СОЦИАЛЬНЫЕ ФАКТОРЫ РАСПРОСТРАНЕНИЯ ОНЛАЙН-МОШЕННИЧЕСТВА

Тургунова Дурдона
студентка 3 курса
Андижанский государственный университет
Республика Узбекистан

Аннотация: *В статье исследуются социальные факторы, определяющие распространение онлайн-мошенничества в современных условиях цифровизации общества. На основе анализа отечественной и зарубежной научной литературы, данных виктимологических обследований и эмпирических исследований рассматриваются социально-демографические характеристики жертв, механизмы социального доверия и его эксплуатации, роль социального неравенства, цифровой грамотности и сетевых структур в формировании уязвимости населения. Особое внимание уделяется феноменам социальной инженерии, эрозии институционального доверия и влиянию медиасреды на виктимизацию. Анализируются теоретические объяснительные модели — теория рутинной деятельности, теория рационального выбора, концепция социального капитала — применительно к онлайн-мошенничеству. Обосновывается необходимость социально ориентированных мер профилактики, выходящих за рамки технических решений.*

Ключевые слова: *онлайн-мошенничество, социальные факторы, виктимология, социальная инженерия, цифровое неравенство, доверие, социальный капитал, интернет-преступность, медиаграмотность, профилактика мошенничества.*

SOCIAL FACTORS IN THE SPREAD OF ONLINE FRAUD

Turgunova Durdona
3rd-year student
Andijan State University
Republic of Uzbekistan

Abstract: *The article examines the social factors that determine the spread of online fraud in the context of the digitalization of modern society. Drawing on domestic and international scholarly literature, victimization survey data, and empirical research, the study analyzes the socio-demographic characteristics of victims, the mechanisms of social trust and its exploitation, and the role of social inequality, digital literacy,*

and network structures in shaping population vulnerability. Special attention is given to the phenomena of social engineering, the erosion of institutional trust, and the influence of the media environment on victimization. Theoretical explanatory models — routine activity theory, rational choice theory, and the concept of social capital — are analyzed in relation to online fraud. The necessity of socially oriented preventive measures that go beyond technical solutions is substantiated.

Keywords: *online fraud, social factors, victimology, social engineering, digital inequality, trust, social capital, internet crime, media literacy, fraud prevention.*

Онлайн-мошенничество является одной из наиболее динамично развивающихся форм противоправного поведения в современном обществе. По данным российских правоохранительных органов, число зарегистрированных преступлений в сфере информационных технологий за последние пять лет выросло более чем в три раза, при этом мошенничество составляет наибольшую долю в структуре киберпреступности [1, с. 54]. Вместе с тем технологические интерпретации этого явления, доминировавшие в научной и управленческой дискуссии на протяжении двух десятилетий, все более очевидно обнаруживают свою недостаточность: ни совершенствование программного обеспечения, ни ужесточение законодательства сами по себе не останавливают рост числа жертв. Это переключает внимание исследователей на социальные измерения проблемы — те характеристики общества, социальных групп и межличностных взаимодействий, которые делают онлайн-мошенничество не только технически возможным, но и социально воспроизводимым явлением.

Онлайн-мошенничество как социальный феномен представляет собой форму обмана, осуществляемую посредством цифровых коммуникаций с целью незаконного извлечения материальной или иной выгоды за счет жертвы. К его основным разновидностям относятся: фишинг и спир-фишинг, романтическое мошенничество, инвестиционные схемы, мошенничество с технической поддержкой, мошенничество на торговых площадках, а также компрометация деловой электронной почты. Каждая из этих разновидностей эксплуатирует специфические социально-психологические механизмы и предполагает определенный социальный профиль жертвы [2, с. 45].

Широко распространенный в обыденном сознании образ жертвы онлайн-мошенничества как человека пожилого, технологически неграмотного и социально изолированного не выдерживает критики при обращении к эмпирическим данным. Исследования последних лет демонстрируют

значительно более сложную картину социально-демографического распределения виктимизации. Действительно, пожилые люди непропорционально часто становятся жертвами ряда схем, однако в целом ряде категорий наиболее уязвимыми оказываются люди среднего и молодого возраста с высоким уровнем образования и активным присутствием в цифровой среде [4, с. 34].

Этот парадокс находит объяснение в концепции «уверенности в своих компетенциях» (overconfidence bias): образованные пользователи нередко переоценивают собственную способность распознать мошенничество, что снижает их бдительность именно в тех ситуациях, когда мошенники применяют более изощренные методы воздействия. Российские социологические исследования фиксируют, что молодежь в возрасте 18–24 лет сообщает о финансовых потерях от онлайн-мошенничества не реже, чем представители старших возрастных групп, хотя суммы ущерба для пожилых жертв в среднем выше [10, с. 78].

Центральным социальным механизмом, на котором паразитирует онлайн-мошенничество, является доверие — фундаментальный ресурс социального взаимодействия. В условиях цифровой экономики доверие приобретает новые формы и функции: оно должно распространяться на анонимных участников транзакций, незнакомые платформы и невидимые технические системы. Этот структурный дефицит сигналов доверия в онлайн-среде создает возможности для манипуляции [9, с. 90].

Мошенники эксплуатируют как межличностное доверие, так и институциональное. Техника имперсонации — выдавание себя за представителя банка, государственного органа или известной компании — эксплуатирует доверие к легитимным институтам. Социальная инженерия является ключевым инструментом онлайн-мошенников. С социологической точки зрения важно, что эти техники не являются «взломом» индивидуальной психики — они эксплуатируют нормативные ожидания и социально одобряемые ценности [7, с. 43].

Одним из ключевых социологически значимых факторов распространения онлайн-мошенничества является социальное неравенство, действующее через несколько взаимосвязанных каналов. Во-первых, существует прямая связь между материальной нуждой и уязвимостью к мошенническим схемам, обещающим быстрое обогащение. Во-вторых, неравенство в распределении цифровых компетенций непосредственно влияет на способность распознавать мошеннические схемы. В-третьих, социальное неравенство связано с неравным

доступом к правосудию и институциональной защите в случае виктимизации [6, с. 5].

Концепция социального капитала открывает дополнительное измерение для понимания уязвимости к онлайн-мошенничеству. Социальный капитал может как снижать, так и повышать риск виктимизации. С одной стороны, включенность в плотные доверительные сети обеспечивает информационные потоки, позволяющие распознавать мошеннические схемы. С другой стороны, именно социальные связи являются каналом распространения мошенничества: пирамидальные схемы вербуют новых жертв через существующие отношения доверия [5, с. 20].

Феномен «мошенничества через доверенные связи» заслуживает отдельного рассмотрения. Исследования зафиксировали устойчивую тенденцию к использованию существующих социальных сетей для распространения мошеннических схем: жертва убеждает своих знакомых и родственников присоединиться, искренне веря в легитимность предложения. Этот механизм превращает жертву одновременно в соучастника распространения мошенничества, что порождает дополнительные психологические травмы [3, с. 480].

Роль одиночества и социальной изоляции в формировании уязвимости к онлайн-мошенничеству подтверждена целым рядом отечественных и зарубежных исследований. Романтическое мошенничество паразитирует на потребности жертв в близости и признании. Пандемия COVID-19 обострила эту уязвимость: условия социальной изоляции, вынудившие людей переносить межличностное общение в онлайн-пространство, сопровождались резким ростом романтического мошенничества [2, с. 50].

Теория рутинной деятельности была адаптирована для объяснения онлайн-мошенничества. Согласно ей, виктимизация происходит при совпадении трех условий: наличии мотивированного правонарушителя, подходящей мишени и отсутствии дееспособного контроля. В цифровом контексте интенсивность онлайн-активности является аналогом «рутинного перемещения» в физическом пространстве: чем больше времени человек проводит на торговых площадках и в социальных сетях, тем выше статистически его подверженность мошеннической виктимизации [3, с. 481].

Стигматизация жертв онлайн-мошенничества является одним из наименее изученных, но социально значимых факторов его воспроизводства в российском контексте. Общественное восприятие жертвы как человека «наивного» или «жадного» создает мощный барьер для обращения в правоохранительные

органы. Исследования показывают, что значительная часть жертв испытывает стыд и самообвинение, нередко более травматичные, чем сам материальный ущерб [10, с. 82].

Медиасреда играет двойственную роль в контексте онлайн-мошенничества. С одной стороны, традиционные и цифровые медиа являются важнейшим каналом информирования населения о новых схемах. С другой — медийные представления о мошенничестве нередко воспроизводят стереотипы, занижающие риск для «образованной» и «современной» аудитории. Транснациональное измерение онлайн-мошенничества является принципиальным социальным фактором его воспроизводства: значительная часть операций организована в странах с низким уровнем правоприменения [8, с. 321].

Меры противодействия онлайн-мошенничеству, исходящие из социологического понимания проблемы, существенно отличаются от узкотехнических подходов. Прежде всего, они предполагают адресность: программы просветительской работы должны учитывать специфику уязвимости разных социальных групп, не воспроизводя стереотипы о «типичной жертве». Де-стигматизация виктимизации является ключевым условием повышения уровня информирования о преступлениях. Роль сообществ взаимопомощи в профилактике остается недооцененной в отечественной практике [9, с. 94].

Подводя итог, можно констатировать, что онлайн-мошенничество является глубоко социальным явлением, коренящимся в фундаментальных характеристиках современного общества: его информационной асимметрии, структурах социального доверия и неравенства, культурных нормах и динамике цифровых сетей. Технические меры защиты необходимы, но недостаточны: они не устраняют социальных условий, воспроизводящих уязвимость. Эффективная стратегия противодействия должна включать развитие цифровых компетенций как элемента социальной политики в области образования, системную работу по укреплению институционального доверия и де-стигматизации виктимизации, регулирование платформенных алгоритмов и международное сотрудничество [1, с. 58].

СПИСОК ЛИТЕРАТУРЫ

1. Лукацкий А. В. Мифы и правда о киберпреступности: социологическое измерение // Вопросы кибербезопасности. — 2015. — № 2 (10). — С. 52–61. — URL: https://cyberleninka.ru/article/n/mify-i-pravda-o-kiberprestupnosti-sotsiologicheskoe-izmerenie

2. Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. — 2012. — № 1 (24). — С. 45–55. — URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnaya-ugroza

3. Осипенко А. Л. Сетевая компьютерная преступность: теория и практика борьбы. — Омск: Омская академия МВД России, 2009. — 480 с. — URL: https://elibrary.ru/item.asp?id=19567234 (дата обращения: 11.03.2024).

4. Богомолова С. Н. Виктимологические аспекты мошенничества в сфере компьютерных технологий // Российский следователь. — 2018. — № 5. — С. 34–39. — URL: https://elibrary.ru/item.asp?id=32867541

5. Ефремова М. А. Уголовная ответственность за мошенничество в сфере компьютерной информации // Информационное право. — 2016. — № 3. — С. 18–22. — URL: https://cyberleninka.ru/article/n/ugolovnaya-otvetstvennost-za-moshennichestvo-v-sfere-kompyuternoy-informatsii

6. Тихомиров Ю. А. Право и цифровое неравенство // Журнал российского права. — 2019. — № 1. — С. 5–14. — URL: https://cyberleninka.ru/article/n/pravo-i-tsifrovoe-neravenstvo

7. Иванов Н. Г. Социальная инженерия как инструмент киберпреступности // Вопросы кибербезопасности. — 2017. — № 3 (21). — С. 41–47. — URL: https://cyberleninka.ru/article/n/sotsialnaya-inzheneriya-kak-instrument-kiberprestupnosti

8. Авдийский В. И. Теневая экономика и экономическая безопасность государства. — М.: Альфа-М, 2016. — 496 с. — URL: https://elibrary.ru/item.asp?id=25843210

9. Поляков В. В. Доверие в цифровую эпоху: социологический анализ // Социологические исследования. — 2019. — № 7. — С. 89–98. — URL: https://cyberleninka.ru/article/n/doverie-v-tsifrovuyu-epohu-sotsiologicheskiy-analiz

10. Смирнова И. Н. Социальные факторы виктимизации в онлайн-пространстве // Юридическая наука и правоохранительная практика. — 2019. — № 3 (49). — С. 77–85. — URL: https://cyberleninka.ru/article/n/sotsialnye-faktory-viktimizatsii-v-onlayn-prostranstve