

**SCIENCE**  
**PROBLEMS.UZ**

ISSN 2181-1342

Actual problems of social and humanitarian sciences  
Актуальные проблемы социальных и гуманитарных наук

**Ijtimoiy-gumanitar  
fanlarning dolzarb  
muammolari**

3-son (6-jild)

**2026**

**SCIENCEPROBLEMS.UZ**

**IJTIMOIIY-GUMANITAR FANLARNING  
DOLZARB MUAMMOLARI**

*№ 3 (6) – 2026*

**АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОЦИАЛЬНО-  
ГУМАНИТАРНЫХ НАУК**

**ACTUAL PROBLEMS OF HUMANITIES AND SOCIAL SCIENCES**

**TOSHKENT-2026**

## **BOSH MUHARRIR:**

Isanova Feruza Tulqinovna

## **TAHRIR HAY'ATI:**

### *07.00.00- TARIX FANLARI:*

Yuldashev Anvar Ergashevich – tarix fanlari doktori, siyosiy fanlar nomzodi, professor;

Mavlanov Uktam Maxmasabirovich – tarix fanlari doktori, professor;

Xazratkulov Abror – tarix fanlari doktori, dotsent;

Tursunov Ravshan Normuratovich – tarix fanlari doktori;

Xolikulov Axmadjon Boymahammatovich – tarix fanlari doktori;

Gabrielyan Sofya Ivanovna – tarix fanlari doktori, dotsent;

Saidov Sarvar Atabullo o'g'li – katta ilmiy xodim, Imom Termiziy xalqaro ilmiy-tadqiqot markazi, ilmiy tadqiqotlar bo'limi.

### *08.00.00- IQTISODIYOT FANLARI:*

Karlibayeva Raya Xojabayevna – iqtisodiyot fanlari doktori, professor;

Nasirxodjayeva Dilafruz Sabitxanovna – iqtisodiyot fanlari doktori, professor;

Ostonokulov Azamat Abdukarimovich – iqtisodiyot fanlari doktori, professor;

Arabov Nurali Uralovich – iqtisodiyot fanlari doktori, professor;

Xudoyqulov Sadirdin Karimovich – iqtisodiyot fanlari doktori, dotsent;

Azizov Sherzod O'ktamovich – iqtisodiyot fanlari doktori, dotsent;

Xojayev Azizxon Saidaloxonovich – iqtisodiyot fanlari doktori, dotsent

Xolov Aktam Xatamovich – iqtisodiyot fanlari bo'yicha falsafa doktori (PhD), dotsent;

Shadiyeva Dildora Xamidovna – iqtisodiyot fanlari bo'yicha falsafa doktori (PhD), dotsent v.b.;

Shakarov Qulmat Ashirovich – iqtisodiyot fanlari nomzodi, dotsent.;

Jabborova Charos Aminovna - iqtisodiyot fanlari bo'yicha falsafa doktori (PhD).

### *09.00.00- FALSAFA FANLARI:*

Hakimov Nazar Hakimovich – falsafa fanlari doktori, professor;

Yaxshilikov Jo'raboy – falsafa fanlari doktori, professor;

G'aybullayev Otabek Muhammadiyevich – falsafa fanlari doktori, professor;

Saidova Kamola Uskanbayevna – falsafa fanlari doktori;

Hoshimxonov Mo'min – falsafa fanlari doktori, dotsent;

O'roqova Oysuluv Jamoliddinovna – falsafa fanlari doktori, dotsent;

Nosirxodjayeva Gulnora Abdulkaxxarovna – falsafa fanlari nomzodi, dotsent;

Turdiyev Bexruz Sobirovich – falsafa fanlari doktori (DSc), Professor.

### *10.00.00- FILOLOGIYA FANLARI:*

Axmedov Oybek Saporbayevich – filologiya fanlari doktori, professor;

Ko'chimov Shuxrat Norqizilovich – filologiya fanlari doktori, dotsent;

Hasanov Shavkat Ahadovich – filologiya fanlari doktori, professor;

Baxronova Dilrabo Keldiyorovna – filologiya fanlari doktori, professor;

Mirsanov G'aybullo Qulmurodovich – filologiya fanlari doktori, professor;

Salaxutdinova Musharraf Isamutdinovna – filologiya fanlari nomzodi, dotsent;

Kuchkarov Raxman Urmanovich – filologiya fanlari nomzodi, dotsent v/b;

Yunusov Mansur Abdullayevich – filologiya fanlari nomzodi;

Saidov Ulugbek Aripovich – filologiya fanlari nomzodi, dotsent;

Qodirova Muqaddas Tog'ayevna - filologiya fanlari nomzodi, dotsent.

### *12.00.00- YURIDIK FANLAR:*

Axmedshayeva Mavlyuda Axatovna – yuridik fanlar doktori, professor;

Muxitdinova Firyuza Abdurashidovna – yuridik fanlar doktori, professor;

Esanova Zamira Normurotovna – yuridik fanlar doktori, professor, O'zbekiston Respublikasida xizmat ko'rsatgan yurist;

Hamroqulov Bahodir Mamasharifovich – yuridik fanlar doktori, professor v.b.,;

Zulfiqorov Sherzod Xurramovich – yuridik fanlar doktori, professor;

Xayitov Xushvaqt Saparbayevich – yuridik fanlar doktori, professor;

Asadov Shavkat G'aybullayevich – yuridik fanlar doktori, dotsent;

Ergashev Ikrom Abdurasulovich – yuridik fanlari doktori, professor;

Utemuratov Maxmut Ajimuratovich – yuridik fanlar nomzodi, professor;

Saydullayev Shaxzod Alixanovich – yuridik fanlar nomzodi, professor;

Hakimov Komil Baxtiyarovich – yuridik fanlar doktori, dotsent;

Yusupov Sardorbek Baxodirovich – yuridik fanlar doktori, professor;

Amirov Zafar Aktamovich – yuridik fanlar doktori (PhD);

Jo'rayev Sherzod Yuldashevich – yuridik fanlar nomzodi, dotsent;

Babadjanov Atabek Davronbekovich – yuridik fanlar nomzodi, professor;

Normatov Bekzod Akrom o'g'li — yuridik fanlar bo'yicha falsafa doktori;

Rahmatov Elyor Jumaboyevich — yuridik fanlar nomzodi;

### *13.00.00- PEDAGOGIKA FANLARI:*

Xashimova Dildarxon Urinboyevna – pedagogika fanlari doktori, professor;

Ibragimova Gulnora Xavazmatovna – pedagogika fanlari doktori, professor;

Zakirova Feruza Maxmudovna – pedagogika fanlari doktori;

Kayumova Nasiba Ashurovna – pedagogika fanlari doktori, professor;

Taylanova Shoxida Zayniyevna – pedagogika fanlari

doktori, dotsent;

Jumaniyozova Muhayyo Tojiyevna – pedagogika fanlari doktori, dotsent;

Ibraximov Sanjar Urunbayevich – pedagogika fanlari doktori;

Javliyeva Shaxnoza Baxodirovna – pedagogika fanlari bo'yicha falsafa doktori (PhD);

Bobomurotova Latofat Elmurodovna — pedagogika fanlari bo'yicha falsafa doktori (PhD).

### *19.00.00- PSIXOLOGIYA FANLARI:*

Karimova Vasila Mamanosirovna – psixologiya fanlari doktori, professor, Nizomiy nomidagi Toshkent davlat pedagogika universiteti;

Hayitov Oybek Eshboyevich – Jismoniy tarbiya va sport bo'yicha mutaxassislarni qayta tayyorlash va malakasini oshirish instituti, psixologiya fanlari doktori, professor

Umarova Navbahor Shokirovna– psixologiya fanlari doktori, dotsent, Nizomiy nomidagi Toshkent davlat pedagogika universiteti, Amaliy psixologiyasi kafedrasini mudiri;

Atabayeva Nargis Batirovna – psixologiya fanlari doktori, dotsent;

Shamshetova Anjim Karamaddinovna – psixologiya fanlari doktori, dotsent;

Qodirov Obid Safarovich – psixologiya fanlari doktori (PhD).

### *22.00.00- SOTSILOGIYA FANLARI:*

Latipova Nodira Muxtarjanovna – sotsiologiya fanlari doktori, professor, O'zbekiston milliy universiteti kafedra mudiri;

Seitov Azamat Po'latovich – sotsiologiya fanlari doktori, professor, O'zbekiston milliy universiteti;

Sodiqova Shohida Marxaboyevna – sotsiologiya fanlari doktori, professor, O'zbekiston xalqaro islom akademiyasi.

### *23.00.00- SIYOSIY FANLAR*

Nazarov Nasriddin Ataqulovich –siyosiy fanlar doktori, falsafa fanlari doktori, professor, Toshkent arxitektura qurilish instituti;

Bo'tayev Usmonjon Xayrullayevich –siyosiy fanlar doktori, dotsent, O'zbekiston milliy universiteti kafedra mudiri.

---

## **OAK Ro'yxati**

Mazkur jurnal Vazirlar Mahkamasi huzuridagi Oliy attestatsiya komissiyasi Rayosatining 2022-yil 30-noyabrdagi 327/5-son qarori bilan tarix, iqtisodiyot, falsafa, filologiya, yuridik va pedagogika fanlari bo'yicha ilmiy darajalar yuzasidan dissertatsiyalar asosiy natijalarini chop etish tavsiya etilgan ilmiy nashrlar ro'yxatiga kiritilgan.

---

**“Ijtimoiy-gumanitar fanlarning dolzarb muammolari”** elektron jurnali 2020-yil 6-avgust kuni 1368-sonli guvohnoma bilan davlat ro'yxatiga olingan.

**Muassis:** “SCIENCEPROBLEMS TEAM” mas'uliyati cheklangan jamiyati

### **Tahririyat manzili:**

100070. Toshkent shahri, Yakkasaroy tumani, Kichik Beshyog'och ko'chasi, 70/10-uy. Elektron manzil: [scienceproblems.uz@gmail.com](mailto:scienceproblems.uz@gmail.com)

### **Bog'lanish uchun telefon:**

(99) 602-09-84 (telegram).

## MUNDARIJA

### 07.00.00 – TARIX FANLARI

<i>Yusupov Shakir Xaitbayevich</i> AMIR TEMUR VA TEMURIYLAR DAVRIDA XORAZM SHAHARSOZLIK MADANIYATI TARAQQIYOTINING NATIJALARI .....	11-18
<i>Saparbaev Bunyod Khurrambek o'gli</i> THE ART OF NEGOTIATION: KHIVA AND RUSSIA ENGAGEMENT UNDER MUHAMMAD RAHIMKHAN I (1806–1825) .....	19-28
<i>Tursunova Gavhar Begmurodovna</i> ROSSIYA IMPERIYASINING SIRDARYO VILOYATIGA AHOLINI KO'CHIRISHDA MAHALLIY AHOLINING QARSHILIK HARAKATLARI (1890–1916-YILLAR) .....	29-32
<i>Polvonov Kozimbek Naimovich, Baratov Otabek Aripovich</i> SHAHARLAR DEMOGRAFIYASI VA KLASSIFIKATSIYASIDAGI O'ZGARISHLAR (QASHQADARYO VILOYATI MISOLIDA) .....	33-40
<i>Sagatova Ziёдахон Бахтияровна</i> МИГРАЦИОННЫЕ ПРОЦЕССЫ МЕЖДУ УЗБЕКИСТАНОМ И ТУРЦИЕЙ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ .....	41-45
<i>Saidboboyeva Gulzora Nematjonovna</i> STATISTIK NASHRLAR VA ADABIYOTLARDA TURKISTONNI ELEKTRLASHTIRISH MASALASI (XX ASRNING 20–50-YILLARI) .....	46-51
<i>Shamshidinov Baxriddin Sharobiddin o'g'li</i> FARG'ONA VODIYSI AHOLISINING ETNIK TARKIBI, ETNOSLARNING JOYLASHUVI VA ETNODEMOGRAFIK XUSUSIYATLARI (XIX ASR — XXI ASR BOSHLARI) .....	52-56

### 08.00.00 – IQTISODIYOT FANLARI

<i>Xudayberganov Dilshod Tuxtabayevich, Achilova Firuza Kurbanovna</i> MINTAQA IQTISODIYOTIDA XIZMATLAR SOHASINI SAMARALI RIVOJLANTIRISH YO'NALISHLARI .....	57-67
<i>Sultonova Дина Файзрахмановна</i> НАУЧНАЯ МЕТОДОЛОГИЯ ИНСТИТУЦИОНАЛЬНОГО МЕХАНИЗМА В ЭКОНОМИКЕ ОТРАСЛИ КОНЕВОДСТВА .....	68-72
<i>Xushvaqtov Jasur Shuhrat o'g'li</i> KO'CHMAS MULKNI HAYOTIY SIKL YONDASHUVI ASOSIDA OMMAVIY BAHOLASH METODOLOGIYASINI TAKOMILLASHTIRISH .....	73-82
<i>Jabbarov Nurbek Atanazarovich</i> O'ZBEKISTON SANOATIGA ENERGIYA RESURSLARINING TA'SIRINI BAHOLASHNING NAZARIY ASOSLARI .....	83-88

### 09.00.00 – FALSAFA FANLARI

<i>Zaripova Hulkar Toxir qizi</i> O'ZBEKISTONDAGI TARIXIY-MADANIY JARAYONLARDAGI MARGINAL QATLAMLARNING O'RNI .....	89-95
---	-------

<i>Abdullayeva Saodat Nurillo qizi</i> PAZANDACHILIK MADANIYATI VA SALOMATLIK FALSAFASI: VOZEHNING “KONI LAZZAT XONI NE’MAT” ASARIDA TAOMLARNING TIZIMLASHTIRILISHI .....	96-99
<i>Rajabov Behruz Baxshillayevich</i> TINCHLIK VA HAMKORLIKNING FALSAFIY MOHIYATI HAMDA ZAMONAVIY JAMIYAT TARAQQIYOTIDAGI O’RNI.....	100-104
<i>Artiqova Adolat Ataboyevna</i> MAHMUD AZ-ZAMAXSHARIYNING “AL-KASHSHAF” ASARI VA UNING TARIXIY AHAMIYATI .....	105-109
<i>Umarova Feruza</i> MAFKURAVIY TAHDIDLARGA QARSHI KURASHDA DIN VA DAVLAT MUNOSABATLARI TAHLILI .....	110-116
<i>Djalalova Nigora Xusanovna</i> IJTIMOIY-MADANIY TEXNOLOGIYALARNI O’RGANISHDA RAQAMLI ONG KONSEPSIYASI .....	117-120
<i>Ходжиметов Шахрух Русланбекович</i> ЭМИГРАЦИОННЫЕ И ИММИГРАЦИОННЫЕ ПРОЦЕССЫ ВЛИЯНИЕ НА СТАБИЛЬНОСТЬ ОБЩЕСТВА .....	121-124
<i>Islamova Gulzamon Madiyevna</i> JADIDLAR DAVRIDA TA’LIM TIZIMIDAGI ISLOHOTLARNING FALSAFIY ASOSLARI .....	125-130
<i>Uraqov Nodirbek Boboqulovich</i> HECI KONSEPSIYASI VA MAHDUMI A’ZAM MEROSI: BAG’RIKENGLIK, AKSIOLOGIK MUSHTARAKLIK, METODOLOGIK TAFOVUT, UMUMIY NUQTALAR VA FARQLAR HAMDA AGRAR TA’LIMDA INSONPARVARLIK G’OYALARINI INTEGRATSIYA QILISH MASALASI.....	131-136
<b>10.00.00 – FILOLOGIYA FANLARI</b>	
<i>Baydjanova Iroda Abdullayevna</i> TARJIMADA HAZIL-MUTOYIBA KONSEPTINING SAQLANISHI MUAMMOLARI: “SHUM BOLA” ASARINING O’ZBEK, INGLIZ VA RUS TILLARIDAGI TARJIMALARI MISOLIDA .....	137-143
<i>Imomiddinova Nargiza</i> ASL XITUYCHA HARBIY TERMINLARNING SHAKLLANISHI VA RIVOJLANISHI .....	144-154
<i>Sobirov Anvar Kuvandikovich</i> JONLI SO’ZLASHUV NUTQIDA SO’Z TARTIBINING LINGVOPOETIK VA LINGVOPRAGMATIK XUSUSIYATLARI .....	155-159
<i>Азизова Насиба Бахритдиновна</i> ЯЗЫКОВАЯ ЛИЧНОСТЬ КАК КУЛЬТУРНЫЙ КОНЦЕПТ: РЕКОНСТРУКЦИЯ ИДЕЙ АЛИШЕРА НАВАИ И ИХ РЕЛЕВАНТНОСТЬ ДЛЯ СОВРЕМЕННОЙ ЛИНГВОКУЛЬТУРОЛОГИИ.....	160-168
<i>Ishankulova Diyora Allovidinovna</i> UMAR XAYYOM SHE’RIYATINING G’OYAVIY-MAZMUNIIY MOHIYATI VA ULARNING TARJIMADAGI TALQINI .....	169-174

<i>Olimjon Jalilov Muxidinovich</i> INGLIZ VA O'ZBEK EPOSLARIDA LINGVISTIK MODELLARNING QIYOSIY XUSUSIYATLARI .....	175-178
<i>Achilova Zuxra Qurbonovna</i> "MALLA SAVDOGAR" DOSTONI VARIANTLARIDA BAXSHIYONA JANG POLOTNOSI VA PEYZAJ ESKIZLARI .....	179-184
<i>Orazgalieva Ayjamal Marat qızı</i> SYNONYMIC AND PRAGMATIC VERBALISATION OF CHILD/BALA IN ENGLISH AND KARAKALPAK LEXICOGRAPHY .....	185-192
<i>Babayeva Irada Sabirovna</i> LINGUOCULTUROLOGICAL APPROACH TO THE STUDY OF EMPATHIC COMMUNICATION .....	193-198
<i>Toʻshtemirova Farangiz Shuxratovna</i> РАЗВИТИЕ СЛОВАРНОГО СОСТАВА СОВРЕМЕННОГО РУССКОГО ЯЗЫКА И РОЛЬ СЛОВООБРАЗОВАНИЯ В ЕГО ОБОГАЩЕНИИ .....	199-202

## **12.00.00 - YURIDIK FANLAR**

<i>Utemuratova Sapargul Shamshetovna</i> EKOLOGIYA SOHASIDAGI JINOYATLARDA MAXSUS SUBYEKT TUSHUNCHASI VA MANSABDOR SHAXSLARNING JINOIY JAVOBGARLIGI .....	203-207
<i>Qilichev Xayrulla Mamatovich</i> FUQAROLARNING O'ZINI O'ZI BOSHQARISH ORGANLARINING DAVLAT XUSUSIY SHERIKLIK BITIMIDA ISHTIROK ETISHINING O'ZIGA XOS JIHATLARI .....	208-217
<i>Burhanova Shuyrin Jamshetovna</i> ГОСУДАРСТВЕННАЯ ПРАВОВАЯ ПОЛИТИКА И НОРМОТВОРЧЕСТВО: ВЗАИМОСВЯЗЬ И ОСОБЕННОСТИ РАЗВИТИЯ .....	218-223
<i>Akayeva Marapat Abduhalikovna</i> GENDER TENGLIGINI TA'MINLASHDA HUQUQIY SIYOSAT: O'ZBEKISTON TAJRIBASINING TAHLILI.....	224-232
<i>Chuboyeva Ozodaxon Quvonbekovna</i> XOTIN-QIZLARNING JAMIYAT IJTIMOIIY-SIYOSIY HAYOTIDAGI O'RNI .....	233-240
<i>Xidoyatov Bahtiyer Batiyrovich, Paraxatova Shahnoza Ernazarovna</i> ПРОЦЕССУАЛЬНЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ СПЕЦИАЛЬНЫХ ЗНАНИЙ В ПОЛУЧЕНИИ ОБРАЗЦОВ ДЛЯ ЭКСПЕРТНОГО ИССЛЕДОВАНИЯ В УГОЛОВНОМ ПРОЦЕССЕ .....	241-250
<i>Dadaboyeva Jumagul Anvarovna, Habibullayev Muhammadrajab Obidjonov</i> JAHON NAMJAMIYATINING GENDER TENGLIGINI TA'MINLASHGA QARATAYOTGAN E'TIBORI.....	251-256
<i>Abdужанпоров Шахбоз Музаффар ўғли</i> МОБИЛЬНОЕ БАНКОВСКОЕ МОШЕННИЧЕСТВО: УГРОЗЫ, МЕХАНИЗМЫ СОВЕРШЕНИЯ И КОМПЛЕКСНЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ .....	257-267
<i>Nasridinov Yigitali Borataliyevich</i> XOTIN-QIZLARNI TAZYIQ VA ZO'RAVONLIKDAN HIMOYA QILISH SOHASIDA DAVLAT SIYOSATI VA HUQUQIY ASOSLAR.....	268-276

<i>Mirzakarimova Dilafruz Doniyorjon qizi</i> SUN'YI INTELLEKT YORDAMIDA KIBERHUUJUMLARNI ANIQLASH VA OLDINI OLISH .....	277-281
<i>Mamatmurodov Farrux Farxod o'g'li</i> O'ZBEKISTON KAPITAL BOZORINI RIVOJLANTIRISHDA SUKUK INSTRUMENTLARINING INSTITUTSIONAL ROLI .....	282-289
<i>Нодирбекова Дилдона Абдумалик кизи</i> КОНСТИТУЦИОННЫЕ ОСНОВЫ ПРАВА НА ДОСТУП К ЭКОЛОГИЧЕСКОЙ ИНФОРМАЦИИ И ПРАВОВОЙ АНАЛИЗ АДМИНИСТРАТИВНОЙ ПРАКТИКИ .....	290-297
<i>Ahmadjonov Sultonbek Shukurillo o'g'li</i> QALBAKI PUL, AKSIZ MARKASI YOKI QIMMATLI QOG'OZLAR YASASH VA ULARNI O'TKAZISH JINOYATINING AYRIM JINOIY-HUQUQIY JIHATLARI .....	298-307
<i>Оттаубаева Айгуль Бахрамовна</i> КЛАССИФИКАЦИЯ АДМИНИСТРАТИВНЫХ ЭКОЛОГИЧЕСКИХ ПРАВОНАРУШЕНИЙ В ЗАКОНОДАТЕЛЬСТВЕ РЕСПУБЛИКИ УЗБЕКИСТАН: СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ С ОПЫТОМ РЕСПУБЛИКИ КАЗАХСТАН .....	308-316
<i>Mukimbayev Otabek Sattarovich</i> GUVOHNING MAQOMINI HUQUQIY HIMOYALASHDA KONSEPTUAL YONDASHUVLAR.....	317-324
<i>Yakubov Mirzaxid Turabayevich</i> NORMATIV-HUQUQIY HUUJATLAR IJROSINI TA'MINLASHNING XORIJIY MODELLARI VA MILLIY AMALIYOT UCHUN XULOSALAR .....	325-333
<b>13.00.00 – PEDAGOGIKA FANLARI</b>	
<i>Jumaniyozova Muhayyo Tojiyevna</i> RAQAMLI TA'LIMDA KREATIV KOMPETENTLIKNI RIVOJLANTIRISHNING DIDAKTIK TALABLARI.....	334-338
<i>Raxmatullaev Dilmurod Raxmatullayevich</i> PROFESSIONAL TA'LIM TIZIMINI RIVOJLANTIRISH VA BO'LAJAK MUTAXASSISLARNING KASBIY KOMPETENSIYALARINI SHAKLLANTIRISHDA STRATEGIK YONDASHUVNING KONSEPTUAL ASOSLARI.....	339-348
<i>Yusupova Kamola Nuriddinovna</i> NEYROPEDAGOGIKA TA'LIM TIZIMINING YANGI ILMIY TARMOG'I SIFATIDA.....	349-353
<i>Umurzoqov Baxtiyor Boxodirovich</i> ZAMONAVIY SHAROITDA HARBIY KADRLAR BOSHQARUVI TIZIMI SAMARADORLIGINING ILMIY-AMALIY ASOSLARI.....	354-358
<i>Qobilova Nilufar Xudoyshukurovna, Xujamova Dilobar Berdiyrovna</i> OLIY PEDAGOGIK TA'LIM MUASSASALARIDA BO'LAJAK O'QITUVCHILARNING SHAXSIY VA KASBIY KONGRUENTLIGINI LOYIHAVIY YONDASHUV ASOSIDA RIVOJLANTIRISH MAZMUNI.....	359-366
<i>Xaitbayeva Durdona Zokirjon qizi</i> SUN'YI INTELLEKT ASOSIDAGI ADAPTIV RAQAMLI TA'LIM TIZIMINI LOYIHALASHNING NAZARIY-METODIK ASOSLARI .....	367-371

<i>Исмаилов Шухрат Абдусоат угли, Инназаров Маджид Амонович</i> МЕХАНИЗМЫ ВНЕДРЕНИЯ МОДЕЛИ ФИНАНСИРОВАНИЯ, ОСНОВАННОГО НА РЕЗУЛЬТАТАХ (PERFORMANCE-BASED FUNDING), В ПРОФЕССИОНАЛЬНОМ РАЗВИТИИ РУКОВОДЯЩИХ КАДРОВ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ .....	372-378
<i>Rakhmatova Madina Abdumumin kizi</i> IMPLEMENTATION OF PROGRAMS FOR AUTOMATIC DETECTION AND CORRECTION OF GRAMMATICAL ERRORS IN ENGLISH WRITING.....	379-384
<i>To'rayev Azamat Maqsudovich</i> TALABALARNING ILMIY-TADQIQOTCHILIK KOMPETENTLIGINI RIVOJLANTIRISHDA BO'SH VAQTN TASHKIL ETISHNING RAQAMLI METODIKASI.....	385-390
<i>Mahmudova Farangiz Qurbonboy qizi</i> STUDENTS' ATTITUDES TOWARD AI USE IN ENGLISH LANGUAGE LEARNING: HELP OR HINDRANCE? .....	391-399
<i>Burxonova Muxlisa Murtoz qizi</i> O'QISH SAVODXONLIGI DARSLIKLARIDAGI BADIY MATNLARNI O'QITISH ORQALI O'QUVCHILARDA 4K KO'NIKMALARINI SHAKLLANTIRISH.....	400-404

**Received:** 16 February 2026

**Accepted:** 01 March 2026

**Published:** 15 March 2026

*Article / Original Paper*

## **MOBILE BANKING FRAUD: THREATS, CRIME MECHANISMS AND COMPREHENSIVE COUNTERMEASURES**

**Abdujapporov Shahboz Muzaffar o'g'li**

Senior Operative Officer, Lieutenant,  
Ministry of Internal Affairs of the Republic of Uzbekistan

**Abstract.** The article examines current threats related to fraud in mobile banking in the context of digital financial services. Major crime mechanisms are analyzed, including social engineering, mobile malware, and compromise of authentication tools. Key factors contributing to the growth of mobile financial fraud are identified, and a comprehensive framework of legal, organizational, and technical countermeasures is proposed. The results of the study can be applied by financial institutions and law enforcement agencies.

**Keywords:** mobile banking, financial fraud, cybercrime, social engineering, banking security, payment data protection.

## **МОБИЛЬНОЕ БАНКОВСКОЕ МОШЕННИЧЕСТВО: УГРОЗЫ, МЕХАНИЗМЫ СОВЕРШЕНИЯ И КОМПЛЕКСНЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ**

**Абдужаппоров Шахбоз Музаффар ўгли**

Старший оперативный сотрудник, лейтенант  
Министерства внутренних дел Республики Узбекистан

**Аннотация.** В статье рассматриваются современные угрозы, связанные с мошенничеством в сфере мобильного банкинга в условиях цифровизации финансовых услуг. Проанализированы основные механизмы совершения преступлений, включая социальную инженерию, вредоносное программное обеспечение и компрометацию средств аутентификации. Выявлены факторы, способствующие росту мобильного финансового мошенничества, а также предложен комплекс правовых, организационных и технических мер противодействия. Практическая значимость исследования заключается в возможности использования результатов финансовыми организациями и правоохранительными органами.

**Ключевые слова:** мобильный банкинг, финансовое мошенничество, киберпреступность, социальная инженерия, банковская безопасность, защита платёжных данных.

DOI: <https://doi.org/10.47390/SPR1342V6I3Y2026N39>

**Введение.** В условиях стремительного развития цифровой экономики и активного внедрения информационных технологий в финансовую сферу мобильный банкинг стал одним из наиболее востребованных и динамично развивающихся инструментов предоставления банковских услуг. Современные мобильные приложения позволяют пользователям осуществлять широкий спектр операций — от проверки баланса и оплаты коммунальных услуг до перевода денежных средств, оформления кредитов и управления инвестициями. Удобство, доступность и высокая скорость обслуживания способствуют постоянному росту числа пользователей мобильных финансовых сервисов.

Одновременно с расширением цифровых каналов обслуживания существенно возрастает уровень рисков, связанных с обеспечением финансовой и информационной безопасности. Практика показывает, что развитие технологий неизбежно сопровождается адаптацией преступной деятельности к новым условиям. В последние годы наблюдается устойчивый рост преступлений, связанных с несанкционированным доступом к мобильным банковским приложениям и последующим хищением денежных средств. Данные преступления формируют самостоятельный сегмент киберпреступности и представляют серьёзную угрозу как для граждан, так и для финансовых организаций.

Современное мобильное мошенничество отличается рядом характерных особенностей. Прежде всего, большинство противоправных действий осуществляется дистанционно, без физического контакта с потерпевшим. Злоумышленники активно используют методы социальной инженерии, направленные на психологическое воздействие на пользователя, а также применяют специализированное программное обеспечение, позволяющее перехватывать данные и управлять устройством удалённо. В отличие от традиционных представлений о банковских преступлениях, в большинстве случаев объектом атаки становится не банковская инфраструктура, а сам пользователь и его мобильное устройство.

Особую значимость проблема приобретает в связи с тем, что мобильный телефон в современных условиях выполняет одновременно несколько критически важных функций: он используется как средство идентификации клиента, канал получения одноразовых кодов, инструмент подтверждения операций и платформа для доступа к финансовым сервисам. Таким образом, компрометация одного устройства может привести к полной утрате контроля над банковским счётом и другими связанными цифровыми сервисами.

Дополнительным фактором риска является расширение дистанционных форм обслуживания, включая удалённую регистрацию, восстановление доступа, смену контактных данных и подтверждение операций без личного посещения банковского отделения. Несмотря на очевидные преимущества таких решений, они увеличивают поверхность атаки и создают дополнительные возможности для злоумышленников, особенно при недостаточной проверке личности клиента или отсутствии многоуровневых механизмов аутентификации.

С криминологической точки зрения мобильное банковское мошенничество характеризуется высокой степенью латентности, трансграничным характером и сложной структурой преступных схем. Во многих случаях противоправные действия реализуются в виде многоэтапных сценариев, включающих сбор персональных данных, получение доступа к устройству, обход механизмов подтверждения операций и вывод похищенных средств через цепочку транзитных переводов. Такая многоуровневая организация преступной деятельности существенно усложняет процессы выявления, расследования и доказывания.

С правовой точки зрения рассматриваемая категория преступлений представляет собой сложный объект квалификации. Деяния, связанные с мобильным банковским мошенничеством, могут включать признаки сразу нескольких составов правонарушений, таких как незаконный доступ к информации, мошенничество,

неправомерное использование персональных данных, распространение вредоносного программного обеспечения и вмешательство в работу информационных систем. Это требует выработки комплексного подхода к правовой оценке и совершенствования методических рекомендаций для правоохранительных органов.[1]

Не менее важным аспектом проблемы является человеческий фактор. Анализ практики показывает, что значительная часть успешных хищений становится возможной вследствие недостаточной цифровой грамотности пользователей, доверия к неизвестным источникам информации, передачи конфиденциальных данных третьим лицам и несоблюдения базовых правил кибербезопасности. В этих условиях повышение уровня информированности населения становится одним из ключевых направлений профилактики.

Таким образом, рост масштабов мобильного банкинга, усложнение преступных схем и увеличение количества дистанционных финансовых операций обуславливают высокую актуальность исследования механизмов совершения мошенничества в данной сфере. Комплексный анализ факторов, способствующих несанкционированному доступу к мобильным банковским сервисам, а также разработка эффективных мер противодействия имеют важное значение для обеспечения финансовой безопасности граждан, повышения устойчивости банковской системы и совершенствования практики правоохранительной деятельности.

Целью настоящего исследования является анализ современных угроз мобильного банковского мошенничества, выявление типовых механизмов совершения преступлений и разработка комплекса правовых, организационных и технических мер, направленных на их предупреждение и эффективное противодействие.

**Методология.** Методологическая основа исследования сформирована с учётом комплексного характера мобильного банковского мошенничества как социально-правового, криминологического и информационно-технического явления. Специфика рассматриваемой проблемы обусловлена тем, что противоправные посягательства в сфере мобильного банкинга формируются на стыке правовых норм, особенностей функционирования финансовой инфраструктуры, технологических процессов обработки данных и поведенческих факторов пользователей. В связи с этим в работе применён междисциплинарный подход, обеспечивающий системное и всестороннее изучение исследуемого объекта.

В качестве базового методологического подхода использован системный анализ, позволивший рассмотреть мобильное банковское мошенничество как совокупность взаимосвязанных элементов, включающих цифровые каналы обслуживания, механизмы аутентификации, поведение пользователей, организационные процедуры финансовых организаций и действия преступных субъектов. Данный подход обеспечил выявление причинно-следственных связей между технологическими уязвимостями, организационными недостатками и ростом преступности в рассматриваемой сфере. [2]

В ходе исследования применялся формально-юридический метод, направленный на анализ действующего законодательства Республики Узбекистан, регулирующего вопросы защиты информации, противодействия мошенничеству, незаконному доступу к информационным системам и использованию электронных платёжных средств. Проведённое правовое исследование позволило определить особенности

квалификации преступлений, совершаемых с использованием мобильного банкинга, выявить проблемные аспекты правоприменительной практики и обозначить направления совершенствования нормативного регулирования.

Для изучения типовых механизмов совершения противоправных действий использовался криминологический анализ, включающий систематизацию распространённых способов совершения преступлений, характеристику моделей поведения злоумышленников, а также выявление факторов, способствующих росту мобильного финансового мошенничества. В рамках данного анализа особое внимание уделялось методам социальной инженерии, комбинированным сценариям атак и многоэтапным схемам несанкционированного доступа к банковским приложениям.

Сравнительно-правовой метод позволил сопоставить национальные подходы к противодействию мобильному банковскому мошенничеству с международной практикой и рекомендациями зарубежных организаций. Проведённое сравнение способствовало выявлению эффективных механизмов защиты, применяемых в иностранных юрисдикциях, и определению перспективных направлений их адаптации к национальной правовой системе.

В работе также использовались аналитический и логический методы, направленные на обобщение научных публикаций, аналитических материалов финансовых организаций и международных отчётов по вопросам киберпреступности. Применение методов индукции и дедукции позволило перейти от анализа отдельных случаев мошенничества к формированию обобщённых выводов о закономерностях развития преступности в сфере мобильного банкинга. [3]

Существенное значение в исследовании имел функционально-технический анализ, направленный на изучение особенностей работы мобильных банковских приложений, механизмов идентификации и аутентификации пользователей, а также способов подтверждения финансовых операций. Данный анализ позволил определить наиболее уязвимые этапы обработки транзакций, на которых вероятность несанкционированного вмешательства является максимальной.

Эмпирическую основу исследования составили материалы открытых источников, аналитические отчёты банковских и платёжных организаций, статистические данные правоохранительных органов, а также обобщённые сведения о практике выявления и расследования преступлений, связанных с мобильным банкингом. Использование практико-ориентированных материалов обеспечило прикладную направленность исследования и позволило учитывать реальные условия функционирования финансовой системы.

Дополнительно применялся поведенческий анализ, направленный на изучение действий пользователей в ситуациях взаимодействия с потенциально мошенническими сценариями. Данный подход позволил выявить типичные ошибки клиентов, связанные с передачей конфиденциальных данных, установкой программного обеспечения из неофициальных источников и недостаточной проверкой получаемой информации.

В рамках исследования также использовался риск-ориентированный подход, предполагающий оценку вероятности реализации угроз на различных этапах взаимодействия пользователя с мобильным банковским приложением. Это позволило определить приоритетные направления профилактики и сформулировать

рекомендации, ориентированные на предупреждение противоправных действий на ранних стадиях их реализации.

Следует отметить, что исследование основывается преимущественно на обобщённых аналитических данных и материалах открытых источников, что обусловлено ограниченным доступом к конфиденциальной информации о конкретных инцидентах. Тем не менее использование различных методов научного познания и сопоставление данных из нескольких источников обеспечили достаточную степень достоверности полученных результатов. [4]

Применение указанных методологических подходов в совокупности позволило обеспечить комплексность исследования, объективность научных выводов и возможность разработки практико-ориентированных мер, направленных на повышение уровня безопасности мобильных банковских услуг и снижение рисков финансового мошенничества.

**Результаты исследования.** Проведённый анализ показал, что преступления, связанные с использованием мобильного банкинга, формируют один из наиболее динамично развивающихся сегментов современной киберпреступности. В отличие от традиционных форм финансовых посягательств, данные преступления реализуются преимущественно дистанционно и характеризуются сочетанием технических методов воздействия и психологического манипулирования пользователями.

Исследование позволило установить, что успешные преступные сценарии в большинстве случаев реализуются по многоэтапной модели, включающей:

1. получение персональных или платёжных данных пользователя;
2. получение доступа к мобильному устройству либо банковскому приложению;
3. обход механизмов подтверждения операций;
4. вывод денежных средств и сокрытие следов противоправной деятельности.

### **1. Основные модели преступных посягательств**

В результате обобщения практических и аналитических материалов были выявлены наиболее распространённые модели мобильного банковского мошенничества. [6]

#### **Социально-инженерные схемы**

Наибольшая доля преступлений связана с психологическим воздействием на пользователя. Злоумышленники представляются сотрудниками банков, правоохранительных органов или сервисных организаций и убеждают клиента:

- сообщить одноразовый код подтверждения;
- установить «защитное» или «служебное» приложение;
- выполнить перевод на так называемый безопасный счёт;
- предоставить доступ к устройству через программы удалённого управления.

Особенностью данной модели является отсутствие прямого взлома системы: пользователь фактически самостоятельно выполняет действия, приводящие к хищению средств.

#### **Использование вредоносного программного обеспечения**

В ходе исследования установлено, что мобильные устройства всё чаще становятся объектом заражения специализированным вредоносным программным обеспечением. Такие программы позволяют:

- перехватывать SMS и push-уведомления;
- считывать данные для входа в банковское приложение;
- подменять интерфейс программ;
- осуществлять удалённое управление устройством.

Наиболее опасными являются сценарии, при которых вредоносное приложение устанавливается самим пользователем под воздействием социальной инженерии. [7]

### **Компрометация средств аутентификации**

Отдельную группу составляют преступления, направленные на получение контроля над средствами подтверждения операций. К ним относятся:

- перевыпуск или подмена SIM-карты;
- компрометация электронной почты;
- получение доступа к облачным сервисам;
- изменение контактных данных пользователя.

Получив контроль над каналами подтверждения, злоумышленник может инициировать восстановление доступа к банковскому приложению и осуществлять финансовые операции.

Наиболее сложные и эффективные преступные схемы представляют собой сочетание нескольких методов. Например: телефонный звонок → установка вредоносного приложения → перехват кодов → вход в мобильный банк → серия переводов на подставные счета.

Такие многоэтапные цепочки существенно усложняют выявление преступления и его последующее расследование.

Исследование позволило определить основные каналы утраты контроля над финансовой информацией:

- фишинговые ссылки в SMS и мессенджерах;
- поддельные сайты и страницы авторизации;
- звонки с подменой номера;
- установка приложений из неофициальных источников;
- утечки данных на сторонних сервисах.

Особую опасность представляют каналы, позволяющие одновременно получить учётные данные и доступ к средствам подтверждения операций.

Анализ показал, что наибольший риск несанкционированного доступа возникает на следующих этапах:

- регистрация и первичная привязка устройства;
- восстановление доступа к учётной записи;
- смена номера телефона или контактных данных;
- подключение нового устройства;
- изменение лимитов и настроек безопасности;
- подтверждение финансовых операций.

В ряде случаев уязвимость обусловлена недостаточной проверкой личности клиента при дистанционном обслуживании.

В ходе исследования были выявлены признаки, позволяющие выявлять противоправные действия на ранней стадии. [8]

**Поведенческие признаки:**

- вход в систему с нового устройства;
- отключение уведомлений;
- изменение параметров безопасности;
- активные действия в нехарактерное время.

**Транзакционные признаки:**

- резкое увеличение активности по счёту;
- серия переводов небольшими суммами;
- операции новым получателям;
- последовательные попытки проведения операций после отказов.

Использование данных признаков может повысить эффективность систем мониторинга.

**Обсуждение.** Полученные результаты позволяют рассматривать мобильное банковское мошенничество не только как совокупность отдельных преступных эпизодов, но и как устойчивую системную угрозу финансовой безопасности в условиях цифровизации. Анализ выявленных моделей противоправных действий показывает, что современная преступная деятельность в данной сфере развивается в направлении усложнения сценариев, комбинирования различных методов воздействия и максимального использования поведенческих особенностей пользователей.

Прежде всего, результаты исследования подтверждают, что ключевым элементом большинства преступных схем является человеческий фактор. Несмотря на высокий уровень технологической защищённости банковских систем, значительная часть успешных хищений становится возможной вследствие действий самих пользователей, вызванных доверием к злоумышленникам, недостаточной проверкой получаемой информации или нарушением базовых правил цифровой безопасности. Это свидетельствует о том, что традиционное понимание киберпреступности как исключительно технической проблемы является ограниченным и требует пересмотра в пользу поведенчески ориентированного подхода. [9]

Анализ показал, что в современных условиях преступники всё реже предпринимают попытки прямого взлома банковской инфраструктуры. Основные усилия направлены на получение доступа к средствам аутентификации и управления счётом через социальную инженерию, компрометацию мобильных устройств или контроль коммуникационных каналов. Такая стратегия позволяет обходить даже сложные системы защиты, поскольку формально операции выполняются от имени самого клиента.

Отдельного внимания заслуживает роль мобильных устройств как критически важного элемента финансовой экосистемы. Смартфон одновременно выполняет функции идентификатора пользователя, канала подтверждения операций и платформы для управления банковским счётом. В результате его компрометация фактически означает утрату контроля над финансовыми ресурсами. Это подтверждает вывод о необходимости пересмотра существующих подходов к аутентификации и усилению контроля операций, связанных с привязкой новых устройств, сменой номера телефона и восстановлением доступа.

Сопоставление выявленных уязвимых этапов обслуживания показывает, что наиболее высокий риск возникает не на стадии проведения транзакции, а на этапах изменения параметров доступа. Процедуры восстановления учётной записи, обновления контактных данных и подключения нового устройства нередко используются злоумышленниками как точка входа в систему. В этой связи особую актуальность приобретает усиление процедур идентификации клиента при выполнении указанных операций.

Результаты исследования также свидетельствуют о том, что значительная часть существующих механизмов противодействия ориентирована на выявление уже совершённых подозрительных операций. Однако современные преступные схемы формируются задолго до фактического списания денежных средств. Сначала происходит сбор информации, установление контакта с жертвой, получение доступа к устройству или каналам связи. Это позволяет сделать вывод о необходимости смещения акцента с постфактум-реагирования на раннее выявление признаков подготовки противоправных действий. [10]

Отдельным направлением анализа является эффективность систем транзакционного мониторинга. Полученные данные показывают, что изолированная оценка суммы операции или её географических параметров недостаточна для выявления мошенничества. Более перспективным представляется использование поведенческого анализа, учитывающего комплекс факторов: устройство, время активности, характер действий пользователя, изменения настроек безопасности и последовательность операций.

Важным результатом исследования является выявление тенденции к усложнению преступных сценариев и их трансграничному характеру. Вывод похищенных средств часто осуществляется через цепочку промежуточных счетов, электронных кошельков или иных платёжных инструментов, что существенно затрудняет их отслеживание и возврат. В этих условиях возрастает значение оперативного межбанковского взаимодействия и обмена информацией о подозрительных операциях.

С правовой точки зрения мобильное банковское мошенничество характеризуется высокой степенью сложности квалификации. Преступные действия могут включать признаки мошенничества, незаконного доступа к информации, неправомерного использования персональных данных, распространения вредоносных программ и иных противоправных деяний. Комбинированный характер преступлений требует разработки комплексных методических подходов к их расследованию и доказыванию, а также расширения использования цифровых следов в качестве доказательственной базы.

Анализ факторов роста преступности в рассматриваемой сфере подтверждает, что её развитие обусловлено объективными процессами цифровой трансформации. Увеличение числа дистанционных операций, массовое использование мобильных устройств и расширение онлайн-сервисов неизбежно приводят к росту потенциальной поверхности атаки. В этой связи полное устранение рисков представляется невозможным, а основная задача заключается в их минимизации и своевременном выявлении.

Особое значение в системе противодействия мобильному мошенничеству имеет профилактическая работа с населением. Повышение уровня цифровой грамотности пользователей, формирование устойчивых навыков безопасного поведения и регулярное информирование о новых мошеннических схемах позволяют существенно снизить вероятность успешной реализации преступных сценариев. Практика показывает, что даже краткие предупреждения и информационные сообщения способны значительно уменьшить число инцидентов. [11]

В целом обсуждение результатов подтверждает, что эффективное противодействие мобильному банковскому мошенничеству возможно только при условии комплексного подхода, объединяющего технологические, организационные и правовые меры. Изолированное применение отдельных инструментов не обеспечивает достаточного уровня защиты, поскольку современные преступные схемы формируются на пересечении нескольких уязвимых элементов.

Таким образом, мобильное банковское мошенничество следует рассматривать как многоуровневую угрозу, требующую координированных действий финансовых организаций, телекоммуникационных операторов, правоохранительных органов и самих пользователей. Только системное взаимодействие всех участников финансовой экосистемы способно обеспечить устойчивое снижение уровня несанкционированного доступа и минимизацию финансовых потерь в условиях дальнейшей цифровизации.

**Заключение.** Проведённое исследование показало, что мобильное банковское мошенничество в условиях цифровизации финансовых услуг представляет собой сложное и многоуровневое явление, формирующееся на пересечении технологических уязвимостей, организационных особенностей дистанционного обслуживания и поведенческих факторов пользователей. Активное развитие мобильного банкинга, расширение спектра онлайн-операций и рост числа пользователей создают объективные предпосылки для увеличения количества преступлений, связанных с несанкционированным доступом к финансовым сервисам и хищением денежных средств.

Установлено, что современные преступные схемы в сфере мобильного банкинга отличаются высокой степенью адаптивности и комбинированным характером. В большинстве случаев противоправные действия реализуются не путём прямого взлома банковской инфраструктуры, а посредством социальной инженерии, компрометации мобильных устройств, получения контроля над средствами аутентификации и эксплуатации доверия пользователей. Это подтверждает вывод о том, что уровень финансовой безопасности определяется не только технической защищённостью банковских систем, но и эффективностью управления рисками, связанными с человеческим фактором. [12]

Анализ выявленных моделей преступных посягательств позволил определить ключевые этапы реализации мошеннических сценариев, включающие получение персональных данных, обход механизмов подтверждения операций и вывод денежных средств через многоступенчатые транзитные схемы. Особую уязвимость представляют процедуры восстановления доступа, смены контактных данных и подключения новых устройств, которые нередко используются злоумышленниками в качестве точки входа в систему.

Результаты исследования также свидетельствуют о том, что значительная часть существующих мер противодействия ориентирована на выявление уже совершённых подозрительных операций. Вместе с тем наибольший потенциал эффективности связан с реализацией профилактических механизмов, направленных на раннее обнаружение признаков подготовки противоправных действий и предотвращение их развития.

С правовой точки зрения мобильное банковское мошенничество характеризуется сложной структурой и нередко включает признаки нескольких составов правонарушений, связанных с мошенничеством, незаконным доступом к информации и неправомерным использованием цифровых данных. Это требует совершенствования методик правовой квалификации, расширения практики использования цифровых доказательств и усиления межведомственного взаимодействия при расследовании данной категории преступлений.

В ходе исследования установлено, что эффективное противодействие мобильному финансовому мошенничеству возможно только при условии комплексного применения правовых, организационных и технических мер. Приоритетное значение имеют внедрение многофакторной и адаптивной аутентификации, развитие систем поведенческого мониторинга, усиление контроля операций повышенного риска, а также системное информирование пользователей о современных угрозах.

Таким образом, обеспечение безопасности мобильных банковских услуг требует согласованных действий всех участников финансовой экосистемы, включая банки, телекоммуникационных операторов, правоохранительные органы и самих пользователей. Реализация комплексного подхода, ориентированного на предупреждение противоправных действий и снижение поведенческих рисков, позволит повысить устойчивость платёжной инфраструктуры и минимизировать финансовые потери в условиях дальнейшего развития цифровых технологий. [13]

**Предложения.** В целях повышения эффективности противодействия мошенничеству, связанному с использованием мобильного банкинга, представляется необходимым совершенствование правового регулирования и правоприменительной практики.

Целесообразно уточнить нормы законодательства, регулирующие ответственность за неправомерный доступ к банковским приложениям, получение контроля над средствами аутентификации и участие в переводе либо обналичивании похищенных денежных средств. Это позволит более точно квалифицировать противоправные действия с учётом их цифрового и комбинированного характера.

Необходимо разработать и внедрить единые методические рекомендации для правоохранительных органов по квалификации и расследованию преступлений, связанных с мобильным банковским мошенничеством, а также расширить практику использования электронных доказательств, включая данные о транзакциях, устройствах и сетевой активности.

Представляется важным законодательное закрепление механизмов оперативного взаимодействия между банками, операторами связи и правоохранительными органами, а также ускоренных процедур временной блокировки подозрительных операций и счетов.

Реализация указанных мер позволит повысить эффективность выявления и расследования преступлений, сократить финансовый ущерб и обеспечить более надёжную защиту прав граждан в условиях цифровизации финансовых услуг.

#### **Литература/References/Adabiyotlar:**

1. Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., ... Savage, S. (2013). Measuring the cost of cybercrime. Workshop on the Economics of Information Security (WEIS).
2. European Central Bank. (2022). Report on cyber resilience of financial institutions. Frankfurt: ECB.
3. Federal Financial Supervisory Authority (BaFin). (2021). Guidelines for secure mobile banking. Bonn: BaFin.
4. Gozman, D., & Curran, K. (2014). Mobile banking fraud: Understanding risks and mitigation strategies. *Journal of Financial Crime*, 21(2), 188–205.
5. Kaspersky Lab. (2023). Mobile malware report. Moscow: Kaspersky.
6. Малышев, В.В. (2020). Киберпреступления в банковской сфере: методы и профилактика. Москва: Финансы и статистика.
7. Официальный веб-сайт Центрального банка Республики Узбекистан. (2025). Информация о защите клиентов банков и предупреждении мошенничества. Доступно: <https://cbu.uz>
8. Smith, A., & Thomas, R. (2020). Social engineering in mobile banking: Psychological manipulation and prevention. *International Journal of Cybersecurity*, 5(1), 23–41.
9. United Nations Office on Drugs and Crime (UNODC). (2022). Global report on cybercrime and digital financial fraud. Vienna: UNODC.
10. Закон Республики Узбекистан «О защите информации» (2020). Ташкент: LexUZ.
11. Закон Республики Узбекистан «О противодействии мошенничеству и незаконному доступу к информационным системам» (2020). Ташкент: LexUZ.
12. Verizon. (2023). Data breach investigations report (DBIR). New York: Verizon.
13. Zetter, K. (2015). Countdown to zero day: Stuxnet and the launch of the world's first digital weapon. New York: Crown.

# SCIENCEPROBLEMS.UZ

## IJTIMOYIY-GUMANITAR FANLARNING DOLZARB MUAMMOLARI

*№ 3 (6) – 2026*

## АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОЦИАЛЬНО- ГУМАНИТАРНЫХ НАУК

## ACTUAL PROBLEMS OF HUMANITIES AND SOCIAL SCIENCES

**“Ijtimoiy-gumanitar fanlarning dolzarb muammolari”** elektron jurnali 2020-yil 6-avgust kuni 1368-sonli guvohnoma bilan davlat ro‘yxatiga olingan.

**Muassis:** “SCIENCEPROBLEMS TEAM”  
mas’uliyati cheklangan jamiyati

**Tahririyat manzili:**

100070. Toshkent shahri, Yakkasaroy tumani, Kichik Beshyog‘och ko‘chasi, 70/10-uy. Elektron manzil:

[scienceproblems.uz@gmail.com](mailto:scienceproblems.uz@gmail.com)

**Bog‘lanish uchun telefon:**

(99) 602-09-84 (telegram).