“BIZNESNI RIVOJLANTIRISH BANKI ” ATB AKSIYADORLIK TIJORAT BANKI
АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК «БАНК РАЗВИТИЯ БИЗНЕСА»

TEXNIK TOPSHIRIQNOMA

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

«20» may 2026 y.
№ 380

“Biznesni rivojlanatirish banki” ATB ning axborot tizimlari, veb-servislari, tashqi perimetri va mobil ilovalarini xavfsizlik tekshiruvi (Penetration Testing)dan o‘tkazish xizmatlarini ko‘rsatish bo’yicha

Toshkenr-2026

1. UMUMIY QOIDALAR

1.1. Ushbu texnik topshiriq (TT) O‘zbekiston Respublikasi tijorat banklarining axborot xavfsizligi va kibexavfsizligiga bo‘lgan minimal talablar to‘g‘risidagi Nizom (18.08.2025 yildagi ro‘yxat raqami 3669) asosida, O‘zbekiston Respublikasi Markaziy banki Boshqaruvining 01.08.2025 yildagi 19/1-sonli Qarori bilan tasdiqlangan holda ishlab chiqilgan.

1.2. TT bank axborot tizimlari, mobil va veb-ilovalarida kompleks Penetration Testing va zaifliklarni tahlil qilishni o‘tkazishga qo‘yiladigan talablarni belgilaydi.

1.3. Ishlarni amalga oshirishning normativ asosi:

- Nizomning 20-bobi – “Zaifliklar va konfiguratsiyalarni boshqarish”;
- Nizomning 21-bobi – “Axborot tizimlari life cycle bosqichlarida axborot xavfsizligini ta’minlash”;
- Nizomning 23-bobi – “Axborot xavfsizligi talablarining bajarilishi ustidan nazorat”.

1.4. Ijrochi Penetration Testing sohasida xalqaro sertifikatlarga ega bo‘lishi shart (OSCP, CWEE, CEH, CISA, CAPT).

(Har bir yo‘nalish bo‘yicha sertifikatlangan mutaxassislar bo‘lishi zarur. Xodimlarning rasmiy ishga olinganligi shart.)

1.5. Barcha ishlar Nizomning 3-bobi talablariga muvofiq maxfiylik talablarini to‘liq qamrab olgan holda bajariladi.

2. MAQSAD VA VAZIFALAR

2.1. Ishlarni o‘tkazishdan ko‘zlangan maqsadlar:

- Bank axborot tizimlari, veb- va mobil ilovalaridagi zaifliklarni aniqlash;
- Tizimlarning tashqi va ichki tahdidlardan himoyalanish darajasini baholash;
- O‘zR Markaziy bankining 3669-son Nizomi talablariga muvofiqligini tekshirish;
- Darknetda va ixtisoslashgan ma’lumotlar bazalarida bank ma’lumotlarining sizib chiqishini qidirish;
- Mavjud axborot himoyasi vositalarining samaradorligini baholash;
- Aniqlangan zaifliklarni bartaraf etish bo‘yicha tavsiyalar ishlab chiqish.

3. ISHLAR TARKIBI VA MAZMUNI

3.1. Tashqi tarmoq perimetrini sinash

Maqsad: Bankning tashqi perimetrini ochiq Internet tarmog‘idan keladigan tahdid va kiber hujumlardan himoyalanish darajasini baholash.

Ishlar ro‘yxati:

- Ma’lumot to‘plash va razvedka (OSINT):
  - DNS-yozuvlar, subdomenlar, MX-yozuvlarni tahlil qilish;
  - Ochiq manbalardan ma’lumot to‘plash (WHOIS, Shodan, Censys);
  - Xodimlarning tarqalib ketgan hisob ma’lumotlarini qidirish;
  - Ochiq hujjatlar metadata-sini tahlil qilish.
- Xizmatlarni skanerlash va identifikatsiyalash:

- Barcha diapazondagi TCP/UDP portlarini skanerlash;
- Xizmatlar versiyalari va operatsion tizimlarni aniqlash;
- Yashirin xizmatlar va boshqaruv interfeyslarini topish.

– Zaifliklarni tahlil qilish:
  - Zaifliklarni avtomatlashtirilgan skanerlash (Nessus, OpenVAS);
  - Aniqlangan zaifliklarni qo‘lda tekshirish;
  - Topilgan dasturiy ta’minot versiyalari uchun ma’lum CVE-larni tekshirish.
– Zaifliklardan foydalanish:
  - Aniqlangan zaifliklardan foydalanishga urinishlar;
  - Ruxsatsiz kirish imkoniyatini tekshirish;
  - Muvaffaqiyatli hujumdan yetkazilishi mumkin bo‘lgan zararni baholash.
– Himoya vositalarini sinash:
  - WAF, IDS/IPS samaradorligini tekshirish;
  - Himoya vositalarini chetlab o‘tishga urinishlar;
  - Tarmoqlararo ekranlar sozlamalarining to‘g‘riligini baholash.

Foydalaniladigan vositalar: Nmap, Masscan, Nessus, Nuclei, Metasploit, Burp Suite Pro.

3.2. Veb-ilovalarni sinash

Maqsad: OWASP metodologiyasiga muvofiq bank veb-ilovalaridagi zaifliklarni aniqlash.

Ishlar ro‘yxati:

– Autentifikatsiya mexanizmlarini tahlil qilish:
  - Parol siyosati va hisob qaydnomalarini blokirovka qilishni tekshirish;
  - Parolni tiklash mexanizmlarini tekshirish;
  - Ko‘p omilli autentifikatsiya (MFA) amalga oshirilishini tekshirish;
  - Session Fixation, Session Hijacking hujumlaridan himoyani tahlil qilish.
– Avtorizatsiya mexanizmlarini tekshirish:
  - Vertikal imtiyozlarni oshirishni tekshirish (IDOR);
  - Gorizontal imtiyozlarni oshirishni tekshirish;
  - Rollar orasidagi kirish cheklovlarini sinash;
  - Biznes-jarayonlar mantiqini chetlab o‘tish nuqtai nazaridan tahlil qilish.
– Injection hujumlarini tekshirish:
  - SQL-injection (Union, Blind, Time-based, Error-based);
  - NoSQL-injection;
  - LDAP-injection;
  - OS Command Injection;
  - XML External Entity (XXE);
  - Server-Side Template Injection (SSTI).
– Saytlararo zaifliklar:
  - Reflected XSS, Stored XSS, DOM-based XSS;
  - Cross-Site Request Forgery (CSRF);

- Clickjacking.

– Biznes-logic zaifliklarini tekshirish:
  - Narx va tranzaksiya summalarini manipulyatsiya qilish;
  - Limitlar va cheklovlarni chetlab o‘tish;
  - Muhim operatsiyalarda Race Condition;
  - Promokodlar va bonuslarni manipulyatsiya qilish.
– Konfiguratsiyani tahlil qilish:
  - HTTP xavfsizlik sarlavhalarini tekshirish;
  - SSL/TLS sozlamalarini tahlil qilish;
  - Maxfiy ma’lumotlarning oshkor etilishini qidirish;
  - Nosozliklarni bartaraf etish interfeyslarini tekshirish.

Foydalaniladigan vositalar: Burp Suite Pro, OWASP ZAP, SQLMap, Nuclei, Nikto, Wapiti.

3.3. API-ni sinash

Maqsad: Bank ilovalarining REST/SOAP/GraphQL API xavfsizligini tahlil qilish.

Ishlar ro‘yxati:

– API hujjatlarini va endpoint-larni tahlil qilish:
  - Swagger/OpenAPI spetsifikatsiyalarini o‘rganish;
  - Yashirin va hujjatlashtirilmagan endpoint-larni aniqlash;
  - GraphQL Introspection-ni tahlil qilish.
– API autentifikatsiyasini sinash:
  - JWT, OAuth 2.0, API Keys mexanizmlarini tahlil qilish;
  - Token amalga oshirishdagi zaifliklarni tekshirish;
  - Tokenlarni yangilash mexanizmlarini tekshirish.
– API avtorizatsiyasini sinash:
  - Broken Object Level Authorization (BOLA);
  - Broken Function Level Authorization (BFLA);
  - Mass Assignment zaifliklar.
– Ma’lumotlarni qayta ishlashni sinash:
  - API parametrlari orqali injection;
  - Excessive Data Exposure;
  - Improper Assets Management.
– Rate Limiting-ni tekshirish:
  - So‘rovlar soniga oid cheklovlarni tekshirish;
  - DDoS hujumlariga chidamliligini sinovdan o‘tkazish.

Foydalaniladigan vositalar: Postman, Burp Suite, GraphQL Voyager, Insomnia, maxsus skriptlar.

3.4. Mobil ilovalarni xavfsizlik tekshiruvidan o‘tkazish

Maqsad: OWASP MASTG metodologiyasiga muvofiq bank mobil ilovalarining iOS va Android uchun xavfsizligini tahlil qilish.

Ishlar ro‘yxati:

- Statik tahlil (SAST):
  - Manba kodini dekompilatsiya qilish va tahlil qilish;
  - Ishlatiladigan kriptografik algoritmlarni tahlil qilish;
  - Kodni obfuskatsiyalashni tekshirish;
  - Ilova ruxsatlarini tahlil qilish.
- Dinamik tahlil (DAST):
  - Ilovaning tarmoq trafigini tahlil qilish;
  - Certificate Pinning-ni tekshirish;
  - Jailbreak/Root Detection bypass-ni sinab ko‘rish;
  - Ma’lumotlarni saqlash joyini tahlil qilish;
  - Jarayonlararo o‘zaro ta’sirni (IPC) tekshirish.
- Biznes-logicni tekshirish:
  - Tranzaksiyalarni manipulyatsiya qilish;
  - Mijoz tekshiruvlarini chetlab o‘tish;
  - Oflayn funksionallikni tekshirish.
- Ma’lumotlarni himoya qilishni tahlil qilish:
  - Tinch holatdagi ma’lumotlar shifrlashini tekshirish;
  - Biometrik ma’lumotlar bilan ishlashni tahlil qilish;
  - Jurnallar va kesh orqali sizib chiqishni tekshirish.

Foydalaniladigan vositalar: MobSF, Frida, Objection, Jadx, Hopper, Charles Proxy, Burp Suite.

3.5. Ijtimoiy muhandislik

Maqsad: Bank xodimlarining axborot xavfsizligi sohasidagi xabardorligini baholash.

Ishlar ro‘yxati:

- Fishing kampaniyalari:
  - Fishing stsenariylarini ishlab chiqish;
  - Fishing sahifalarini yaratish (korporativ resurslarning klonlari);
  - Kelishilgan xodimlar ro‘yxatiga fishing xatlarini jo‘natish;
- Vishing:
  - Telefon hujum stsenariylarini ishlab chiqish;
  - Xodimlarga qo‘ng‘iroq qilish;
  - Maxfiy ma’lumotlarning oshkor etilishini baholash.

Natija: Xodimlarni o‘qitish bo‘yicha tavsiyalar bilan birga statistik hisobot tayyorlash.

3.6. Manba kodini statik tahlil qilish (SAST)

Maqsad: Bank ilovaları manba kodidagi zaifliklarni aniqlash.

Ishlar ro‘yxati:

- Avtomatlashtirilgan tahlil:
  - SAST vositalaridan foydalangan holda kodni skanerlash;
  - Ma'lum zaifliklar bo‘yicha bog‘liqliklarni tahlil qilish (SCA);

- Xavfsiz dasturlash standartlariga muvofiqligini tekshirish.

– Kodni qo‘lda tahlil qilish:
  - Muhim modullarni tahlil qilish (autentifikatsiya, to‘lovlar);
  - Kriptografik amalga oshirishlarni tekshirish;
  - Biznes-logic dagi mantiqiy xatolarni qidirish;
  - Foydalanuvchi kiritmasini qayta ishlashni tahlil qilish.
– Aniqlanadigan zaifliklar turlari:
  - SQL/NoSQL injection;
  - Hardcoded hisob ma’lumotlari va sirlar;
  - Xavfsiz bo‘lmagan deserialization;
  - Path Traversal, SSRF;
  - Kriptografiya xatolari.

Foydalaniladigan vositalar: SonarQube, Checkmarx, Semgrep, Bandit, Dependency-Check.

3.7. Darknet monitoringi va ma’lumotlarni sizib chiqishlarni tahlil qilish

Maqsad: Darknetda va ixtisoslashgan bazalarda bank ma’lumotlarining tarqalib ketishini qidirish.

Ishlar ro‘yxati:

– Hisob ma’lumotlari sizib chiqishini qidirish:
  - Sizib chiqish bazalarini monitoring qilish (Have I Been Pwned, DeHashed, LeakCheck);
  - Sizib chiqishlarda korporativ email-manzillarni qidirish;
  - Parollarni xavfsizlik siyosatlariga muvofiqligini tahlil qilish.
– Darknet resurslarini monitoring qilish:
  - Darknet forumlarida bank eslatmalarini qidirish;
  - Ma’lumotlar sotilishi bo‘yicha marketpleys-larni monitoring qilish;
  - Telegram-kanallar va chatlarni tahlil qilish.
– Hujjatlar sizib chiqishini qidirish:
  - Bank ichki hujjatlarini ochiq kirish manbalarida qidirish;
  - GitHub/GitLab-da kod sizib chiqishlarini tahlil qilish;
  - Pastebin va shunga o‘xshash resurslarni monitoring qilish.

Natija: Murosaga tushgan hisob qaydnomalari ro‘yxati va munosib choralar bo‘yicha tavsiyalar.

3.8. Konfiguratsiyalarni audit qilish (ixtiyoriy)

Maqsad: Tizimlar konfiguratsiyalarining xavfsizlik bo‘yicha eng yaxshi amaliyotlarga muvofiqligini tekshirish.

Ishlar ro‘yxati:

– Server konfiguratsiyasini tahlil qilish:
  - Operatsion tizimlar sozlamalarini tekshirish;
  - Veb-serverlar konfiguratsiyasini audit qilish (Apache, Nginx, IIS);
  - Ma’lumotlar bazalari konfiguratsiyasini tekshirish.
– Tarmoq qurilmalarini tahlil qilish:

    - Tarmoqlararo ekranlar sozlamalarini audit qilish;
    - ACL va marshrutlash qoidalarini tekshirish;
    - VPN sozlamalarini tahlil qilish.
- Bulutli infratuzilmani tekshirish (mavjud bo'lgan hollarda):
    - IAM siyosatlarini audit qilish;
    - S3/Blob Storage sozlamalarini tekshirish;
    - Security groups va tarmoq ACL-larini tahlil qilish.

4. TEKSHIRUV OBYEKTLARI

4.1. Veb-ilovalar:

- Yuridik shaxslar uchun internet-banking;
- Bankning korporativ veb-sayti;
- Boshqaruv administrator panellari;
- Veb-ilovalarning API-lari.

4.2. Mobil ilovalar:

- iOS uchun mobil ilova;
- Android uchun mobil ilova;
- Mobil ilovalarning API-lari.

4.3. Tarmoq infratuzilmasi:

- Tashqi tarmoq perimetri;
- Ochiq DNS-serverlar;
- Pochta serverlari;
- VPN-shluzy.

5. METODOLOGIYA VA STANDARTLAR

Testlash quyidagi metodologiyalardan foydalangan holda amalga oshiriladi:

- OWASP Testing Guide v4.2 - veb-ilovalar uchun;
- OWASP Mobile Application Security Testing Guide (MASTG) - mobil ilovalar uchun;
- OWASP API Security Top 10 - API uchun;
- NIST SP 800-115 - penetratsion testlash metodologiyasi;
- PTES (Penetration Testing Execution Standard);
- MITRE ATT&CK Framework - hujum taktikalari va texnikalari matritsasi;
- CVSS v3.1 - zaifliklarni tasniflash uchun.

5.1. Testlash usuli:

- Black Box: tizim haqida oldindan ma’lumot berilmagan holda sinash;

6. HISOBOTLARGA QO‘YILADIGAN TALABLAR

6.1. Oraliq hisobotlar:

- Kritik zaifliklar haqida xabarnoma - aniqlanganidan keyin 24 soat ichida;
- Ishlar borishi bo'yicha haftalik holat hisobotlari.

6.2. Yakuniy hisobot quyidagilarni o‘z ichiga olishi kerak:

- Executive Summary - rahbariyat uchun qisqacha xulosa;
- Metodologiya va foydalanilgan vositalar tavsifi;
- Har bir zaiflikning batafsil tavsifi:
  - Nomi va CVSS v3.1 bo'yicha tasnifi;
  - Zarar ko'rgan tizimlar/komponentlar;
  - Qayta ishlab chiqarish uchun bosqichma-bosqich ko‘rsatmalar (PoC);
  - Skrinshotlar va dalillar bazasi;
  - Biznesga potentsial ta’siri;
  - Prioritetlar bilan bartaraf etish bo‘yicha tavsiyalar.
- O‘zR Markaziy bankining 3669-son Nizomi talablariga muvofiqlik matritsasi;
- Zaifliklarni bartaraf etish yo‘l xaritasi;
- Ilovalar: jurnallar, demplar, texnik tafsilotlar.

6.3. Hisobot formati:

- Asosiy hisobot - PDF;
- Ilovalar - texnik materiallar bilan ZIP-arxiv;
- Rahbariyat uchun taqdimot - PPTX, 10-15 slayd.

7. IJROCHIGA QO‘YILADIGAN TALABLAR

7.1. Malaka talablari:

– Moliyaviy tashkilotlar uchun pentestlash tajribasi kamida 2 yil (soni ko‘rsatiladi);
– Bank va fintech yo‘nalishida kamida 5 ta bajarilgan loyihalar portfeli taqdim etiladi.

7.2. Maxfiylik talablari:

- Ishlarni boshlashdan oldin maxfiylik to‘g‘risida bitim (NDA) imzolash;
- Hisobotlarni uzatish uchun himoyalangan aloqa kanallaridan foydalanish;
- Barcha ish materiallarini shifrlash;

8. BAJARISH MUDDATLARI

	Ishlar bosqichi	**Muddat**
1	Tayyorlov bosqichi, kelishish	10 kun
2	Tashqi perimetrni sinash	10 kun
3	Veb-ilovalarni sinash	10 kun
4	API-ni sinash	10 kun
5	Mobil ilovalarni sinash	10 kun
6	Ijtimoiy muhandislik	10 kun

7	Manba kodini tahlil qilish (SAST)	10 kun
8	Hisobotlarni tayyorlash	10 kun
	JAMI	80 kun

9. KAFOLATLAR VA JAVOBGARLIK

9.1. Ijrochi ushbu TT ga muvofiq ishlarni sifatli bajarishni kafolatlaydi.

9.2. Kritik zaifliklar aniqlanganda (CVSS >= 9.0) Ijrochi Buyurtmachini 24 soat ichida xabardor qilishi shart.

9.3. Ijrochi olingan ma'lumotlarning saqlanishi uchun to‘liq javobgarlikni zimmasiga oladi.

9.4. Ijrochi hisobotlarni topshirgandan keyin 30 kun davomida konsultatsion yordam berishni kafolatlaydi.

9.5. Ijrochi aniqlangan zaifliklar to‘g‘risidagi ma’lumotni uchinchi shaxslarga oshkor qilmaslikka majburiyat oladi.

10. NORMATIV HAVOLALAR

- O‘zbekiston Respublikasi tijorat banklarining axborot xavfsizligi va kibexavfsizligiga bo‘lgan minimal talablar to‘g‘risidagi Nizom (18.08.2025 yildagi ro'yxat raqami 3669);
- O‘zbekiston Respublikasining “O‘zbekiston Respublikasi Markaziy banki to‘g‘risida”gi Qonuni;
- O‘zbekiston Respublikasining “Axborotlashtirish to‘g‘risida”gi Qonuni;
- O‘zbekiston Respublikasining “Kibexavfsizlik to‘g‘risida”gi Qonuni;
- ISO/IEC 27001:2022 - Axborot xavfsizligi menejment tizimlari;
- PCI DSS - to‘lov kartalari sanoatining ma’lumotlar xavfsizligi standarti.

11. ILOVALAR

- 1-ilova: Sinash obyektlari ro‘yxati (IP-manzillar, domenlar, ilovalar);
- 2-ilova: Mas’ul shaxslarning aloqa ma’lumotlari;
- 3-ilova: Sinov hisob qaydnomalari ro‘yxati;
- 4-ilova: Ishlarni topshirish-qabul qilish dalolatnomasi shakli;
- 5-ilova: Maxfiylik to‘g‘risida bitim (NDA).

kelishuvchilar: B.Shamsiev