksiya bajarish, profilni o‘zgartirish kabi holatlar;

- mobil OT va brauzerlar haqidagi ma’lumotlarga asoslanib harakatning qonuniyligi to‘g‘risida qaror qabul qilish;

- SAT antidetect brauzerlarini aniqlashi kerak;

- root/jailbreak qilingan mobil qurilmalarni aniqlash;

- firibgar harakatlarini avtomatlashtirishda ishlatiladigan headless brauzerlarni aniqlash.

- SAT modullari ma’lumotlarini uzatish uchun HTTPS ulanishidan (TLS va SSL) foydalanish;

- mobil ilova tomonida SSL pinning imkoniyati taqdim etilishi kerak.

- Buyurtmachi ilovasidan foydalanilganda foydalanuvchi harakatlari haqidagi ma’lumotlarni qabul qilish va qayta ishlash quyi tizimiga uzatish;

- yig‘ilgan ma’lumotlarni yaxlitligini nazorat qilgan holda obfuskatsiyalangan ko‘rinishda uzatish;

- yig‘ilgan ma’lumotlarni foydalanuvchi va Buyurtmachi o‘rtasidagi ma’lumot uzatish kanallari orqali yuborishni qo‘llab-quvvatlash;

- veb-sensor kodini dinamik obfuskatsiyalash va uzatilayotgan ma’lumotlar obfuskatsiyasi parametrlarini o‘zgartirishni, shuningdek, obfuskatsiya chastotasini belgilash imkoniyatini qo‘llab-quvvatlash;

- avtonomlik, yaxlitlik va xavfsizlikni ta’minlash uchun veb-sensorni modullarsiz, monolit yetkazib berish (arxitektura) shakliga ega bo‘lish;

6.3 Ma’lumotlarni qayta ishlash va tahlil qilish quyi tizimiga talablar.

Quyi tizim quyidagilarni bajarishi kerak:

- ma’lumot yig‘ish quyi tizimidan ma’lumotlarni qabul qilish va ularning yaxlitligini tekshirish;

- SAT mijoz modulidan uzatilgan ma’lumotlar server qismigacha yetib borgunga qadar firibgar tomonidan almashtirilmaganini aniqlash uchun ularning yaxlitligini tekshirish;

- ma’lumot yig‘ish quyi tizimlaridan olinadigan ma’lumotlar asosida foydalanuvchi va uning qurilmalari profilini tuzish;

- Buyurtmachining har bir foydalanuvchisi sessiyalari bo‘yicha kanallararo ma’lumotlar korrelyatsiyasini amalga oshirish;

- Buyurtmachi uchun yakuniy foydalanuvchi qurilmasini veb va mobil kanallarda yagona va noyob tarzda identifikatsiya qilishni ta’minlash. Device fingerprinting bunday identifikator hisoblanmaydi, chunki u muayyan qurilma uchun noyob emas;

- ayni yechimdan foydalanuvchi Tashkilotlar o‘rtasida (ularning roziligi bilan), shu jumladan on-premise o‘rnatishda qurilmalarni birgalikda tasniflash uchun ma’lumot almashish va korrelyatsiya mexanizmini taqdim etish; bunday ma’lumotlarga qurilmaning yagona noyob identifikatori, IP-manzillar va ularning tasnifi, zararli dasturlar signaturalari, yuqori xavfli geolokatsiyalar va boshqalar kiradi;

- Buyurtmachi mijozining identifikatori, qurilma izi, IP-manzili, sessiya identifikatori va SAT yig‘ish tizimining boshqa parametrlari bo‘yicha tezkor qidiruvni amalga oshirish;

- Buyurtmachi xodimlariga har bir sessiya bo‘yicha firibgarlik faoliyatini aniqlash va bloklash qoidalari hamda xavf darajasini mustaqil sozlash imkonini berish, jumladan:

- qoidalarni faollashtirish/faolsizlantirish imkoniyati;

- «YOKI», «VA» hamda «EMAS» shartlari asosida muayyan hodisalarni qo‘shish orqali qoidalarni moslashuvchan tahrirlash imkoniyati;

- qoidadagi har bir hodisani qo‘shish yoki olib tashlash orqali mustaqil va moslashuvchan sozlash imkoniyati;

- «>», «<» yoki «=», «o‘z ichiga oladi» va «o‘z ichiga olmaydi» kabi shartlar asosida hodisaning ishga tushish darajasini o‘zgartirish imkoniyati;

- firibgarlikni aniqlash bo‘yicha yangi gipotezalarni sinash uchun haqiqiy ish ma’lumotlarida onlayn rejimda sinov hodisalarini yaratish imkoniyatini taqdim etish;

- samaradorlikni baholash va firibgarlikni aniqlash bo‘yicha yangi gipotezalarni tekshirish uchun tarixiy ma’lumotlarda qoidalarni sinash imkoniyatini taqdim etish;

- hodisalarni (hodisalar guruhini) shakllantirish uchun korrelyatsiya qoidalarida hodisalar majmuasini sozlash va ishlatish imkoniyatiga ega bo‘lish;

- qoidalarda foydalanuvchilar, IP-manzillar, qurilma identifikatorlari bo‘yicha maxsus ro‘yxatlar (masalan, bloklash, istisno, shubhali qurilmalar ro‘yxatlari va boshqalar) yaratish va ulardan foydalanish imkoniyatini qo‘llab-quvvatlash;

- tashqi ma’lumot manbalarining indikatorlari bilan boyitilish.

- aniqlangan alohida hodisalarni hamda foydalanuvchi qurilmasidagi brauzer sessiyalari bo‘yicha guruhlangan hodisalarni ko‘rish imkoniyatini amalga oshirish;

- mijoz masofaviy bank xizmati sessiyasida bo‘lgan paytda uyali tarmoq orqali faol kiruvchi/chiquvchi qo‘ng‘iroqni aniqlash;

- mijoz masofaviy bank xizmati sessiyasida bo‘lgan paytda tezkor xabar almashish xizmatlari orqali faol kiruvchi/chiquvchi qo‘ng‘iroqni aniqlash;

- tizim boshqa ishlab chiqaruvchilarning tashqi antifrod tizimlari bilan integratsiyalasha olishi kerak;

- mijozlarning hisob ma’lumotlaridan ruxsatsiz foydalanish holatlarini (masofaviy bank xizmatlariga yangi qurilmadan yoki firibgarlik qurilmasidan kirishni) aniqlash;

- aniqlangan har bir hodisaning quyidagi tafsilotlarini ko‘rish imkoniyatini amalga oshirish:

- hodisa vaqti;

- jiddiylik darajasi;

- aniqlangan hodisa turi;

- hodisa turiga qarab uning tafsilotlari

- asosiy obyektlar (qurilmalar, sessiyalar, geolokatsiyalar) bo‘yicha aloqalarni guruhlagan holda mijoz profilini ko‘rish uchun alohida vositani amalga oshirish

- Buyurtmachi sahifalariga kiritilgan inyeksiyalarni ko‘rish va toifalash imkoniyatini amalga oshirish;

- Buyurtmachi resurslarida foydalanuvchi sessiyalari davomida murojaat qilingani qayd etilgan domenlarni (masalan, zararli, shubhali va qonuniy) ko‘rish va toifalash;

- foydalanuvchilar faolligi va ular orasida aniqlangan hodisalar soni bo‘yicha statistikani chiqarish;

- SAT egasi tomonidan tizim hisob qaydnomalarini boshqarish, yangi rollar yaratish va rollar hamda hisob qaydnomalariga ko‘ra huquqlarni ajratish imkoniyatini ta’minlash;

- maxsus interfeysda ma’lumotlarni tahlil qilish imkoniyatini ta’minlash.

6.4 Buyurtmachi administratorlari va tahlilchilari uchun SAT veb-interfeysiga talablar

Quyidagi talablar bajarilishi kerak:

- SAT veb-interfeysi operator qurilmasiga qo‘shimcha dasturiy ta’minot (Java, ActiveX, brauzerning qo‘shimcha modullari) o‘rnatishni talab qilmasligi kerak.

- veb-interfeysda kirish huquqlari ajratilishi va parol siyosatiga qo‘shimcha ravishda quyidagi usullardan biri bilan kirish cheklanishi kerak:

- IP-manzillar diapazoni bo‘yicha kirishni cheklash;

- ikki omilli autentifikatsiya tizimi.

SAT veb-interfeysi quyidagilardan foydalanish imkonini berishi kerak:

- SAT statistikasi (davr bo‘yicha foydalanuvchi faolligi, hodisalar turlari va holatlari haqidagi umumlashtirilgan ma’lumotlar);

- olingan hodisalar haqidagi ma’lumotlar;

- hodisalar tafsilotlari;

- SAT foydalanuvchisining veb-interfeysi hodisalar bo‘yicha hisobotlar yaratish imkonini beruvchi hisobot xizmatidan foydalanish huquqini taqdim etishi kerak.

- SAT foydalanuvchisining veb-interfeysi va barcha ma’lumotnoma hujjatlari tizim buyruqlaridan tashqari to‘liq rus tilida bo‘lishi kerak.

6.5 SAT API dasturiy interfeysiga talablar

Quyidagi talablar bajarilishi kerak:

- API bilan o‘zaro aloqa chaqirilayotgan funksiyalarga kirish huquqlarini tekshirgan holda himoyalangan HTTPS protokoli orqali amalga oshiriladi;

- API dasturiy interfeysi JSON formatidan foydalanib tashqi tizimlarga aniqlangan hodisalar haqidagi ma’lumotlarga real vaqt rejimida kirish imkonini beradi;

- dasturiy interfeys orqali uzatiladigan ma’lumotlar tarkibiga quyidagilar kiradi:

- hodisaning noyob identifikatori;

- hodisa turi bo‘yicha tasnif;

- hodisa manbai (kanal, sessiya, qurilma, foydalanuvchi hisob qaydnomasi);

- hodisa vaqti;

- sessiyaning noyob identifikatori;

- foydalanuvchi nomi;

- foydalanuvchining brauzeri va qurilmasi haqidagi ma’lumot;

- hodisa sodir bo‘lgan URI;

- foydalanuvchining User-Agent ma’lumoti.

- umumiy xavf bahosi olinganda ishga tushgan qoidalar identifikatorlari va har bir qoida bo‘yicha xavf bahosini ham olish;

- aniqlangan hodisalar haqidagi ma’lumotlarni real vaqt rejimida ham, so‘rov asosida ham olish imkonini berish;

- aniqlangan hodisalarning bir qismini quyidagi parametrlar birikmasi bo‘yicha olish imkonini ta’minlash:

- vaqt oralig‘i;

- Buyurtmachi sessiyasining identifikatori bo‘yicha (imkon bo‘lsa);

- belgilangan hodisa turlari majmuasi bo‘yicha.

- xavfga asoslangan autentifikatsiya (RBA — risk-based authentication) texnologiyasini qo‘llab-quvvatlash, shu jumladan Buyurtmachi tizimlarida xavfga asoslangan autentifikatsiya bo‘yicha avtomatik xulosa taqdim etish. Xavfga asoslangan autentifikatsiya xulosasini shakllantirish vaqti 1000 ms dan oshmasligi kerak.

- tranzaksiya turidagi ma’lumotlarni quyidagilar bilan boyitish mexanizmini taqdim etish, shu jumladan, lekin ular bilan cheklanmagan holda:

- yuboruvchi va oluvchi kartalarining shaxssizlantirilgan identifikatori;

- summa;

- to‘lov terminali.

- aniqlangan hodisa haqidagi ma’lumotlar formati yagona bo‘lishi, shu bilan birga hodisaga xos qo‘shimcha ma’lumotlarni ko‘rsatishga ruxsat berishi kerak;

- tizimni o‘qitish va firibgarlikni aniqlash sifatini oshirish maqsadida aniqlangan hodisalar yuzasidan qayta aloqa berish imkoniyatini taqdim etish;

- ma’lumotlarni eksport/import qilishning standart sanoat protokollari va usullaridan foydalanish;

- aniqlangan hodisalarda uzatiladigan ma’lumotlarning maxfiyligini ta’minlash;

- hodisalarni pull, push va gibrid shaklda uzatishni ta’minlash;

- aloqalarni tahlil qilish va ulardan foydalanish bo‘yicha quyi tizimga talablar

- masofaviy bank xizmatlari tizimida bir qurilmadan bir nechta foydalanuvchi foydalanishini aniqlash;

- masofaviy bank xizmatlari foydalanuvchilari boshqa foydalanuvchilarning qurilma identifikatorlariga mos qurilmalar yordamida tizimga kirish holatlarini aniqlash imkoniyati;

- belgilangan foydalanuvchi/foydalanuvchilar bilan bir xil qurilmalardan masofaviy bank xizmatlariga kirishda foydalangan foydalanuvchilar identifikatorlarini (foydalanuvchi interfeysi yoki API so‘rovi orqali) qidirish va eksport qilish imkoniyati;

- masofaviy bank xizmatlari foydalanuvchilarining identifikatorlarini (login yoki boshqa identifikator) hodisa raqami, qurilmaning noyob identifikatori, IP-manzil kabi parametrlar bo‘yicha (foydalanuvchi interfeysi yoki API so‘rovi orqali) qidirish va eksport qilish imkoniyati;

- hodisalarni turi, raqamlari, IP-manzil, qurilmaning noyob identifikatori, foydalanuvchi logini yoki boshqa identifikatori, hodisa sanasi va vaqti kabi parametrlar bo‘yicha (foydalanuvchi interfeysi yoki API so‘rovi orqali) qidirish va eksport qilish imkoniyati;

- tizim Buyurtmachi bilan kelishilgan kunlik so‘rovlar sonining eng yuqori qiymatida ham so‘rovlarni onlayn rejimda qayta ishlashi kerak.

6.6 O‘zbekiston Respublikasi Markazlashtirilgan antifrod tizimi bilan axborot almashinuvi quyi tizimiga talablar

- SAT shubhali va firibgarlik hodisalari bo‘yicha sessiya ma’lumotlarining O‘zbekiston Respublikasi Markazlashtirilgan antifrod tizimiga uzatilishini ta’minlashi kerak.

7. Ishonchlilikka talablar

Quyidagi talablar bajarilishi kerak:

- bir nechta (kamida ikkita) maydonda nosozliklarga bardoshli sxema asosida ishlash va favqulodda vaziyatlarga bardoshli konfiguratsiyaga ega bo‘lish imkoniyati;

- SAT sessiya ma’lumotlarini qayta ishlashni zaxira maydonga o‘tkazish bo‘yicha avariyadan tiklanish (disaster recovery, DR) rejasini ta’minlashi kerak;

- asosiy maydon sozlamalari o‘zgarganda zaxira maydon ham yangilanishi kerak;

- asosiy maydon ishlamay qolganda zaxira maydonning to‘g‘ri ishlashi uchun yaratilgan qurilma va foydalanuvchi profillari zaxira maydonda avtomatik yangilanishi kerak.

- unumdorlikni oshirish talab etilganda mavjud o‘rnatmani qayta o‘rnatmasdan va arxitekturani sezilarli o‘zgartirmasdan kengaytirishni qo‘llab-quvvatlash;

- eng yuqori yuklama xavfga asoslangan autentifikatsiya xulosalarini olish uchun ishlatiladigan xabar almashish API unumdorligining pasayishiga olib kelmasligi kerak;

- ma’lumotlar qatlamini zaxiralash va tiklashning o‘z mustaqil mexanizmlariga ega bo‘lish;

- asosiy komponentlarni zaxiralashni ta’minlash;

- nosozliklarga bardoshlilikni nazorat qilish talablariga mos kelish:

- asosiy komponentlar holatini monitoring va nazorat qilishni ta’minlash;

- diskdagi bo‘sh joy, protsessor va xotira resurslari sarfi, qayta ishlanayotgan foydalanuvchi sessiyalari sonini nazorat qilish mexanizmlarini ta’minlash;

- kritik qiymatlar, hodisalar va ishlashdagi nosozliklar haqida SMTP protokoli orqali xabar berish.

- quyidagi ishonchlilik ko‘rsatkichlariga mos kelish:

- SATning odatiy ish rejimi – haftada 7 kun, sutkada 24 soat;

- frontend, backend va db serverlarning server qismi yillik mavjudligi kamida 99,95% bo‘lishi kerak

- veb-konsolaning yillik mavjudligi kamida 99,90% bo‘lishi kerak

- Buyurtmachi tizimlari bilan o‘zaro ishlashda aloqa uzilganda ma’lumotlarning yaxlitligi va to‘g‘riligini ta’minlash.

8. SAT xavfsizligiga talablar

Quyidagi talablar bajarilishi kerak:

- operatorlarning xizmat vazifalarini hisobga olgan holda sozlanadigan rollar modeli asosida kirish huquqlarini ajratishni qo‘llab-quvvatlash;

- SAT boshqaruv panelida operatorlar harakatlarini qayd etishni ta’minlash;

- boshqaruv veb-interfeysiga himoyalangan, shifrlangan ulanishni ta’minlash;

- unutilgan sessiyadan himoyalash – belgilangan vaqt o‘tgach yoki brauzer yopilganda veb-interfeys bilan faol bo‘lmagan ulanishni uzishni qo‘llab-quvvatlash;

- SATning barcha tugunlari o‘rtasida himoyalangan, shifrlangan ulanishni ta’minlash;

- operatsion tizim darajasida himoya mexanizmlarini (kirish huquqlarini cheklash, ishlatilmaydigan tarmoq xizmatlarini taqiqlash va boshqalar) ta’minlash;

- SAT ma’lumotlar bazasiga tarmoq orqali kirishni cheklashni ta’minlash.

9. Xodimlarni o‘qitishga talablar

Ijrochi Buyurtmachi talabiga binoan Buyurtmachining kamida 3 nafar mutaxassisini o‘qitishni ta’minlashi shart.

O‘quv dasturi quyidagilarni o‘z ichiga olishi kerak:

- O‘quv hujjatlarini taqdim etish;
- SAT tahlil vositalari va tahlilchi panelida ishlashni o‘rgatish;
- SATni administratsiya qilishni o‘rgatish.

10. Sifatga talablar

Ijrochi SATni joriy etishga oid barcha o‘rnatish va ishga tushirish-sozlash ishlarini bajarishi shart, jumladan konfiguratsiyalash, sinovdan o‘tkazish, Buyurtmachining ichki tizimlari (kamida
2 ta) bilan integratsiyalash, integratsiyaning to‘g‘riligini tekshirish, yo‘riqnomalar taqdim etish va tizimning ishlashini namoyish qilish.

Tizimning to‘g‘ri ishlashi qabul qilish-topshirish sinovlari mezonlari bo‘yicha tekshiriladi.

11. Yetkazib berish miqdori, tarkibi, joyi va muddati (davriyligi)ga talablar

Yechimni foydalanish huquqini beruvchi litsenziyalarni yetkazib berish muddati – shartnoma tuzilgan kundan boshlab 7 ish kunigacha.

12. Litsenziyalashga talablar

SAT Buyurtmachining masofaviy kanallaridagi yillik faol foydalanuvchilar soniga ko‘ra litsenziyalanishi va so‘rovlar, autentifikatsiyalar hamda faol integratsiyalar soni uchun qo‘shimcha to‘lov talab qilmasligi kerak.

Litsenziya to‘loviga mobil yoki veb-kanallarga, shuningdek, bankning ichki tizimlariga (kamida 2 ta) integratsiya qilish ishlari kiritilishi kerak.

Litsenziyalashda bir yil uchun 1 100 000 faol foydalanuvchi hisobga olinishi kerak.

13. Qo‘shimcha talablar

Ijrochi O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-sonli «Shaxsga doir ma’lumotlar to‘g‘risida»gi, 2003-yil 30-avgustdagi 530-II-sonli «Bank siri to‘g‘risida»gi qonunlariga hamda boshqa normativ-huquqiy hujjatlarga amal qilishi shart.

Kelishildi:

Z.X.Mamajonov 

A.R.Ibodov 

S.R.Mamasiddikov 

A.G.Samiyev 

A.F.Iskandarov 