O‘ZBEKISTON RESPUBLIKASI
ICHKI ISHLAR VAZIRLIGI

O‘ZBEKISTON RESPUBLIKASI
KRIMINOLOGIYA TADQIQOT INSTITUTI

KRIMINOLOGIYANING DOLZARB MASALALARI

Respublika ilmiy-amaliy konferensiya materiallari to‘plami

TOSHKENT – 2026

O‘zbekiston Respublikasi Kriminologiya tadqiqot instituti kengashining yig‘ilishida (2026 йил 28-сентябрдаги 10-сонли баённома) muhokama qilingan hamda nashrga tavsiya etilgan

Mas’ul muharrir
O‘zbekiston Respublikasi Kriminologiya tadqiqot instituti boshlig‘i, yuridik fanlar bo‘yicha falsafa doktori (PhD), **B.E. Berdialiyev.**

Taqrizchilar:
siyosiy fanlar doktori, professor **I. Ergashev;**
yuridik fanlar bo‘yicha falsafa doktori (PhD), dotsent **D.Yu.Payziyev.**

Nashrga tayyorlovchilar:
falsafa doktori (PhD), professor **R.O. Nigmatov**; filologiya fanlari nomzodi **B.A. Yarov;** tibbiyot fanlari bo‘yicha falsafa doktori (PhD) **I.E. To‘raev**; falsafa fanlari bo‘yicha falsafa doktori (PhD), dotsent **Sh.Sh. Hasanov**; yuridik fanlari bo‘yicha falsafa doktori (PhD) **U.A. Irisbekov; D.B.Mamarajabova.**

Kriminologiyaning dolzarb masalalari: Respublika ilmiy-amaliy konferensiyasi materiallari to‘plami (2026-yil 25-sentyabr). – T.: O‘zbekiston Respublikasi Kriminologiya tadqiqot instituti, 2026. – 332 b.

Mazkur to‘plamda Kriminologiyaning dolzarb masalalari, jinoyatchilikning zamonaviy tendensiyalari, uning sabab va shart-sharoitlarini aniqlash, jinoyatchilikning oldini olish hamda profilaktika tizimini takomillashtirishning nazariy va amaliy jihatlari yoritilgan. Unda jinoyatchilikning miqdor va sifat ko‘rsatkichlari, uning hududiy va ijtimoiy xususiyatlari, zamonaviy kriminogen omillar, jinoyat sodir etuvchi shaxsning kriminologik tavsifi, viktimologik jarayonlar, shuningdek, jinoyatchilikka qarshi kurashish va uni barvaqt profilaktika qilishning samarali mexanizmlari tahlil qilingan.

Shuningdek, to‘plamda raqamlashtirish, sun’iy intellekt, kiberjinoyatchilik, uyushgan va transmilliy jinoyatchilik, yoshlar va voyaga yetmaganlar jinoyatchiligi, oilaviy-maishiy nizolar, zo‘ravonlik bilan bog‘liq jinoyatlar kabi zamonaviy kriminologik muammolarga alohida e’tibor qaratilgan. Mavjud muammolarni bartaraf etish, ilg‘or xorijiy tajribani o‘rganish va milliy amaliyotga joriy etish, kriminologik prognozlash va ilmiy asoslangan profilaktika choralarini ishlab chiqish yuzasidan ilmiy-amaliy taklif va tavsiyalar ilgari surilgan.

To‘plam huquqni muhofaza qiluvchi organlar xodimlari, oliy ta’lim muassasalarining professor-o‘qituvchilari, olimlar, tadqiqotchilar, mustaqil izlanuvchilar, talabalar va kursantlar, shuningdek, kriminologiya, jinoyatchilikka qarshi kurashish va huquqbuzarliklar profilaktikasi masalalari bilan shug‘ullanuvchi mutaxassislar uchun mo‘ljallangan.

© O‘zbekiston Respublikasi Kriminologiya tadqiqot instituti, 2026-y.

KIRISH

Hozirgi globallashuv, raqamlashtirish va ijtimoiy munosabatlarning tezkor transformatsiyasi sharoitida jinoyatchilikning mazmun-mohiyati, tuzilishi va namoyon bo‘lish shakllari ham sezilarli ravishda o‘zgarib bormoqda. Jinoyatchilikning an’anaviy ko‘rinishlari bilan bir qatorda kiberjinoyatchilik, transmilliy va uyushgan jinoyatchilik, raqamli texnologiyalar hamda sun’iy intellekt vositalaridan jinoiy maqsadlarda foydalanish bilan bog‘liq yangi kriminogen tahdidlarning yuzaga kelishi kriminologiya fani oldiga yangi ilmiy-nazariy va amaliy vazifalarni qo‘ymoqda.

Shu nuqtayi nazardan, jinoyatchilikni faqat huquqiy hodisa sifatida emas, balki ijtimoiy, iqtisodiy, demografik, psixologik, madaniy hamda institutsional omillar bilan uzviy bog‘liq bo‘lgan murakkab ijtimoiy hodisa sifatida kompleks o‘rganish muhim ahamiyat kasb etadi. Jinoyatchilikning sabab va shart-sharoitlarini aniqlash, uning dinamikasi va tarkibiy xususiyatlarini tahlil qilish, kriminogen omillarni ilmiy asosda baholash hamda samarali profilaktik mexanizmlarni ishlab chiqish zamonaviy kriminologiyaning ustuvor vazifalaridan biri hisoblanadi.

“Kriminologiyaning dolzarb masalalari” mavzusidagi mazkur ilmiy-amaliy konferensiya aynan ana shu muammolarni ilmiy muhokama qilish, nazariy yondashuvlar va amaliy tajribalarni uyg‘unlashtirish, jinoyatchilikka qarshi kurashish hamda uning oldini olish sohasida innovatsion va ilmiy asoslangan yechimlarni ishlab chiqishga qaratilgan.

Konferensiya materiallarida jinoyatchilikning zamonaviy tendensiyalari, uning hududiy va ijtimoiy xususiyatlari, jinoyat sodir etuvchi shaxsning kriminologik portreti, viktimologik jarayonlar, retsidiv, yoshlar va voyaga yetmaganlar jinoyatchiligi, ayollar jinoyatchiligi, uyushgan va transmilliy jinoyatchilik, zo‘ravonlik bilan bog‘liq jinoyatlar, kiberjinoyatchilik, raqamli muhitdagi xavflar, shuningdek, kriminologik prognozlash va profilaktikaning zamonaviy usullari kabi yo‘nalishlar qamrab olingan.

To‘plamga kiritilgan ilmiy maqolalarda jinoyatchilikka ta’sir etuvchi determinantlar, jinoiy xulq-atvor mexanizmlari, huquqbuzarliklar profilaktikasining tashkiliy-huquqiy va institutsional asoslari, huquqni muhofaza qiluvchi organlar faoliyati samaradorligini oshirish masalalari, shuningdek, ilg‘or xorijiy tajribadan foydalanish imkoniyatlari tahlil qilingan. Mualliflar tomonidan nazariy xulosalar bilan bir qatorda huquqni qo‘llash amaliyotini takomillashtirishga qaratilgan ilmiy-amaliy taklif va tavsiyalar ham ilgari surilgan.

Mazkur ilmiy to‘plam kriminologiya sohasidagi zamonaviy ilmiy qarashlarni umumlashtirish, mavjud ilmiy muammolarni tizimli tahlil qilish, jinoyatchilikning yangi shakllarini o‘rganish va ularga qarshi samarali profilaktik choralarni belgilash nuqtayi nazaridan muayyan nazariy va amaliy ahamiyatga ega.

Shu bilan birga, konferensiya natijalari kriminologiya sohasida fundamental va amaliy tadqiqotlarni yanada rivojlantirish, ilmiy muassasalar, oliy ta’lim tashkilotlari va huquqni muhofaza qiluvchi organlar o‘rtasidagi ilmiy hamkorlikni mustahkamlash, kriminologik tahlil va prognozlashning zamonaviy metodlarini amaliyotga joriy etish hamda jinoyatchilik profilaktikasining samaradorligini oshirishga xizmat qilishi kutilmoqda.

Umid qilamizki, mazkur to‘plamda jamlangan ilmiy izlanishlar va amaliy takliflar kriminologiya fanining nazariy-metodologik asoslarini boyitish, milliy kriminologik tadqiqotlar sifatini oshirish va jinoyatchilikka qarshi kurashish sohasida ilmiy asoslangan yondashuvlarni shakllantirishga munosib hissa qo‘shadi.



ВИКТИМОЛОГИЧЕСКИЕ ФАКТОРЫ УЯЗВИМОСТИ ЛИЧНОСТИ В СФЕРЕ ЦИФРОВЫХ ФИНАНСОВЫХ ТЕХНОЛОГИЙ

Исаков Лутфуллохон Карамат угли
Главный юрисконсульт Исследовательского института криминологии Республики Узбекистан
https://orcid.org/0009-0007-1014-1105

Аннотация. *В статье исследуется уязвимость личности перед преступными посягательствами в сфере цифровых финансовых технологий. Актуальность темы обусловлена тем, что в 2025 году почти половина преступлений в Республике Узбекистан совершена с использованием информационных технологий, причём свыше 95 % из них составили кражи и мошенничества. Цель работы состоит в разработке модели виктимологической уязвимости и типологии её факторов. Использованы системный подход, сравнительный анализ научных подходов, формально-юридический метод, анализ статистики МВД и данных Global Findex 2025. Обосновано, что уязвимость является не свойством личности, а соотносительным состоянием, образуемым подверженностью преступному воздействию и восприимчивостью к нему. Предложена трёхуровневая типология факторов и раскрыт принцип их сопряжённости со стадией виктимизации и типом схемы. Результаты применимы в виктимологической профилактике и при совершенствовании законодательства.*

Ключевые слова: *виктимность, виктимизация, виктимологическая уязвимость, цифровая финансовая виктимизация, цифровые финансовые технологии, подверженность, восприимчивость, потерпевший, мошенничество, цифровая грамотность.*

Цифровые финансовые технологии за последние годы стали для большинства граждан обычным способом распоряжаться деньгами. По данным Всемирного банка, в 2024 году счёт в банке или иной финансовой организации имели 59,7 % взрослого населения Узбекистана, а мобильный телефон 82,3 % [24]. Вместе с удобством эта среда открыла и новые возможности для преступников. По ведомственным данным МВД Республики Узбекистан, доля преступлений, совершённых с использованием информационных технологий, выросла с 44,4 % в 2024 году до 49,6 % в 2025 году и достигла 54,2 % за восемь месяцев 2026 года [6]. Почти все такие деяния направлены против имущества граждан.

Защита в этой сфере традиционно строится вокруг технологий. Однако значительная часть посягательств совершается без взлома информационных систем. Операцию проводит сам владелец счёта либо она проводится с использованием переданных им данных. Главным звеном механизма становится человек, принимающий финансовое решение, поэтому необходимо понять, почему одни пользователи становятся потерпевшими, а другие нет.

Распространённое объяснение сводится к тому, что жертвами становятся доверчивые и финансово неграмотные люди. Именно так характеризует

адресатов мошеннических схем Центральный банк Республики Узбекистан [10]. Такое объяснение понятно, но для криминологии его недостаточно. Оно не отличает обстоятельства, которые приводят человека к контакту с преступником, от обстоятельств, которые мешают ему распознать обман. Оно не учитывает, что значение каждого фактора зависит от схемы и ситуации. Наконец, оно перекладывает ответственность на потерпевшего и оставляет в стороне условия, которые создают поставщики финансовых услуг.

Проблема исследования состоит в отсутствии научно обоснованной модели, которая объясняла бы уязвимость личности в цифровой финансовой среде как результат взаимодействия разных факторов, а не как личный недостаток потерпевшего. Цель статьи заключается в разработке такой модели и типологии образующих её факторов. Для этого необходимо разграничить основные виктимологические понятия, критически обобщить научные подходы к факторам виктимизации, обосновать основания их классификации, показать механизм взаимодействия факторов с криминогенным воздействием и соотнести полученную модель с данными по Узбекистану.

Механизм социальной инженерии рассматривался автором в отдельной работе, поэтому здесь меняется перспектива. Вопрос ставится не о том, как преступник воздействует на человека, а о том, почему конкретный человек оказывается более уязвимым перед этим воздействием.

Анализ литературы по теме

Классическая виктимология исходила из того, что жертва не является пассивным объектом преступления. Г. фон Хентиг обратил внимание на взаимодействие преступника и жертвы и на свойства, повышающие риск стать жертвой [18]. В советской науке Л.В. Франк ввёл понятие виктимности как повышенной способности лица становиться жертвой преступления [9]. Д.В. Ривман развил это учение, разграничив личностную и ролевую виктимность и описав виктимогенные ситуации [5]. Эти концепции сложились на материале преступности, при которой преступник и жертва встречаются лично. В цифровой среде такой встречи нет, и поведение жертвы проявляется в её действиях в интерфейсе финансового сервиса.

Второе направление связано с теориями возможностей. Согласно теории рутинной активности, преступление происходит при совпадении мотивированного преступника, подходящей цели и отсутствия способного защитника [12]. К. Холтфретер, М. Рейсиг и Т. Пратт показали, что дистанционные покупки повышают риск стать объектом мошеннической попытки, а низкий самоконтроль связан с виктимизацией [19]. Последующие работы подтвердили, что активность в сети повышает вероятность стать мишенью мошенников [22]. Вместе с тем проверка теории на выборке свыше девяти тысяч человек показала, что её элементы применимы к киберпреступлениям неодинаково и наиболее отчётливо действует видимость пользователя [21]. Эти теории хорошо объясняют, как человек попадает в поле зрения преступника. Хуже они объясняют, почему при одинаковом контакте один человек уступает обману, а другой нет.

Третье направление представлено эмпирическими исследованиями факторов мошеннической виктимизации. М. Уитти на выборке из 11 780 человек установила, что жертвы кибермошенничества чаще были старше, отличались импульсивностью и чаще совершали рискованные действия в сети [23]. Л. Конинг, М. Юнгер и Б. Велдкамп на репрезентативной голландской выборке пришли к выводу, что устойчивого профиля жертвы не существует. Исключение составили низкий самоконтроль, мигрантское происхождение и частое пользование интернетом, а знание мошеннических схем снижало восприимчивость к ним [20]. Они рассматривают виктимизацию как двухстадийный процесс, в котором за контактом с попыткой обмана следует уступка ей или противодействие, причём разные факторы действуют на этих стадиях по-разному [20]. Систематический обзор 2025 года подтвердил, что жертвы мошенничества не образуют однородной группы, а одни и те же признаки могут снижать риск контакта с мошенником и одновременно повышать риск виктимизации после контакта [14]. Австралийский институт криминологии установил, что привычность к онлайн-операциям снижает вероятность стать жертвой [15].

Особого внимания заслуживает вопрос о доверчивости. В русскоязычной литературе её обычно называют главным качеством жертвы мошенничества. Однако в исследовании Л. Конинга и соавторов связь общего уровня доверия к людям с виктимизацией не подтвердилась, и авторы указывают на работы, где она не подтверждалась и прежде [20]. Это не означает, что доверие не имеет значения. По нашему мнению, значимо не общее доверие к людям, а доверие к конкретному источнику в конкретной ситуации, которое преступник создаёт намеренно. Следовательно, доверчивость правильнее рассматривать не как устойчивую черту жертвы, а как результат воздействия.

Четвёртое направление составляет русскоязычная кибервиктимология. Д.В. Жмуров систематизировал факторы кибервиктимизации [2], А.В. Майоров обосновал виктимологию цифровой преступности как самостоятельное научное направление [3]. В этих работах накоплен ценный перечень качеств жертвы, но факторы, как правило, перечисляются без разграничения стадий виктимизации и без учёта типа схемы. Встречается и позиция, согласно которой поведение жертв хищений, прежде всего мошенничества, имеет ярко выраженный виктимный характер [1]. С ней трудно согласиться без оговорок. К. Кросс показала, что представление о жертвах онлайн-мошенничества как о жадных и легковерных людях широко распространено и разделяется самими жертвами, а это мешает им обращаться за помощью [13]. Анализ, построенный на таком представлении, рискует превратиться в обвинение жертвы.

Пятое направление отражает подход финансовых регуляторов. Британский регулятор понимает уязвимого клиента как лицо, особенно подверженное вреду в силу личных обстоятельств, в том числе когда финансовая организация не проявляет должной заботы, и рассматривает уязвимость как спектр риска, которому подвержен каждый [16]. Принципы G20 и ОЭСР 2022 года также предусматривают усиленную защиту потребителей, которые могут оказаться

уязвимыми, и противодействие мошенничеству [17]. При таком подходе уязвимость зависит не только от человека, но и от среды, которую создаёт поставщик услуги.

Таким образом, в науке установлено, что устойчивого профиля жертвы не существует и что виктимизация включает стадию контакта и стадию уступки обману. Спорной остаётся роль доверчивости, возраста и образования. Недостаточно исследованы зависимость факторов от типа схемы, роль институциональных условий и ситуация в Узбекистане, где зарубежные выводы эмпирически не проверялись. Настоящая статья предлагает модель, которая объединяет эти элементы.

Методология исследования

Исследование носит теоретико-аналитический характер и построено по дедуктивной логике. Общие положения виктимологии и теорий возможностей конкретизируются применительно к цифровой финансовой среде и затем соотносятся с доступными данными. Использованы системный подход, анализ и синтез, сравнительный анализ научных подходов, а также формально-юридический метод при изучении Закона Республики Узбекистан «О профилактике правонарушений» [4] и Уголовного кодекса Республики Узбекистан [8].

Эмпирическую базу составили вторичные данные двух видов. Первый вид представляет ведомственная статистика МВД Республики Узбекистан о преступлениях, совершённых с использованием информационных технологий, и о мошенничестве за 2024 год, 2025 год и январь – август 2026 года по республике в целом [6]. Общее число преступлений за 2024 год в этих данных совпадает с опубликованным Агентством статистики [7; С. 427], что подтверждает надёжность источника. Второй вид представляют данные Global Findex 2025, собранные Всемирным банком в ходе национально репрезентативного опроса взрослого населения в 2024 году [24].

Эти данные имеют ограничения. Статистика МВД описывает преступления, а не потерпевших, и не содержит сведений о возрасте, образовании или занятости жертв. Данные Всемирного банка относятся ко всему взрослому населению. Поэтому они показывают распространённость отдельных факторов, но не доказывают их связь с виктимизацией. Анкетирование и изучение уголовных дел не проводились, поэтому выводы о значении факторов опираются на научную литературу.

Анализ и результаты

1. Понятийный аппарат и цифровая финансовая виктимизация

Потерпевший является правовым статусом. Закон «О профилактике правонарушений» понимает под потерпевшим от правонарушения лицо, пострадавшее вследствие причинения ему физического, морального или имущественного вреда [4]. Жертва преступления представляет собой более широкое криминологическое понятие. Оно охватывает и тех, кто не обратился в правоохранительные органы, что особенно важно для цифрового мошенничества с его высокой латентностью. Виктимность обозначает способность лица стать

жертвой, а виктимизация означает процесс и результат превращения лица в жертву. Виктимогенная ситуация представляет собой обстановку, повышающую вероятность виктимизации, а фактор виктимности является обстоятельством, которое такую вероятность повышает.

Цифровая виктимизация охватывает все случаи, когда лицо становится жертвой преступления в цифровой среде [2]. Цифровая финансовая виктимизация уже по объёму. Под ней предлагается понимать причинение лицу имущественного вреда посредством посягательства, при котором цифровые финансовые сервисы служат каналом доступа к его средствам или инструментом распоряжения ими. Её отличительная черта состоит в том, что операция нередко совершается самим потерпевшим или с использованием переданных им данных и выглядит для системы как законное распоряжение владельца. Данные МВД показывают, что в Узбекистане цифровая виктимизация является преимущественно финансовой (таблица 1).

Таблица 1. Преступления, совершённые с использованием информационных технологий, в Республике Узбекистан

Показатель	**2024**	**2025**	**Январь – август 2026**
Всего преступлений	132 298	155 002	111 429
Преступления с использованием ИТ	58 800	76 852	60 369
Их доля во всех преступлениях, %	44,4	49,6	54,2
В том числе кражи (ст. 169 УК)	36 444	37 261	29 859
В том числе мошенничества (ст. 168 УК)	21 036	36 265	26 492
Доля краж и мошенничеств среди ИТ-преступлений, %	97,8	95,7	93,3
Доля ИТ-мошенничеств во всех мошенничествах, %	71,9	82,2	85,4

Кражи и мошенничества составили от 93 до 98 % преступлений с использованием информационных технологий. Не менее важно соотношение между ними. При краже, предусмотренной статьёй 169 УК, преступник распоряжается средствами тайно, используя данные потерпевшего. При мошенничестве, предусмотренном статьёй 168 УК, операцию совершает сам потерпевший под влиянием обмана [8]. В 2024 году кражи преобладали в 1,7 раза, а в 2025 году и 2026 году число мошенничеств почти сравнялось с числом краж. Значит, всё большая часть посягательств требует активного участия самого потерпевшего. Для краж ведущее значение имеет защищённость данных, а для мошенничества способность распознать обман. Уже это показывает, что единый перечень качеств жертвы не может одинаково объяснять оба вида посягательств.

Эти наблюдения позволяют уточнить понятие виктимологической уязвимости. Классическая виктимность характеризует прежде всего само лицо, и для цифровой финансовой среды этого недостаточно по трём причинам. Во-первых, уязвимость складывается из двух разных компонентов.

Подверженность определяет вероятность контакта с преступным воздействием, а восприимчивость определяет вероятность не распознать это воздействие и уступить ему. Во-вторых, уязвимость проявляется только в конкретной ситуации. Человек, уверенно пользующийся мобильным банком, может уступить обману в момент стресса или спешки. В-третьих, уязвимость зависит от условий, которые создаёт поставщик услуги. Мгновенный и необратимый перевод или кредит, оформляемый за несколько минут, превращают кратковременную ошибку в невосполнимый ущерб.

С учётом этого виктимологическую уязвимость личности в сфере цифровых финансовых технологий предлагается определить как соотносительное состояние лица, образуемое его подверженностью преступному воздействию и восприимчивостью к нему, которое актуализируется в конкретной виктимогенной ситуации и усиливается или ослабляется институционально-технологическими условиями цифровой финансовой среды. Слово «соотносительное» подчёркивает, что уязвимость существует не в человеке самом по себе, а в его отношении к среде и к конкретному воздействию. Виктимность при таком подходе остаётся родовым понятием, а виктимологическая уязвимость служит её конкретизацией для цифровой финансовой среды.

2. Типология факторов виктимологической уязвимости

Перечни факторов, которые обычно приводятся в литературе, смешивают разные основания деления. В один ряд ставятся личностные черты, уровень знаний, поведение и действия преступника. Между тем действия преступника характеризуют не потенциальную жертву, а источник угрозы, и их включение в число виктимологических факторов стирает грань между механизмом преступления и уязвимостью личности. Кроме того, в таких перечнях почти не отражены условия, которые создаёт финансовая среда. В предлагаемой типологии единым основанием служат место действия фактора и его устойчивость во времени (таблица 2).

Таблица 2. Типология факторов виктимологической уязвимости личности в сфере цифровых финансовых технологий

Уровень	Группа факторов	Содержание	Компонент уязвимости	Подтверждённость в исследованиях
Диспозиционный	Социально-демографические	возраст, пол, образование, занятость, мигрантское происхождение, первичное обращение к финансовым услугам	подверженность и восприимчивость (разнонаправленно)	зависит от типа схемы [14, 20]
	Психологические	низкий самоконтроль, импульсивность, склонность к риску, реакция на авторитет	восприимчивость	низкий самоконтроль подтверждён устойчиво, общая доверчивость не подтверждена [19, 20, 23]

Уровень	Группа факторов	Содержание	Компонент уязвимости	Подтверждённость в исследованиях
	Компетентностные	цифровая и финансовая грамотность, навыки защиты устройства, знание схем	восприимчивость	знание схем и навыки защиты снижают риск [11, 20]
Поведенческо-средовой	Поведенческие	интенсивность пользования сервисами, онлайн-покупки, раскрытие данных, кредитное и инвестиционное поведение	подверженность	подтверждено [15, 21, 22]
	Социальные	изоляция, зависимость от помощи других лиц, поддержка семьи, информационная среда	подверженность и восприимчивость (разнонаправленно)	подтверждено частично [11]
Ситуационный	Ситуационные	эмоциональное напряжение, дефицит времени, финансовая нужда, тяжёлые жизненные события	актуализация уязвимости	признаны регуляторами, эмпирически подтверждены частично [16]
Внешние условия	Институционально-технологические	скорость и необратимость переводов, дистанционный кредит, утечки данных, информирование о рисках	усиливают или ослабляют оба компонента	признаны регуляторами, эмпирически изучены слабо [16, 17]

Диспозиционный уровень объединяет относительно устойчивые характеристики личности. Среди психологических факторов наиболее устойчиво подтверждён низкий самоконтроль [19, 20]. Роль возраста зависит от схемы, и это хорошо видно на примере компетентностных факторов в Узбекистане. По данным Всемирного банка, в 2024 году защиту телефона паролем или отпечатком пальца использовали 46,9 % взрослых, а самостоятельно сменить пароль на телефоне могли лишь 33,9 %. Этим навыком владели 39,3 % мужчин и 28,8 % женщин, 45,7 % лиц в возрасте 15–24 лет и 30,4 % лиц старше 25 лет, 26,2 % лиц с начальным образованием и 27,9 % лиц вне рабочей силы. Различий между городом и селом почти нет, 34,3 % против 33,7 % [24]. Исследование пожилых пользователей в Китае показало, что именно ограниченные навыки цифровой защиты повышали вероятность стать жертвой после контакта с мошенником [11]. Сопоставление этих данных позволяет предположить, что в Узбекистане существуют группы с повышенной восприимчивостью, однако это предположение требует проверки на материале уголовных дел и опросов потерпевших.

Поведенческо-средовой уровень включает поведение пользователя и его социальное окружение. Интенсивность пользования сервисами, покупки на

онлайн-площадках, размещение личных данных и интерес к инвестиционным предложениям прежде всего повышают подверженность [21, 22]. Социальные факторы действуют разнонаправленно. Социальная изоляция облегчает преступнику установление контакта, а помощь родственников, напротив, может защищать. В упомянутом китайском исследовании вмешательство младших членов семьи снижало финансовые потери пожилых пользователей [11].

Ситуационный уровень включает состояние лица в момент контакта. Это эмоциональное напряжение, дефицит времени, острая финансовая нужда, недавние жизненные события. Британский регулятор прямо относит тяжёлые жизненные события к источникам уязвимости потребителя [16]. Ситуационный фактор не создаёт уязвимость с нуля, а переводит её из возможности в действительность.

Сопоставление уровней позволяет сформулировать принцип сопряжённости. Значение фактора определяется не им самим, а связкой «фактор, компонент уязвимости, тип схемы». Молодой человек чаще пользуется цифровыми сервисами и потому чаще сталкивается с преступником, но лучше владеет навыками защиты устройства. Пожилой человек реже сталкивается с попытками обмана, но хуже распознаёт их. Поэтому вопрос о том, какая возрастная группа уязвимее, без указания схемы и стадии не имеет однозначного ответа. Этот вывод согласуется с данными систематического обзора о разнонаправленном действии одних и тех же признаков [14].

3. Механизм взаимодействия факторов с криминогенным воздействием

Факторы уязвимости сами по себе не приводят к виктимизации. Виктимизация наступает лишь тогда, когда уязвимость встречается с криминогенным воздействием в конкретной ситуации и в определённой институциональной среде (рисунок 1).

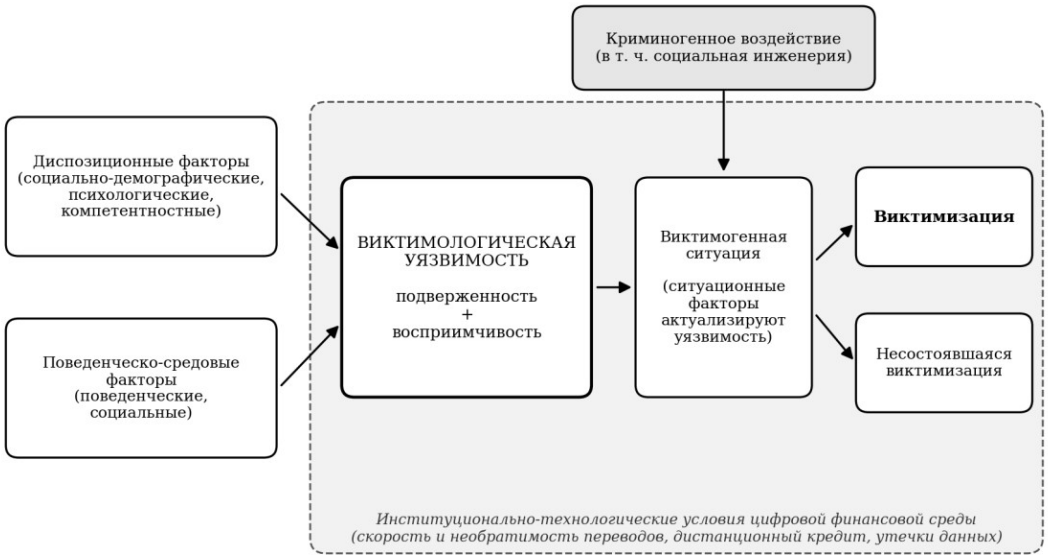


Рисунок 1. Модель виктимологической уязвимости личности в сфере цифровых финансовых технологий (разработано автором)

Социальная инженерия в этой модели занимает место внешнего актуализатора. Типичные сценарии дистанционного мошенничества целенаправленно обращены к разным компонентам уязвимости. Звонок от имени службы безопасности банка о подозрительной операции создаёт ситуационный фактор страха и спешки. Предложение быстрого кредита или высокодоходных инвестиций использует финансовую нужду и особенности финансового поведения. Требование сообщить код подтверждения рассчитано на пробел в компетенциях, при котором человек не понимает, что код равнозначен его подписи. Эти сценарии служат здесь контекстом, в котором проявляется уже существующая уязвимость.

Важным элементом модели служит несостоявшаяся виктимизация. Большинство людей, столкнувшихся с попыткой обмана, не становятся жертвами [20]. Именно сравнение тех, кто уступил, и тех, кто противостоял воздействию, позволяет выявить реальные факторы восприимчивости. Модель показывает и границы ответственности потерпевшего. Даже при высокой восприимчивости вред может быть предотвращён, если среда замедляет необратимые операции или предупреждает пользователя о риске. Поэтому часть ответственности за уязвимость лежит на тех, кто проектирует финансовые сервисы.

Национальное законодательство пока не отражает эту специфику. Закон «О профилактике правонарушений» определяет виктимологическую профилактику как деятельность по снижению у конкретного лица риска стать потерпевшим, однако меры, перечисленные в статье 44, ориентированы на традиционную преступность. К ним относятся обучение разрешению межличностных конфликтов, информирование о способах самообороны и контроль мест, где часто совершаются правонарушения [4]. Факторы цифровой финансовой уязвимости в этом перечне не учтены.

Выводы и предложения

Виктимность в цифровой финансовой среде целесообразно конкретизировать через понятие виктимологической уязвимости, понимаемой как соотносительное состояние, образуемое подверженностью преступному воздействию и восприимчивостью к нему. Это состояние актуализируется ситуацией и зависит от институционально-технологических условий. Цифровая финансовая виктимизация отличается тем, что вред причиняется через операцию, которая выглядит для системы как законное распоряжение владельца.

Факторы уязвимости обоснованно группировать по трём уровням, а именно диспозиционному, поведенческо-средовому и ситуационному. Институционально-технологические условия образуют внешнюю по отношению к личности группу, а криминогенное воздействие выступает не фактором уязвимости, а её актуализатором. Значение каждого фактора определяется его связью с компонентом уязвимости и типом схемы. Устойчиво подтверждена роль низкого самоконтроля и знания схем, тогда как роль общей доверчивости, возраста и образования неоднозначна.

Научный вклад работы состоит в уточнении понятия виктимологической уязвимости для цифровой финансовой среды, в построении типологии факторов на едином основании и в обосновании принципа сопряжённости. На национальном материале показано, что рост доли мошенничеств среди ИТ-преступлений повышает значение восприимчивости потерпевшего, а базовые навыки цифровой защиты распределены среди населения неравномерно.

Перечень мер виктимологической профилактики в статье 44 Закона «О профилактике правонарушений» требует дополнения мерами, учитывающими цифровые финансовые риски. Содержание таких мер составит предмет дальнейшего исследования, посвящённого виктимологической профилактике и формированию цифровой гигиены населения. Перспективным направлением является также эмпирическая проверка предложенной модели на материалах уголовных дел и опросах потерпевших.

Список использованной литературы

1. Бобровничий И. Н., Тайбаков А. А. Виктимологические особенности хищений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации // Социология и право. 2025. Т. 17, № 2. С. 243–260. DOI: 10.35854/2219-6242-2025-2-243-260.
2. Жмуров Д. В. Факторы кибервиктимизации // Академический юридический журнал. 2021. Т. 22, № 3 (85). С. 268–276. DOI: 10.17150/1819-0928.2021.22(3).268-276.
3. Майоров А. В. Виктимология цифровой преступности: концепция научного направления // Виктимология. 2024. Т. 11, № 1. С. 7–12. DOI: 10.47475/2411-0590-2024-11-1-7-12.
4. О профилактике правонарушений: Закон Республики Узбекистан от 14 мая 2014 г. № ЗРУ-371 // Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz/docs/2387359 (дата обращения: 24.09.2026).
5. Ривман Д. В. Криминальная виктимология. СПб.: Питер, 2002. 304 с.
6. Сведения о преступлениях, совершённых с использованием информационных технологий, и о мошенничестве за 2024 г., 2025 г. и январь – август 2026 г.: ведомственная статистическая отчётность Министерства внутренних дел Республики Узбекистан. Ташкент, 2025–2026.
7. Социально-экономическое положение Республики Узбекистан. Раздел XVII. Правонарушения (январь – декабрь 2024 г.). Ташкент: Агентство статистики при Президенте Республики Узбекистан, 2025. С. 427–445.
8. Уголовный кодекс Республики Узбекистан: утверждён Законом Республики Узбекистан от 22 сентября 1994 г. № 2012-XII // Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz/docs/111457 (дата обращения: 24.09.2026).
9. Франк Л. В. Виктимология и виктимность. Душанбе: Ирфон, 1972. 49 с.
10. Центральный банк призывает остерегаться мошенников // Центральный банк Республики Узбекистан: официальный сайт. 2020. URL: https://cbu.uz/ru/press_center/news/425175/ (дата обращения: 24.09.2026).
11. Chen H., He M., Xu X., Atkin D. Examining older adults' vulnerability to online health scams: insights from routine activity theory // Frontiers in Public Health. 2025. Vol. 13. Art. 1585851. DOI: 10.3389/fpubh.2025.1585851.
12. Cohen L. E., Felson M. Social Change and Crime Rate Trends: A Routine Activity Approach // American Sociological Review. 1979. Vol. 44, № 4. P. 588–608. DOI: 10.2307/2094589.
13. Cross C. No laughing matter: Blaming the victim of online fraud // International Review of Victimology. 2015. Vol. 21, № 2. P. 187–204. DOI: 10.1177/0269758015571471.

14. Dadà C. B., Colautti L., Rosi A., Cavallini E., Antonietti A., Iannello P. Uncovering vulnerability to fraud and scams among adult victims in online and offline contexts: A systematic review // Computers in Human Behavior. 2025. Vol. 172. Art. 108734. DOI: 10.1016/j.chb.2025.108734.
15. Emami C., Smith R. G., Jorna P. Online fraud victimisation in Australia: Risks and protective factors. Research Report № 16. Canberra: Australian Institute of Criminology, 2019. DOI: 10.52922/rr09319.
16. Financial Conduct Authority. Guidance for firms on the fair treatment of vulnerable customers (FG21/1). London: FCA, 2021. URL: https://www.fca.org.uk/publication/finalised-guidance/fg21-1.pdf (дата обращения: 24.09.2026).
17. G20/OECD High-Level Principles on Financial Consumer Protection 2022. Paris: OECD Publishing, 2022. DOI: 10.1787/48cc3df0-en.
18. Hentig H. von. The Criminal and His Victim: Studies in the Sociobiology of Crime. New Haven: Yale University Press, 1948.
19. Holtfreter K., Reisig M. D., Pratt T. C. Low self-control, routine activities, and fraud victimization // Criminology. 2008. Vol. 46, № 1. P. 189–220. DOI: 10.1111/j.1745-9125.2008.00101.x.
20. Koning L., Junger M., Veldkamp B. Risk factors for fraud victimization: The role of socio-demographics, personality, mental, general, and cognitive health, activities, and fraud knowledge // International Review of Victimology. 2024. Vol. 30, № 3. P. 443–479. DOI: 10.1177/02697580231215839.
21. Leukfeldt E. R., Yar M. Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis // Deviant Behavior. 2016. Vol. 37, № 3. P. 263–280. DOI: 10.1080/01639625.2015.1012409.
22. Pratt T. C., Holtfreter K., Reisig M. D. Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory // Journal of Research in Crime and Delinquency. 2010. Vol. 47, № 3. P. 267–296. DOI: 10.1177/0022427810365903.
23. Whitty M. T. Predicting susceptibility to cyber-fraud victimhood // Journal of Financial Crime. 2019. Vol. 26, № 1. P. 277–292. DOI: 10.1108/JFC-10-2017-0095.
24. World Bank. The Global Findex Database 2025: Connectivity and Financial Inclusion in the Digital Economy. Washington, DC: World Bank, 2025. URL: https://www.worldbank.org/en/publication/globalfindex/download-data (дата обращения: 24.09.2026).

MUNDARIJA

Kirish so‘zi.....**3**

1. Нигматов Руфтулло Олимджонович – “Основные характеристики британской модели предупреждения преступности”.....**5**

2. Матчанов Алимжан Атабаевич – “Кибержиноятчиликни криминологик прогнозлаш ва унинг олдини олишда ички ишлар органлари фаолиятини такомиллаштириш”.....**12**

3. Xudoyberdiyev Ahror Qosimaliyevich – “O‘zbekistonda huquqbuzarliklarning oldini olishda aholi huquqiy ongi va madaniyatini oshirish istiqbollari”.....**17**

4. Хужакулов Сиёвуш Бахтиёрович – “Криминологик диагностика ва прогнозлашда рақамли технологиялардан фойдаланиш”.....**20**

5. Сирлиев Бахтиёр Назарович – “Криминологические и психологические основания подготовки кадров органов внутренних дел: практическая модель предупреждения служебной делинквентности”.....**27**

6. Ummatov Muhammadrasul Tursunovich – “O‘zbekiston Respublikasida jamoat xavfsizligini ta’minlashning konstitutsiyaviy-huquqiy asoslari va uning qonunchilik tizimidagi o‘rni”.....**32**

7. Musayev Djamaliddin Kamalovich – “Giyohvandlik vositalarining noqonuniy muomalasiga qarshi kurashishda xalqaro-huquqiy hamkorlik”.....**37**

8. Пайзиев Дилшат Юлдашбаевич – “Навоий вилоятида жиноятчилик тенденциялари ва криминоген вазиятнинг ўзига хос хусусиятлари”.....**43**

9. Hasanov Sharofiddin Shamshurovich – “Raqamli makonda kiberjinoyatchilik: kriminologik tahlil va profilaktikaning zamonaviy mexanizmlari”.....**48**

10. Umirzakov Begzod Ataboevich – “Kriminologik bilimlarni huquqni muhofaza qilish faoliyatiga joriy etish: muammolar va samaradorlikni oshirish yo‘llari”.....**54**

11. Saitqulov Qodirali Abdisalimovich – “Ekologiya sohasidagi jinoyatlarning kriminologik tavsifi va oldini olishning zamonaviy mexanizmlari”.....**59**

12. Abdullayev Sardorbek Usmonxudjayevich – “Kriminogen xulq-atvor profilaktikasida psixologik diagnostika va individual ta’sir mexanizmlarining integratsiyasi” **64**

13. Ирисбеков Улуғбек Асқарбекович – “Уюшган жиноятчиликнинг замонавий криминологик тавсифи ва унга қарши курашишнинг самарали механизмлари” **70**

14. To‘raev Ilhomjon Esanovich – “Internet tarmog‘ida giyohvandlik vositalarining noqonuniy muomalasiga qarshi kurashishning zamonaviy usullari” **78**

15. To‘xtashev Hikmatilla Ismatillayevich – “Ekologik huquqbuzarliklarning oldini olishda ruxsat berish va litsenziyalash mexanizmlarining kriminologik ahamiyati” **84**

16. Исаев Сардор Алишерович – “Ишсизлар томонидан содир этиладиган жиноятларнинг криминологик тавсифи ва профилактикаси”.....**95**

17. Aslanov Bobur Tuxtayevich – “Uyushgan jinoyatchilik latentligini aniqlashning zamonaviy kriminologik yondoshuvlari va uni milliy tizimga joriy etish”.....**108**

18. Turaxodjayev Najmiddin Sadirovich – “Huquqni muhofaza qiluvchi organlarning masofaviy axborot almashish tizimlarida ma’lumot hayotiy sikli va boshqaruv konturi”.....**113**
19. Шодиев Абдукарим Абдурахмонович – “Янги Ўзбекистонда жазони ижро этиш тизимида амалга оширилаётган ислоҳотларнинг амалий натижалари”.....**119**
20. Тиллаходжаев Баҳодир Абдуллахонович – “Синтетик гиёҳвандлик воситалари ноқонуний айланмасининг олдини олиш: ички ишлар органлари фаолиятининг замонавий криминологик модели”.....**123**
21. Джурабаев Рустам Тураббоевич – “Қидирувдаги шахсларни аниқлаш ва ушлашни криминологик таъминлашнинг замонавий йўналишлари”.....**129**
22. Allayorov Djura Xaykalovich – “Zamonaviy rahbar faoliyatida hissiy holatlarni o‘rni” **134**
23. Choriyev Mirsardor Abdimo’min o’g’li – “Ijtimoiy-iqtisodiy hayot liberallashishi jarayonining jinoyatchilikka ta’siri haqidagi mushohadalar” **138**
24. Исаков Лутфуллохон Карамат угли– “Виктимологические факторы уязвимости личности в сфере цифровых финансовых технологий” **148**
25. Хамидов Асилбек Алишер ўғли – “Ўзбекистон Республикасида киберфирибгарлик жиноятларига қарши курашишнинг ҳуқуқий асослари: замонавий ҳолат ва такомиллаштириш йўналишлари” **159**
26. Убайдуллаева Дилноза Акмаловна – “Болаларни зўравонликнинг барча шаклларидан ҳимоя қилиш: ҳуқуқий ислоҳотлар ва илмий-назарий таҳлили” **167**
27. Ешмуратов Шерали Бахитович – “Ички ишлар органлари фаолиятида вояга етмаганлар томонидан содир этилган ҳуқуқбузарликларни олдини олишнинг криминологик чоралари” **172**
28. Tursunov Akramjon Baxodirjon o‘g‘li – “Mahkumlar huquqlarini ta’minlashda ozodlikdan mahrum qilish jazosini ijro etuvchi jazoni ijro etish muassasalari xodimlarining huquqiy maqomini takomillashtirish” **177**
29.Samiyev Mironshoh Saloxiddin o‘g‘li – “Raqamli iqtisodiyot sharoitida virtual pul o‘tkazmalari va kriptovalyutadan foydalanish bilan bog‘liq jinoyatchilikning kriminologik xususiyatlari” **184**
30. Латипов Элдор Икромович – “Гиёҳвандлик воситалари, психотроп моддалар ва уларнинг аналоглари билан қонунга хилоф муомала қилишда қидирувдаги шахсларни аниқлашнинг замонавий криминологик жиҳатлари” **190**
31. Чориев Анвар Қўзиевич – “Шахсга доир маълумотлар тўғрисидаги қонунчиликни бузиш жиноятининг объектив белгилари” **196**
32. Тошқулов Ғайрат Эркабаевич – “Рақамлаштириш шароитида холислар институтини такомиллаштириш: криминоген хавфлар ва уларни бартараф этиш механизмлари” **202**
33. Kutlimuratov Maxmudjon Sharipbayevich – “Qoraqalpog‘iston Respublikasi mahallalarida kriminogen xavfni baholash va manzilli profilaktikani takomillashtirish” **207**
34. Султанов Даврон Иброхимович – “Самарқанд вилоятидаги “қизил” тоифадаги маҳаллаларда жиноятчилик профилактикаси: илмий-манзилли ёндашув” **216**

35. Jurayev Zoxidjon Ashurovich – “O‘g‘irlik jinoyatchiligining kriminologik tavsifi va zamonaviy tendensiyalari” **225**
36. Салимова Дилноза Илҳам қизи – “Электрон тўлов воситалари орқали содир этиладиган фирибгарлик учун жиноий жавобгарлик: жиноят таркиби таҳлили ва қонунчиликни такомиллаштириш муаммолари” **231**
37. Qo‘chqarova Sarvinoz Vahob qizi – “Voyaga yetmaganlar o‘rtasida nazoratsizlik va huquqbuzarliklar profilaktikasini tashkil etish: huquqiy-kriminologik tahlil” **238**
38. Allambayev Javlonbek Rustamovich – “Raqamli texnologiyalar sharoitida bojxona rejimlari bilan bog‘liq ma’muriy huquqbuzarliklar to‘g‘risidagi ishlarni yuritishning ayrim masalalari” **242**
39. Radjapova Lola Nuriddinovna – “Ichki ishlar organlari xodimlarining ijtimoiy kafolatlari: xorijiy tajriba va milliy qonunchilikni takomillashtirish istiqbollari” **245**
40. Абдухошимов Исмоил Абдуғани ўғли – “Совға ва пора ўртасидаги ҳуқуқий чегара: сифат мезонидан миқдорий мезонга ўтиш” **249**
41. Nurullaeva Laylo Xayrulloevna – “Raqamli muhitda gender asosidagi kiberzo‘ravonlik: sextortion va intim materiallarni roziliksiz tarqatishning kriminologik xususiyatlari va profilaktika mexanizmlari” **253**
42. Boliyev Umar Usmonovich – “Jinoyatchilikning oldini olish va unga qarshi kurashishning samarali mexanizmlarini takomillashtirish” **266**
43. Ниматов Шерзод Ниматжонович – “Вояга етмаганлар томонидан содир этиладиган ўғирликлар профилактикасида рақамли технологияларни қўллашнинг амалий механизми” **274**
44. Кодиркулов Ануш Саидкулович – “Криминологические аспекты обеспечения безопасности в киберпространстве: от теоретического анализа детерминант к практике предупреждения” **279**
45. Urinkulov Odiljon Naziraliyevich – “Ko‘p manbali ma’lumotlar asosida kiberfiribgarliklarni aniqlash usullari” **283**
46. Atajanov O‘tkir Mamatsalayevich – “Mahallada xavfga yo‘naltirilgan profilaktika: empirik tahlil asosida raqamli xavfsizlik profilini shakllantirish” **290**
47. Adxamov Zafar Akbarovich – “Ilgari sudlangan shaxslar o‘rtasida huquqbuzarliklarning yakka tartibdagi profilaktikasining nazariy-huquqiy asoslari” **299**
48. Shermatova Nazokat Safarovna – “Kursantlarning kasbiy-psixologik tayyorgarligini takomillashtirishda fan, ta’lim va huquqni muhofaza qilish amaliyoti integratsiyasi” **308**
49. Mannonov Avazbek Mirzanazarovich – “Jinoyatga oid arizalar, xabarlar va boshqa ma’lumotlarni ko‘rib chiqishni raqamlashtirish: muammo va yechimlar” **313**
50. Abdumalikov Alisher Abdulazizovich – “Voyaga yetmaganlar tomonidan sodir etiladigan jinoyatlarning oldini olishda hamkorlikni tashkil etish: muammo va yechimlar” **319**

Kriminologiyaning dolzarb masalalari: Respublika ilmiy-amaliy konferensiyasi materiallari to‘plami (2026-yil 25-sentyabr). – T.: O‘zbekiston Respublikasi Kriminologiya tadqiqot instituti, 2026. – 332 b.

Muharrirlar: B.A. Yarov, D.B. Mamarajabova
Texnik muharrir: Z.M. Oxunov

O‘zbekiston Respublikasi Kriminologiya tadqiqot instituti,
100187, Tos’hkent s’h., Buyuk ipak yo‘li ko‘chasi, 243.