

УДК 343.9

От цифровизации и сетевизации к цифровой девиантации в обществе рисков**Комлев Ю.Ю.**

Доктор социологических наук,
профессор кафедры философии, политологии, социологии и психологии
Казанского юридического института МВД России

В статье описаны цифровизация и сетевизация в эпоху постмодерна, в обществе рисков, как факторы цифровой девиантации. На основе содержательного анализа англоязычных источников, интернет-исследований рассмотрены новые формы кибердевиантности и интегративные подходы к их изучению.

Ключевые слова: пандемия коронавируса, цифровизация, сетевизация, эпоха постмодерна, киберпреступность, кибердевиантность, цифровая девиантация социума, цифровая девиантология, интегративный подход.

Все возрастающие риски и неопределенности и, в частности, те, что вызваны пандемией коронавируса, побуждают к осмыслению социальных, технологических проблем девиантации социума в эпоху постмодерна. Социально-медицинская сторона пандемии и массового социального дистанцирования требует специальных исследований, поскольку это предмет самостоятельного социологического анализа. Однако фактом является и то, что развитие глобальной эпидемии повлияло на стремительное вторжение в жизнь современных людей феноменов и эффектов цифровизации. В сфере управления, бизнеса, образования, перешедшей на «удаленку» в срочном порядке, оказались востребованными цифровые технологии. Не стала исключением и криминальная среда. Так, российские банки, в том числе Сбербанк, в условиях пандемии выявляют все новые уловки мошенников с использованием социальной инженерии, чтобы выманить у граждан персональные данные и даже оформить на них кредиты в режиме онлайн [1].

Показателен и собственный опыт автора. Как взволнованный преподаватель, готовясь к очередному вебинару с курсантами КЮИ МВД России, принимаю звонок из Москвы с трогательной заботой о моем банковском депозите. Интеллигентный, взволнованный голос «банковского клерка» сообщает, что злоумышленники попытались проникнуть в мой личный кабинет, и для того, чтобы заблокировать транзакции, голос из далека просит сообщить реквизи-

ты счета. ...Но у меня не открыт личный кабинет в Сбербанке. После этой реплики связь мгновенно прекращается.

Кибержульничество, кибермошенничество и другие преступления в цифровом мире подстерегают многих из нас на каждом шагу, особенно в эту пандемийную пору. Это обстоятельство и побудило автора серии девиантологических работ в ВЭПС и других социологических и юридических журналах еще раз обратиться к теме цифровизации и сетевизации социума и влияния этих глобальных социально-технологических процессов на девиантацию общества все возрастающих рисков.

Действительно, информационные технологии радикально изменили мир постмодерна и жизнь отдельно взятого в нем человека.

С середины прошлого века начинается компьютерная эра. Компьютеры и информационные технологии постоянно совершенствуются, быстро и широко внедряются в многообразную деятельность человека. С развитием Интернета и социальных сетей социум меняется еще быстрее.

В итоге технологических и социальных сдвигов наряду с массой положительных результатов цифровизации человечество столкнулось со все возрастающей кибердевиантностью и киберпреступностью в виртуальном пространстве – новыми глобальными социальными вызовами и рисками. Ответы на них может дать интегративное социально-технологическое знание, которое формируется в новом

предметном поле цифровой девиантологии на стыке социологии, юриспруденции, теории масс-медиа, математики, информационных технологий.

Что в основном характеризует хронологию социально-технологических перемен на рубеже и в первые десятилетия XXI в.?

Во-первых, благодаря техническому и технологическому прогрессу к концу XX столетия персональные компьютеры становятся доступными для массового потребителя. В начале нового века идет процесс развития связанных между собой компьютерных станций от частных и ведомственных закрытых сетей до открытой, глобальной информационной системы Интернет, объединяющей по каналам цифровой связи всех своих абонентов.

«Глобальная сеть» становится потенциально общедоступной различным пользователям с появлением графического браузера. Она предоставляет им неограниченные возможности для общения, создания, накопления, передачи, получения текстовых, графических, аудио- и видеоданных. Интернет входит важной составной частью в повседневную жизнь и деятельность не только организаций, но и обычного человека. В последующем новые программные продукты и системы *online* доступа к «мировой паутине» с мобильных телефонов и других устройств многократно расширяют круг ее пользователей. По оптимистическим прогнозам в 2020 г. количество пользователей интернета достигнет отметки в 5 млрд чел. [2, с. 31-40].

Во-вторых, с 2002 г. по настоящее время происходит стремительное распространение *online*-платформ и социальных сетей в Интернете. Социальные сети в социологическом смысле как структуры, объединяющие взаимодействующих людей, существовали, разумеется, во всех обществах и до компьютерной эпохи. Однако создание Интернета и *online*-платформ привело к многократному расширению социальных контактов и связей в реальном времени между множеством людей, распределенных по всему земному шару. В 2019 г. в мире насчитывалось 250 социальных сетей и их количество продолжает расти. Среди *online*-платформ особенно популярны «Facebook», «Twitter», «Instagram», «ВКонтакте», «Одноклассники». Стремительный рост числа сетевых связей наблюдается особенно в молодежной среде. По числу интернет-пользователей Россия занимает 8-е место в мире [2, с. 31-40].

1. *Цифровизация и цифровое общество в России*. За весьма короткое по историческим меркам время, благодаря компьютеризации и цифровым технологиям обработки и передачи данных, в центре которых Интернет, социум постмодерна приобрел зримые черты *цифрового общества*. Процесс *цифровизации* («перехода на цифру») можно определить в широком социологическом значении как широко-масштабное внедрение цифровых технологий во все

сферы социальной реальности – жизни и деятельности человека. Особенно ярко и даже безальтернативно этот процесс заявил о себе в условиях пандемии коронавируса.

Цифровизация оказывает колоссальное влияние на основные подсистемы российского социума (экономику, политику и управление, образование, культуру и масс-медиа, здравоохранение), на его социальную структуру («цифровая стратификация») и функционирование, вызывая новые социально-коммуникативные эффекты и практики. Цифровизация наиболее наглядно проявляет себя в экономической сфере. Весьма успешно она развивается в банковском деле, в распространении интернет-торговли, в транспортных системах, в нефте- и газодобыче, а также на ТВ и мультимедиа, в образовании и медицине. Примером реальной цифровизации в повседневной жизни россиян является использование интернета вещей в управлении транспортом с помощью Яндекс.Навигатора. По индексу цифровизации (*digital evolution index*) Россия находится на 39 месте, соседствуя с Китаем и Индией [2, с. 31-40].

Цифровизация как процесс движения к цифровому обществу – неотвратимый, но неоднозначный тренд. С одной стороны, она стимулирует позитивные социальные перемены. Например, в хозяйственной деятельности: исключает рутинный бумажный документооборот, ускоряет все технологические процессы, повышает производительность труда, прибыль, снижает издержки, обеспечивая простоту и точность в предоставлении и получении услуг и товаров, минимизирует влияние ошибок, связанных с «человеческим фактором».

С другой стороны, цифровизация уже сегодня создает немало социальных, экономических и правовых проблем. Среди них – феномен «цифрового неравенства», состоящий в разрыве уровней образования между людьми, в неравных условиях доступа к цифровым услугам и продуктам. В цифровой экономике неизбежна компрессия рынка труда, поскольку уже в недалеком будущем не нужны будут многие массовые профессии: водители, продавцы, учителя, госслужащие, банковские клерки, занятые рутинной, поддающейся оцифровке. Все эти люди, как жертвы массовой безработицы, могут стать девиантами, адаптируясь соответствующим образом к новым цифровым условиям на рынке труда. Перевод личной и конфиденциальной информации в цифровую форму создает невиданную ранее зависимость человека от того, как и где хранятся, используются его данные.

2. *Сетевизация и online-общество*. Экономическая и социальная динамика нового века, происходящая под влиянием фундаментальных последствий информационных технологий, описывается в работах М. Кастельса. По его предположению, именно сети будут составлять новую социальную морфологию постиндустриального мира. В «сете-

вом обществе» все ключевые социальные структуры и деятельность его членов будут организованы вокруг сетей электронных коммуникаций [3]. Действительно, в первые два десятилетия XXI в. благодаря развитию *online*-платформ в Интернете произошел взрывной рост социальных сетей – состоялась *сетевизация социума*. Сетевизация, происходящая за счет роста числа сетевых ресурсов и сетевых пользователей, достигла такого уровня к настоящему времени, что позволяет электронным коммуникациям с помощью *online*-платформ охватить практически все общности и социальные слои социума. Она привела к образованию и стремительному расширению *online*-сообществ. Развивающееся по экспоненциальному закону социальное *online*-пространство представляет собой, по оценке Моссбергпер, «социально-технологическую совокупность, которая создает новую публичную сферу, обеспечивающую цифровое гражданство» [4, р. 211-238].

К плюсам сетевизации можно отнести: неограниченные социальные возможности для общения вне расстояния и времени, создание новых и поиск утраченных контактов, а также неограниченный потенциал для самовыражения и саморазвития личности, для обучения, чтения, просмотра и прослушивания, использования развлечений, для рекламы и продвижения бизнеса, интернет-торговли, организации заработка. Однако социально-технологический феномен сетевизации, как и цифровизация, порождает не только новые возможности, но и новые социальные проблемы, глобальные риски, связанные с распространением сетевой девиантности и виктимизацией сетевых пользователей.

3. *От цифровизации и сетевизации к цифровой девиантации социума*. Цифровизация создает невиданные ранее возможности для развития высокотехнологичной кибердевиантности и прежде всего ее криминальных форм: хищений, мошенничества, взломов и других проявлений инновационной, по Р. Мертону, адаптации девиантов в киберпространстве Интернета. В результате наблюдается всплеск *цифровой девиантации* социума как распространение в киберпространстве «старых» и новых форм девиантности и преступности. Эти перемены иллюстрируют результаты многочисленных интернет-исследований. Так, в обзоре австралийских криминологов структурирован ряд киберпреступлений, обусловленных технологическими факторами цифровизации. Среди них:

- киберпреступления, включающие несанкционированный доступ к компьютерной системе, сетевым данным с помощью взломов, онлайн-атак и/или «вредоносных программ, вирусов»;
- киберкражи, в том числе хищение денег, данных, интеллектуальной собственности, электронное пиратство, совершаемые путем мошенничества или с помощью вредоносных программ;

- кибертерроризм в форме сообщений, поддерживающих предполагаемые террористические акты; распространение инструкций по изготовлению взрывчатых веществ и другого оружия и прочее;

- киберсекс-торговля людьми и секс-туризм, а также сексуальная эксплуатация детей в киберпространстве [5].

В 2018 г. на Всемирном экономическом форуме в Давосе было признано, что киберпреступность стала одним из наиболее критических, глобальных рисков. По экспертным оценкам финансовый ущерб от кибератак в мировой экономике составил в 2019 г. до 2 трлн долл., в 2020 г. приблизится к 3 трлн долл. Причем эти оценки весьма условны, поскольку не отражают в полной мере положения дел в бизнесе из-за стремления финансовых организаций избежать репутационных потерь. По данным аналитиков Сбербанка, потери от киберпреступлений в 2017 г. во всех отраслях российской экономики оценивались в 550-600 млрд руб. В следующем году, согласно ожиданиям экспертов, размеры ущерба должны приблизиться к 1 трлн руб. [2, с. 31-40].

Online-платформы и социальные сети порождают не только *online-сообщества* и новые возможности для общения, но и социотехнологические предпосылки для дальнейшей цифровой девиантации социума. Среди новых проявлений кибердевиантности следует выделить такие, как: сетевая зависимость с утратой навыков реального общения, бегство от действительности (искейперство), киберлудомания, виртуальные сексуальные домогательства и насилие; компьютерная педофилия; запугивание и киберпреследование, интернет-торговля наркотиками, пропаганда ненависти и распространение экстремистских идей.

Кроме того, сетевизация является источником новых форм *кибервиктимизации*. Многие молодые люди, беспечно размещая в социальных сетях личную информацию, фото и видео, рискуют стать жертвами злоумышленников, поскольку *online*-платформы никогда не удаляют контент пользователей и о пользователях. Так, серверы «Facebook» каждую неделю накапливают около 100 терабайт личной информации. По мере роста *online*-сообществ быстро растет объем и так называемой «темной стороны» социальных сетей, где не соблюдаются законы, где похищаются и продаются личные данные пользователей и клиентов, различных чаще всего банковских сервисов. Наибольшие риски кибервиктимизации существуют для таких уязвимых социальных групп, как обладатели личных кабинетов – электронных кошельков, а также подорожки, женщины, пожилые люди, этнические меньшинства, участвующие в сетевом общении. С кейса на данную тему и начинается эта статья.

4. *Интегративные исследования кибердевиантности и киберпреступности*. На протяжении десяти

последних лет к изучению девиантности и других социальных феноменов Интернета активно обращаются зарубежные и отечественные социологи и девиантологи, другие представители обществоведения. В интернет-исследованиях широко используются положения семиотики, теории масс-медиа, социологии культуры, социологии науки и технологий. Так, начиная с 2010-2012 гг. ряд американских и британских социологов (Д. Лаптон, Д. Фаррелл, Дж. Петерсон М. Карриган, Э. Хэад, Х. Дэвис и др.) сосредоточили внимание на определении предметного поля цифровой социологии как интегративной науки о цифровом обществе и его киберфеноменах. В частности, Д. Лаптон обратил внимание на большой социальный смысл включения цифровых технологий, цифровых средств массовой информации и социальных сетей в повседневную жизнь современного человека. Особую роль цифровой реальности он увидел в контексте совершения киберпреступлений, наступления последствий цифровой виктимизации, цифрового неравенства и обеспечения социальной справедливости в цифровом мире. Для зарубежных интернет-исследований весьма типичен анализ идентификационных процессов, происходящих в киберпространстве. Среди них: изучение *online*-сообществ, представителей маргинальных групп, расовых и этнических меньшинств, ЛГБТ-сообществ, а также экстремистов и групп ненависти.

Весьма интересные обобщения в рамках социологической рефлексии цифровой социальной реальности содержат публикации российских исследователей: М.В. Кибакина, С.А. Гришаевой, В.Ф. Ницевича и др. В работах отечественных социологов широко обсуждается научный арсенал различных социологических концепций, подходов и методов, применяемых к осмыслению социальных аспектов цифровизации и сетевизации. Исследователи обращают внимание на социальные эффекты и проблемы, создаваемые Интернетом, популярными социальными сетями и медиа в российском обществе [6; 7].

В целом зарубежные и отечественные социологические работы посвящены анализу проблематики «цифрового разрыва в стратификации»; специфики функционирования социальных медиа, новых идентификационных процессов, новых коммуникативных, в том числе девиантных практик. В результате непродолжительного развития цифровой социологии были концептуализированы такие понятия, как «цифровое общество», «социальная цифровизация», «цифровое неравенство», «цифровое наблюдение». Вместе с тем социальной теории цифровизации все еще нет, несмотря на существенный рост числа социологических интернет-исследований.

Судя по возрастающему количеству научных конференций и публикаций в ведущих социологических и криминологических журналах, наиболь-

ший интерес зарубежные и отечественные исследователи проявляют к изучению киберпреступности и кибердевиантности как последствий цифровизации и сетевизации в мире постмодерна, специфики социального контроля над их проявлениями.

Весьма существенно то, что на начальном этапе цифровизации в конце XX в. и первые годы XXI в. интерес исследователей (Монтгомери, Клаф, Уолл, Смит, Грабоски, Урбас и др.) был преимущественно обращен к киберпреступлениям, совершаемым в отношении компьютеров. Среди них: взломы операционных систем, похищение программных продуктов, несанкционированный доступ к компьютерам, киберкражи денежных средств и финансовых данных, интеллектуальной собственности с помощью вредоносных программ у корпоративных клиентов [5]. При изучении киберпреступлений, «сфокусированных на компьютере», в этот период еще используются традиционные теории преступности и объяснительные модели, выстроенные на их основе для обычных «уличных» краж.

На следующем – современном этапе с развитием цифровизации и сетевизации, когда невероятно возросла доступность *online*-информации, у киберпреступников появилось значительно больше новых возможностей для совершения *online*-преступлений и девиаций, прежде всего в отношении обычных людей – пользователей цифровых услуг и сетевых ресурсов. Типичным инновационным способом кибератак и по сей день являются не только звонки частным клиентам банков, но и рассылка киберпреступниками фишинговых сообщений (поддельных писем) интернет-пользователям с целью войти к ним в доверие и совершить кибермошенничество. Наряду с корыстной киберпреступностью, в исследовательский ракурс социологов и девиантологов вошли новые социально опасные проявления кибердевиантности. Они включают в себя: *online* сексуальную эксплуатацию детей и детскую порнографию, секс-торговлю людьми и секс-туризм (Митчелл, 2010; Рейнс, Хенсон, Фишер 2011); различные формы кибернасилия, киберпреследования и киберзапугивания (киберсталкерство, кибербуллинг), кибертерроризм и распространение инструкций по изготовлению взрывчатых веществ) (Веббер, 2013; Мартин, 2014; Уэйменн, 2016 и др.) [5]. В новом междисциплинарном поиске продуктивно работают и российские исследователи. Ряд оригинальных обобщений содержат публикации Я.И. Гилинского, Я.В. Костюковского, Д.Н. Карповой, С.В. Бондаренко, Ю.Ю. Комлева, В.А. Номоконова, Т.Л. Тропиной, Э.Л. Кочкиной, А.В. Федорова, М.В. Немова и многих других авторов.

Стало очевидно, что новые проявления кибердевиантности и способы совершения киберпреступлений стали сложнее, разнообразнее, динамичнее. Потенциал традиционных криминологических те-

орий оказался недостаточным для их объяснения и моделирования. Отсюда, для изучения кибердевиантности и киберпреступности в зарубежных и отечественных работах стали больше использоваться интегративные концепции и подходы. Эмпирические интернет-исследования в этой области широко опираются не только на бесконтактные методы сбора информации, но и вычислительные алгоритмы и аналитику «*big data*» («больших данных»), что весьма поучительно для отечественных молодых исследователей. Девиантологи и криминологи за рубежом активно ассоциируются в исследовательские группы с прикладными математиками, IT-специалистами. Так, например, поступили британские исследователи, изучающие терроризм, преступления ненависти и «триггерную» преступность [4].

Опыт изучения цифровой девиантации социума формирует предметное поле цифровой девиантологии и криминологии, которое лежит на пересечении социологических и юридических наук, семиотики, теории масс-медиа, математики и информационных технологий. Так, в работах криминологов Ш. Браун (2006), М. Яра (2012) К. Хейворда (2012) широко использовались идеи гибридации социологических, криминологических и технологических знаний для исследования цифровых проявлений девиантности и преступности [5]. Эти и другие труды наметили основные пути построения интегрированного социально-технологического знания о природе и детерминации кибердевиантности и киберпреступности в первые десятилетия XXI в. Исследователи предложили для построения объяснительных моделей различных проявлений киберпреступности объединить знания из различных социальных и технологических дисциплин с опорой на непротиворечивые положения дополняющих друг друга криминологических теорий. Например, гибридизированный подход, обозначенный Ш. Браун, позволяет учитывать роль цифровых технологий в широком спектре правонарушений и виктимизации; сетевого опыта в совершении преступлений; online-маргинализацию по признакам пола, возраста, этничности; состояние и динамику цифрового неравенства и другие социоструктурные и процессуальные факторы киберпреступности.

Австралийские исследователи Г. Страттон, А. Пауэлл, Р. Кэмерон – теоретики цифровой криминологии – также использовали интегративный подход, концептуализируя киберпреступность и кибердевиантность как техносциальные практики в цифровом мире. Они исходили из объединения знаний социологии, криминологии, юриспруденции, политической науки, культурологии, теории масс-медиа, информационных технологий [5].

Таким образом, интегративное теоретико-эмпирическое изучение киберпреступности и кибердевиантности позволяет многомерно и диалектично

моделировать причины и следствия, формы многообразной девиантной активности в цифровом обществе. Использование расширенной методологической триангуляции в интернет-исследованиях с привлечением бесконтактных опросных методик, контент-анализа цифровой текстовой и видеоинформации, вычислительных алгоритмов для обработки структурированных, неструктурированных «больших данных» и других эмпирических материалов – надежный путь для построения прогностических моделей киберпреступности и кибердевиантности [8, с. 97-104]. Возможность предвидеть с помощью аналитики «*big data*» время и место совершения киберпреступлений позволяет значительно улучшить использование ограниченных правоприменительных ресурсов полиции и других силовых структур. Более того, за математически выверенным прогнозированием следует и выработка новых правовых форм и практик социального контроля в киберпространстве более адекватных социально-технологической реальности «цифрового мира», в том числе в условиях новых технологически и биологических обусловленных рисков, пандемий.

Литература:

1. Банки рассказали о новых уловках. – URL: <https://news.mail.ru/economics/41522024/?frommail=1> (дата обращения: 28.04.2020).
2. Комлев Ю.Ю. Цифровизация, сетевизация общества постмодерна и развитие цифровой криминологии и девиантологии // Вестник КЮИ МВД России. – 2020. – № 1. – С. 31-40.
3. Кастельс М. Информационная эпоха: экономика, общество и культура / Пер. с англ. под науч. ред. О.И. Шкаратана. – М.: ГУ ВШЭ, 2000. – 608 с.
4. Matthew L. Williams Pete Burnap Cyberhate on Social Media in the aftermath of Woolwich: A Case Study in Computational Criminology and Big Data // The British Journal of Criminology. – 2016. – Vol. 56. – Iss. 2. – URL: <http://www.doi.org/10.1093/bjc/azv059> (дата обращения: 19.10.2019).

5. Stratton G, Powell A., Cameron R. Crime and Justice in Digital Society: Towards a 'Digital Criminology' // International Journal for Crime, Justice and Social Democracy. – 2017. – № 6(2). – P. 17-33. – URL: http://www.digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1233&context=facsch_lawrev (дата обращения: 28.10.2019).
6. Кибакин М.В., Гришаева С.А. Актуальные проблемы рефлексии цифровой социальной реальности: переосмысление научных концепций. // Цифровая социология. – 2019. – № 2(1). – С. 4-9. – URL: <https://www.doi.org/10.26425/2658-347X-2019-1-4-9> (дата обращения: 28.10.2019).
7. Ницевич В.Ф. Цифровая социология: теоретико-методологические истоки и основания // Цифровая социология. – 2018. – № (1). – С. 18-28. – URL: <https://www.doi.org/10.26425/2658-347X-2018-1-18-28> (дата обращения: 28.10.2019).
8. Комлев Ю.Ю. Интеграция криминологических знаний, расширенная методологическая триангуляция и «big data» в социологическом изучении преступности // Вестник экономики, права и социологии. – 2019. – № 3. – С. 97-104.

From Digitalization and Networkization to Digital Deviantization in a Society of Risks

Komlev Yu. Yu.

Kazan Law Institute of the Ministry of Internal Affairs of Russia

The article describes digitalization and networkization in the postmodern era, in a society of risks, as factors of digital devianization. Based on a content analysis of English-language sources, Internet research, new forms of cyber deviance and integrative approaches to their study are considered.

Key words: coronavirus pandemic, digitalization, networkization, postmodern era, cybercrime, cyber deviance, digital deviantization of society, digital deviantology, integrative approach.

