ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-6

СОЦИОЛОГИЧЕСКИЕ МЕТОДЫ ИССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Тургунова Дурдона
студентка 3 курса
Андижанский государственный университет
Республика Узбекистан

Аннотация: В статье рассматриваются социологические методы исследования киберпреступлений как самостоятельная и развивающаяся область научного знания на пересечении социологии, криминологии и информационных технологий. Анализируются количественные и качественные подходы к изучению киберпреступности, специфика применения опросных методов, контент-анализа, этнографии виртуальных пространств, а также возможности больших данных и цифровой аналитики. Особое внимание уделяется методологическим вызовам, связанным с латентностью киберпреступлений, анонимностью цифровой среды и трансграничным характером противоправных действий. Показано, что эффективное социологическое исследование киберпреступности требует методологического плюрализма и межотраслевой кооперации. Рассмотрен международный и отечественный опыт эмпирических исследований в данной области, выявлены перспективные направления развития методологического инструментария.

Ключевые слова: киберпреступность, социологические методы, криминология, виктимологические опросы, контент-анализ, цифровая этнография, большие данные, латентность преступлений, информационная безопасность, интернет-девиантность.

SOCIOLOGICAL METHODS OF CYBERCRIME RESEARCH

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

Abstract: The article examines sociological methods of cybercrime research as an independent and developing field of academic knowledge at the intersection of sociology, criminology, and information technologies. It analyses quantitative and qualitative approaches to the study of cybercrime, the specifics of survey methods, content analysis, ethnography of virtual spaces, as well as the possibilities of big data and digital analytics. Special attention is paid to methodological challenges associated with the latency of cybercrimes, the anonymity of the digital environment, and the transboundary nature of criminal activities. It is demonstrated that effective sociological research into cybercrime requires methodological pluralism and inter-sectoral cooperation. International and domestic empirical research experience in this field is reviewed, and promising directions for the development of methodological tools are identified.

Keywords: cybercrime, sociological methods, criminology, victimization surveys, content analysis, digital ethnography, big data, crime latency, information security, internet deviance.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-6

Киберпреступность как социальный феномен возникла одновременно с массовым распространением цифровых технологий и глобальных коммуникационных сетей. Уже к концу 1990-х годов исследователи зафиксировали устойчивую тенденцию к миграции традиционных форм противоправного поведения в цифровое пространство, а вместе с тем — появление принципиально новых видов преступлений, не имеющих аналогов в доцифровую эпоху [1, с. 8]. Хакерские атаки, онлайн-мошенничество, кража персональных данных, распространение вредоносного программного обеспечения, кибербуллинг, торговля запрещенными веществами и оружием в темной паутине — все это образует сложный и динамично изменяющийся объект научного познания, требующий адекватного методологического инструментария.

Социология обратилась к проблематике киберпреступности позднее, чем правовые дисциплины или компьютерные науки, однако именно социологический ракурс позволяет раскрыть социальные детерминанты, механизмы воспроизводства и общественные последствия данного явления. Если криминалистика изучает следы преступлений, а информационная безопасность — технические уязвимости, то социология ставит иные вопросы: кто и почему совершает киберпреступления, какие социальные группы несут наибольшие риски виктимизации, каким образом общество реагирует на новые формы девиации и как трансформируются социальные нормы в цифровой среде [2, с. 47].

Методологическое своеобразие социологического исследования киберпреступлений определяется рядом фундаментальных особенностей объекта. Прежде всего, это высочайший уровень латентности: подавляющая часть киберпреступлений не регистрируется официальной статистикой либо потому, что жертвы не осознают факта виктимизации, либо потому, что не сообщают о ней в правоохранительные органы из соображений репутации, недоверия к институтам или убежденности в бесперспективности жалобы. По оценкам ряда исследований, официальная статистика отражает не более 10–15% реального объема киберпреступности [7, с. 112]. Это делает административные данные заведомо недостаточным источником и выдвигает на первый план прямые социологические методы сбора информации.

Вторая принципиальная особенность — анонимность и псевдонимность цифровой среды, которая затрудняет как изучение правонарушителей, так и выявление жертв. Исследователь, работающий в физическом пространстве, может наблюдать за поведением людей, проводить интервью, формировать выборки на основе социально-демографических характеристик. В киберпространстве идентичность пользователя конструируется им самостоятельно и может кардинально расходиться с реальными характеристиками личности. Это создает серьезные проблемы верификации данных и репрезентативности выборок при онлайн-опросах [3, с. 512].

Третья особенность — трансграничность киберпреступлений. Преступник, жертва, серверная инфраструктура и финансовые потоки могут располагаться в разных юрисдикциях. С социологической точки зрения это означает необходимость кросс-национального дизайна исследований, сопоставления данных из разных правовых и культурных контекстов, что требует унифицированных операциональных определений и методологических стандартов [4, с. 14].

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-6

Среди количественных методов ведущее место в социологии киберпреступности занимают виктимологические опросы — специализированные или включенные в более широкие социальные обследования анкетирования, направленные на выявление фактов виктимизации в цифровой среде. Российские исследования в этой области демонстрируют, что уровень осведомленности населения о киберрисках существенно дифференцирован в зависимости от возраста, образования и типа населенного пункта [7, с. 113]. Молодежные когорты демонстрируют более высокий уровень цифровой грамотности, однако одновременно — и более интенсивное присутствие в онлайн-средах, сопряженных с повышенным риском.

Методология виктимологических опросов в сфере киберпреступности сталкивается с рядом специфических проблем. Ключевая из них — проблема определения и однозначной операционализации объекта. В отличие от кражи кошелька или физического насилия, границы «киберпреступления» для обычного респондента размыты: является ли спам-письмо с мошеннической ссылкой, на которую он не кликнул, попыткой преступления? Считать ли взлом аккаунта в социальной сети виктимизацией, если денежного ущерба не последовало? Различные операциональные определения в разных исследованиях существенно затрудняют сопоставление данных [10, с. 130].

Помимо виктимологических обследований, важным количественным инструментом являются самоотчетные исследования (self-report studies), в которых респонденты сообщают о совершенных ими самими правонарушениях. Этот метод адаптирован для изучения онлайн-девиантности, включая несанкционированный доступ к информационным системам, пиратство, кибербуллинг и торговлю в даркнете. Самоотчетные исследования позволяют преодолеть ограничения официальной статистики и виктимологических данных, однако неизбежно страдают от эффекта социальной желательности — занижения признаний в противоправном поведении [8, с. 315].

Качественные методы образуют не менее значимый сегмент методологического арсенала социологии киберпреступности. Глубинные интервью с жертвами киберпреступлений позволяют реконструировать субъективный опыт виктимизации, выявить механизмы принятия решений — в том числе о нераскрытии информации о преступлении, — а также изучить стратегии совладания с последствиями. Исследование правонарушителей с применением качественных методов сопряжено с очевидными этическими и практическими сложностями. Тем не менее в литературе накоплен значительный корпус работ, основанных на интервью с осужденными или бывшими участниками хакерских группировок [8, с. 316].

Этнографические методы применительно к киберпространству трансформировались в самостоятельное исследовательское направление — цифровую этнографию. Исследователи проводят длительное наблюдение за форумами даркнета, чат-каналами и другими площадками, на которых осуществляется координация противоправной деятельности, фиксируют нормы, ритуалы, иерархии и механизмы доверия внутри нелегальных сообществ. Цифровая этнография сопряжена с острыми этическими дилеммами, касающимися информированного согласия и допустимости внедрения исследователя [5, с. 67].

Контент-анализ применяется в социологии киберпреступности преимущественно в двух направлениях. Первое — анализ медиадискурса о киберпреступности: как средства массовой информации конструируют образ киберпреступника и жертвы, какие нарративы доминируют в публичном пространстве. Второе направление — анализ самого цифрового контента

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-6

противоправного характера: сообщений на хакерских форумах, объявлений на нелегальных торговых площадках, публикаций в социальных сетях [6, с. 4].

С развитием вычислительных методов и появлением больших данных контент-анализ претерпевает существенную трансформацию. Автоматизированная обработка больших массивов текстов с применением методов машинного обучения позволяет анализировать миллионы публикаций в реальном времени, выявлять скрытые тематические кластеры, отслеживать динамику нарративов. Большие данные открывают принципиально новые перспективы для социологии киберпреступности, одновременно порождая новые методологические вопросы. Доступ к коммерческим и ведомственным данным, как правило, закрыт для академических исследователей [9, с. 608].

Сетевой анализ занял важное место в изучении организационных структур киберпреступности. Картирование связей между участниками нелегальных онлайн-рынков, хакерских групп и мошеннических сетей позволяет выявлять ключевые узлы, посредников и точки уязвимости, воздействие на которые наиболее эффективно с точки зрения правоохранительной деятельности. Применение смешанных исследовательских стратегий все более утверждается в качестве методологического стандарта: широта охвата и статистическая обобщаемость опросных данных сочетаются с глубиной понимания, достигаемой через интервью [8, с. 318].

Сравнительные исследования занимают особое место в методологии социологии киберпреступности. Кросс-национальные сопоставления позволяют выявить, в какой мере уровень и структура киберпреступности определяются технологическими факторами, а в какой — социокультурными и институциональными. Практическое измерение социологического знания о киберпреступности связано с запросами государственных органов, правоохранительных структур и коммерческих организаций на прикладные исследования. Социологические данные используются при разработке национальных стратегий кибербезопасности, обосновании законодательных изменений и проектировании программ виктимологической поддержки [1, с. 20].

Перспективные направления развития социологической методологии в изучении киберпреступности определяются как технологическими трендами, так и теоретическими лакунами. Развитие искусственного интеллекта, интернета вещей и метавселенных создает новые пространства и формы противоправного поведения, методологически пока слабо освоенные. Методологический прогресс в данной области неотделим от решения вопросов этики исследований. Работа с данными о жертвах преступлений, осужденными, несовершеннолетними участниками онлайн-пространств требует строгого соблюдения принципов конфиденциальности, минимизации рисков и информированного согласия [4, с. 16].

Подводя итог, можно констатировать, что социологические методы исследования киберпреступлений образуют зрелую, хотя и продолжающую активно развиваться методологическую традицию. Количественные методы — виктимологические опросы, самоотчетные исследования, сетевой анализ, методы больших данных — обеспечивают масштаб и обобщаемость результатов. Качественные методы — глубинные интервью, нетнография, контент-анализ — дают глубину понимания, недостижимую количественными средствами. Смешанные исследовательские стратегии позволяют использовать

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

преимущества обоих подходов. Ни один из них, примененный изолированно, не способен дать исчерпывающее представление о столь многомерном явлении, как киберпреступность. Именно методологический плюрализм и межотраслевое сотрудничество определяют будущее этой исследовательской области [2, с. 52].

СПИСОК ЛИТЕРАТУРЫ

1. Лунеев В. В. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы // Труды Института государства и права РАН. — 2018. — № 4. — С. 8–35. — URL: https://cyberleninka.ru/article/n/kiberprestupnost-ponyatie-sostoyanie-ugolovno-pravovye-mery-borby

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. Маслакова Е. А. Понятие и виды киберпреступлений в уголовном праве России и зарубежных стран // Молодой ученый. — 2015. — № 6. — С. 511–513. — URL: https://moluch.ru/archive/86/16354

4. Осипенко А. Л. Новые направления противодействия сетевой преступности // Вестник Воронежского института МВД России. — 2016. — № 3. — С. 14–22. — URL: https://cyberleninka.ru/article/n/novye-napravleniya-protivodeystviya-setevoy-prestupnosti

5. Скородумова О. Б. Социология Интернета: специфика изучения виртуальных сообществ // Вестник Московского государственного университета культуры и искусств. — 2004. — № 2. — С. 67–73. — URL: https://cyberleninka.ru/article/n/sotsiologiya-interneta-spetsifika-izucheniya-virtualnyh-soobschestv

6. Бачило И. Л. О праве на информацию в Российской Федерации // Информационное право. — 2011. — № 3. — С. 3–9. — URL: https://cyberleninka.ru/article/n/o-prave-na-informatsiyu-v-rossiyskoy-federatsii

7. Смирнова И. Н. Латентность киберпреступлений: причины и способы преодоления // Юридическая наука и правоохранительная практика. — 2018. — № 2 (44). — С. 112–119. — URL: https://cyberleninka.ru/article/n/latentnost-kiberprestupleniy-prichiny-i-sposoby-preodoleniya

8. Агапов П. В. Организованная преступность в сфере высоких технологий: криминологический анализ // Всероссийский криминологический журнал. — 2017. — Т. 11, № 2. — С. 315–323. — URL: https://cyberleninka.ru/article/n/organizovannaya-prestupnost-v-sfere-vysokih-tehnologiy-kriminologicheskiy-analiz

9. Красинский В. В. Защита государственного суверенитета. — М.: Норма, 2017. — 608 с. — URL: https://elibrary.ru/item.asp?id=30086421

10. Цымбалюк В. С. Латентность киберпреступлений: методологические аспекты измерения // Криминологический журнал Байкальского государственного университета. — 2017. — Т. 11, № 2. — С. 128–138. — URL: https://cyberleninka.ru/article/n/latentnost-kiberprestupleniy-metodologicheskie-aspekty-izmereniya