

УДК 343.9

DOI: 10.24412/1998-5533-2025-2-378-382

От цифровизации социума и киберпреступности к подготовке киберполицейских**Комлев Ю.Ю.**

Доктор социологических наук, профессор кафедры философии, политологии, социологии и психологии Казанского юридического института МВД России, профессор кафедры уголовного права и процесса Университета управления «ТИСБИ» (Казань)

Цифровые технологии в жизнедеятельности современного человека привели не только к позитивным, но и негативным последствиям. Среди них наибольшие риски представляет киберпреступность, темпы роста которой возрастают с каждым годом. Несмотря на институционализацию киберполицейской службы, чрезвычайно актуальной остается подготовка кадров киберполицейских для ОВД. Цель и задачи исследования состоят в обосновании необходимости подготовки киберполицейских в рамках междисциплинарной магистерской программы, например, с профилем «расследование цифровых преступлений»; оценке тенденций в трансформации «старых» и «новых» цифровых форм девиантности; анализе развития киберпреступности и кибервиктимизации, цифрового социального контроля и его правоприменительных институтов; интеграции правовых, поведенческих и технологических знаний в образовательном проекте. Используются статистический метод и контент-анализ научной литературы, обобщен некоторый опыт подготовки киберполицейских. Значение работы состоит в постановке социальной проблемы, ее осмыслении и обосновании варианта решения. Подготовку киберполицейских предлагается реализовать в ведомственной образовательной системе, где сформирован фундамент правовых, девиантологических исследований и знаний с привлечением специалистов из IT-сферы и правоприменительной практики.

Ключевые слова: цифровизация, сетевизация, кибердевиантность, киберпреступность, кибервиктимизация, киберполиция междисциплинарная магистерская программа

Для цитирования: Комлев Ю.Ю. От цифровизации социума и киберпреступности к подготовке киберполицейских // Вестник экономики, права и социологии. 2025. № 2. С. 378–382. DOI: 10.24412/1998-5533-2025-2-378-382.

Мир стремительно изменился в первой четверти XXI в. Российский социум, как и другие постиндустриальные общества, вовлечен в лабиринты четвертой технологической революции, основными социальными измерениями которой стали цифровизация и сетевизация всех сторон жизни и деятельности общества и человека. Миллионы пользователей по всему миру объединил Интернет, началась и продолжается экспансия цифровых технологий во все сферы жизнедеятельности человека. Техноло-

гические инновации повлияли на структуру социума, изменили мир социальных институтов, создали новые формы социальной связи и взаимодействия, породили новые социальные практики. Движение к цифровому обществу – процесс прогрессивный, неотвратимый, но и весьма неоднозначный. С одной стороны, он стимулирует позитивные социальные сдвиги, с другой, – создает ряд сложных социальных проблем. Многие зарубежные и отечественные исследователи (Д. Лаптон, Ш. Браун, М. Яр, К. Хей-

ворд, Г. Барак, Г. Страттон, Н. Селвин, Я. Гилинский, В. Овчинский, В. Номоконов, Ю.Ю. Комлев и др.) обращают внимание на эту двойственность цифровых перемен и считают, что «современное общество лучше понимать как сплетение человечности, материальности и дигитальности». В социологическом анализе последствий распространения цифровых технологий используются «концепция заботы» и «концепция страха».

В рамках первой из них цифровизация исключает рутинный бумажный документооборот; минимизирует издержки, повышает производительность труда и прибыль. Цифровые технологии снижают роль ошибок, связанных с «человеческим фактором», повышают качество прогнозов и управленческих решений. Так, за счет цифровизации и сетевизации социума реализуются повсеместно фактически неограниченные возможности для интернет-общения, обучения, путешествий, покупок, работы. Цифровизация в конечном счете обеспечивает более высокое качество жизни миллионов людей – просвещенных цифровых пользователей за счет повышения объема, доступности и скорости предоставления разнообразных киберуслуг. Вовлеченность в цифровой мир позволяет пользователям приобщиться к новым сферам и способам цифрового самовыражения и самореализации. Кроме того, в цифровом мире значительно лучше обеспечены права человека на свободу выражения мнений и свободу доступа к информации. Распространение онлайн-сообществ и социальных сетей, по мысли М. Кастельса, привело к тому, что «дух свободы выпущен из запечатанной бутылки медиа, и эта свобода оказывается доступной людям во всем мире» [1].

В рамках «концепции страха» цифровизация и сетевизация продуцируют цифровое неравенство, состоящее в разрыве уровней обладания цифровыми компетенциями; неравный доступ к цифровым услугам и продуктам; кибердевиантность, киберпреступность и кибервиктимизацию. В цифровой экономике неизбежна компрессия рынка труда. Возможно, что уже в недалеком будущем не нужны будут многие массовые профессии: водители, продавцы и клерки, занятые рутинной, поддающейся цифровой автоматизации. Многие из них, как жертвы вынужденной безработицы, могут оказаться девиантами, адаптируясь к цифровым условиям на рынке труда, в том числе в форме ретретизма или «бегства от действительности».

Сетевые ресурсы и медиа, увы, обслуживают в первую очередь материальные интересы корпоративных собственников, а не обычных пользователей. Отсюда неумное, патологическое стремление цифровых корпораций – гигантов ИТ-индустрии (*Google, YouTube, Samsung Electronics, Apple, Amazon, Facebook, Sony*, Яндекс и др.) к извлечению прибыли, наживы в рамках цифровой экономики,

что нередко сопряжено с нарушением и даже разрушением социальных и правовых норм сомнительным контентом. Перевод личной и конфиденциальной информации в цифровую форму создает невиданную ранее зависимость человека от того, кем, как и где хранятся, используются его личные данные. Кроме того, пользователи цифровых услуг, проводя время в интернете, на цифровых платформах и иных сервисах сами оставляют свои «цифровые следы» и нередко становятся объектами манипуляций и кибербуллинга. Вовлеченность массы людей в цифровизацию и сетевизацию провоцирует массовое распространение кибермошенничества и цифровую виктимизацию. Киберпреступники, применяя психологические методы манипуляции и приемы социальной инженерии, умело разыгрывают драмы и другие постановки перед своими жертвами, управляя процессом впечатлений, по И. Гофману. Они, нагоняя на своих жертв страх, или вызывая иные эмоции, добиваются в итоге реализации преступных целей.

Контент-анализ публикаций в ведущих социологических и криминологических журналах показывает, что повышенный интерес зарубежные и отечественные девиантологи проявляют к изучению трансформации «старых» и «новых» цифровых форм преступности. Происходит, как пишет Я.И. Гилинский, ««переструктуризация» преступности, когда преступления в цифровом мире теснят «обычную», «уличную преступность» (*street crime*)» [2, с. 182–190]. Более того, в цифровом мире наблюдается переход от компьютерного хулиганства и других девиаций, преступлений против компьютеров и компьютерных систем, запущенный в начале века, к массовым преступлениям против пользователей интернета и социальных сетей, цифровых платежных систем и абонентов сотовой связи с низкой цифровой культурой. Жертвами кибермошенников все чаще становятся не только пенсионеры, но и молодые люди, подростки. Среди новых проявлений кибердевиантности следует выделить такие, как: сетевая зависимость с утратой навыков реального общения; бегство от действительности в мир виртуальных симуляций (искейперство); киберлудомания (игровая зависимость); кибербуллинг (травля в интернете, социальных сетях, мессенджерах), кибергруминг (виртуальные сексуальные домогательства и насилие над несовершеннолетними); компьютерная педофилия; интернет-торговля наркотиками; пропаганда ненависти и распространение экстремистских идей, фишинг и кибермошенничество, вовлечение подростков и простаков в террористическую деятельность или в финансирование неприятеля на фронтах СВО. Непрерывно расширяется палитра кибердевиантности и киберпреступности. С учетом новых реалий современную киберпреступность можно определить как множество проявлений негативной кибердевиантности, состоящих

в нарушении уголовно-правовых запретов с использованием компьютеров, смартфонов, цифровых технологий и обращенных против пользователей интернета, социальных и телефонных сетей.

По данным МВД РФ из открытых источников, общее количество зарегистрированных преступлений в стране продолжает незначительно снижаться. Так, за последние три года ежегодно уменьшаются доли преступлений, совершаемых в общественных местах, против личности; стало меньше уличных разбоев и обычных краж из квартир и автомобилей и т.п. В то же время продолжается стремительный рост регистрируемой киберпреступности. По отчетам МВД России, представленных в открытых источниках, в 2022 г. совершено каждое четвертое преступление, в 2023 г. – каждое третье преступление с использованием информационно-телекоммуникационных технологий (ИКТ). В 2024 г. в целом по стране зарегистрировано 40 % киберпреступлений в форме мошенничества [3].

Риски киберугроз состоят не только в мошенничестве, но и в DDoS атаках, вирусах шифровальщиках, трояках, вирусах вымогателей. Причем, киберзлодеи всех мастей, совершенствуясь, используют и возможности искусственного интеллекта на разных стадиях подготовки и проведения кибератак. У преступников появился собственный чат-бот *GhostGPT*, который используется для подготовки текстов писем в целях мошеннических действий, что не может не беспокоить экспертов по кибербезопасности и правоохранителей. «Прогресс» в киберпреступности продолжается. В итоге общий ущерб, который она нанесла отечественной экономике в 2023–2024 гг. эксперты Сбера оценили в 1 трлн руб.

Из выступления министра внутренних дел по Республике Татарстан Д. Сатретдинова в Государственном совете РТ в феврале 2025 года следует, что за 2024 г. удельный вес зарегистрированных киберпреступлений в регионе вырос с 48 до 57 %. По количеству ИТ-мошенничеств Татарстан уступает лишь Москве, Санкт-Петербургу, Ленинградской области и Краснодарскому краю. В 2024 г. киберпреступники «вынесли» у татарстанцев 5,7 млрд руб. Согласно оценкам МВД по РТ, полиция достаточно успешно противодействует киберпреступности. По количеству выявленных ИТ-преступников Татарстан находится на 2-м месте в РФ. Регионы с высоким уровнем цифровизации и сетевизации, качеством жизни населения, где есть высокооплачиваемая работа и возможности для накоплений, всегда будут привлекать не только трудовые ресурсы, но и киберпреступников [4].

Несложно предположить, что тенденция, состоящая в высоких темпах роста киберпреступности, скорее всего сохранится, поскольку в киберпространстве не вполне реализуется принцип неотвратимости наказания, а барыши от высокотехнологичной преступности существенно превышают доходы

от обычных краж, разбоев и других форм «уличной преступности». Неслучайно, 90 % всех мошеннических действий совершается сегодня в киберпространстве. Практика противодействия преступности вообще и киберпреступности, в частности, осложнена дефицитом кадровых ресурсов в правоохранительных органах.

На мировом рынке труда по мере роста киберпреступности, очередным триггером которого стала пандемия коронавируса, сложился высокий и устойчивый спрос на подготовку специалистов по кибербезопасности, по розыску киберпреступников и расследованию киберпреступлений – киберполицейских. Однако подготовленных специалистов такого рода в России хронически не хватает.

Во всех странах с высоким уровнем цифровизации и сетевизации социума создаются и развиваются факультеты, кафедры, образовательные программы, как правило магистратуры, по подготовке междисциплинарных специалистов по кибербезопасности. В России – это либо технические направления подготовки («Безопасность информационных технологий в правоохранительной сфере» – 10.05.05; «Информационная безопасность» – 10.03.01)) специалистов по защите информации, либо юридическое («Правовое обеспечение национальной безопасности» – 40.05.01) с профилизацией по розыску преступников и расследованию киберпреступлений.

Для правоведа, специализирующегося в сфере кибербезопасности расследования киберпреступлений, необходимы фундаментальные знания, умения и навыки в области цифровых технологий; передачи, хранения и обработки цифровой информации; методологии защиты цифровой информации; криптографии; электронной коммерции; кибердевиантности и киберпреступности; документирования цифровых следов преступлений против личности и др. Если в бизнесе, в банковской сфере подразделения по кибербезопасности созданы и успешно функционируют уже не первый год, то в правоохранительных органах этот процесс явно запаздывает. Крупный бизнес привлекает и готовит ИТ-специалистов, закрепляя в основном выпускников технических вузов с медианной зарплатой в 150 000 руб. и выше. В ОВД, по экспертным оценкам, средняя зарплата «опера» не многим больше 60 000 руб. В таких условиях закрепить специалиста по кибербезопасности – выпускника гражданского вуза в правоохранительных органах практически нереально. Надо готовить свои ведомственные кадры. С этой проблемой сталкиваются правоохранители во всех технологически развитых странах. Они идут по пути создания специализированных полицейских структур по борьбе с киберпреступностью и занимаются подготовкой и особенно переподготовкой полицейских сил.

В США еще в 2002 г. был создан кибердивизион ФБР, деятельность которого сосредоточена на трех

основных направлениях: компьютерные вторжения, кража персональных данных и кибермошенничество. В Великобритании с 2013 г. работает Национальное агентство по борьбе с киберпреступностью. В Китае с 2015 г. создана «сетевая полиция» в Министерстве общественной безопасности. Для борьбы с кибермошенничеством организованы отделы кибербезопасности в крупнейших китайских интернет-компаниях. Киберполиция создана и в Германии, как подразделение Федерального уголовного агентства. Международная киберполиция (ICP) создана в 2018 г. для реализации решений ООН по борьбе с организованной преступностью, коррупцией и терроризмом, криминалом, нарушением прав человека во всех регионах мира. Шесть государств Евросоюза (Эстония, Хорватия, Польша, Нидерланды, Румыния, Литва) в 2020 г. создали Кибернетические силы быстрого реагирования. В Польше в 2025 г. планируют сформировать киберполицию как самостоятельное подразделение.

В России продуктивно работает Центр информационной безопасности ФСБ. Преступлениям в IT сфере противодействует управление «К» МВД РФ. С 2020 г. идет работа по созданию российской киберполиции. Активно противоборствуют киберпреступности специальные подразделения кибербезопасности в федеральных и региональных ведомствах, крупных компаниях и банках России. Работа по защите сервисов и цифровых данных организована в Минцифры, ЦБ РФ, Сбере, ВТБ, МТС и др.

Вместе с тем в стране чрезвычайно высока потребность в квалифицированных специалистах «на местах» по обеспечению кибербезопасности, особенно в осуществлении розыска преступников и расследовании киберпреступлений. Существуют хорошо зарекомендовавшие себя специальные программы подготовки специалистов по кибербезопасности и защите информации в Московском университете МВД России, Санкт-Петербургском университете МВД РФ. В Российской академии народного хозяйства и государственной службы стали готовить медиаполицейских для выявления деструктивных и экстремистских материалов в интернете и противодействия кибербуллингу. По мнению экспертов, киберполицейский, как специалист по кибербезопасности, – это тот, кто хорошо разбирается в праве, в девиантных практиках, цифровых технологиях, способах совершения деликтов, расследования и противодействия цифровым преступлениям.

С 1 сентября 2026 г. Россия отходит от Болонской системы образования и выстраивает свою собственную. Как известно, анонсированная реформа высшей школы предполагает три уровня высшего образования: «базовое высшее» вместо бакалавриата и специалитета, «специализированное высшее» для программ магистратуры и «профессиональное» – аспирантура.

Выпускник ведомственного вуза системы МВД на основе базового образования по направлению подготовки «Правовое обеспечение национальной безопасности» – 40.05.01 может продолжить «специализированное» обучение в рамках междисциплинарной программы магистратуры, например, по профилю «расследование цифровых преступлений», или «кибербезопасность в правоохранительной сфере». Реформа высшей школы предполагает не только коренной пересмотр основных образовательных программ обучения, но и создание новых (надеюсь, у вузов сохранится право самостоятельно определять их основное содержание). Важно уже сегодня предложить образовательные проекты, учитывающие кадровый спрос на рынке труда, подготовить их концептуальное научное и учебно-методическое обеспечение. Увязать теорию с передовой практикой, вовлечь в учебный процесс потенциальных работодателей и специалистов-практиков из подразделений кибербезопасности и киберполиции. Недавнее политическое решение Президента РФ В.В. Путина повысить престиж и конкурентноспособность полицейского труда дает надежду на рост денежного содержания полицейских и привлечение в ОВД компетентных специалистов по кибербезопасности. Кроме того, разработка междисциплинарных программ магистратуры в ведомственных вузах МВД по направлению подготовки «Правовое обеспечение национальной безопасности» – 40.05.01 соответствующего профиля могли бы удовлетворить растущий спрос на подготовленных к работе в новых технологических условиях киберполицейских.

Как известно, с 2002 г. в стенах Московского университета МВД России имени В.Я. Кикотя создан факультет подготовки специалистов (технического профиля) с учетом межвузовской кооперации с Московским авиационным институтом в области информационной безопасности, на котором выпускаются специалисты по защите информации (направление подготовки «Безопасность информационных технологий в правоохранительной сфере» – 10.05.01). Подготовка «цифровых специалистов» для следствия организована в Московской академии СК России, где в 2021 г. открыта кафедра информационных технологий и организации расследования киберпреступлений. Подготовка и переподготовка киберследователей осуществляется путем введения в учебный процесс новых «цифровых» дисциплин и программ ДПО, например, «расследование преступлений, совершаемых с использованием ИКТ». В образовательной системе Следкома активно идет процесс подготовки киберследователей по специальности «Правовое обеспечение национальной безопасности» – 40.05.01. В рамках этого направления ведется обучение будущих следователей на юрфаке Всероссийского государственного университета юстиции (РПА Минюста России), в структурах

Российского экономического университета имени Г.В. Плеханова. Специалистов по защите информации готовят Московский государственный технический университет имени Н. Э. Баумана, Российский университет транспорта (МИИТ), Национальный исследовательский университет «Высшая школа экономики». Однако, этого явно недостаточно, чтобы удовлетворить растущий спрос в ОВД и других правоохранительных структурах на подготовку киберполицейских.

Обзор положительного отечественного опыта показывает, что подготовку кадров для киберполиции Поволжья, Татарстана и других регионов вполне реалистично организовать в Казани – крупном вузовском центре – в стенах Казанского юридического института МВД России. Это может быть междисциплинарный образовательный проект в формате магистерской программы, в основе которой будет лежать фундамент правовых, девиантологических и ИТ-исследований, передовой правоприменительной практики. Квалифицированный профессорско-преподавательский состав и учебно-методическая база ведомственного вуза в кооперации с МВД по РТ, Университетом Иннополиса, другими заинтересованными вузами Казани способен разработать и реализовать инновационную магистерскую программу обучения киберполицейских в рамках развития направления подготовки «Правовое обеспечение национальной безопасности» – 40.05.01 с профилизацией «расследование цифровых преступлений»

или «кибербезопасность в правоохранительной сфере», а также специализированные программы ДПО.

Для успешного воплощения этого замысла сформировался социальный заказ на рынке труда и существуют все необходимые материальные, кадровые, научные, учебно-методические условия. Киберполицейские – это весьма востребованная профессия настоящего и ближайшего цифрового будущего.

Литература:

1. Кастельс М. Власть коммуникации: учеб. пособие / Пер. с англ. Н.М. Тылевич; под науч. ред. А.И. Черных. М.: Изд. дом Высшей школы экономики, 2023. 590 с.
2. Гишинский Я.И. Девиантность в цифровом мире // Проблемы деятельности ученого и научных коллективов. 2019. № 4 (34). С. 182–190.
3. На кибермошенничества в РФ пришлось 40 % от всех преступлений в 2024 года. URL: <https://www.interfax.ru/russia/1003799> (дата обращения: 22.05.2025).
4. «Едут и те, кто хочет подкормиться, провороваться!»: как впервые публично отчитался Дамир Сатретдинов. URL: <https://dzen.ru/a/Z7cUwTcGzVdrIhqj?ysclid=mao195k4e1494719960> (дата обращения: 22.05.2025).

From the Digitalization of Society and Cybercrime to the Training of Cyber Police Officers

Komlev Yu. Yu.

**Kazan Law Institute of the Ministry of Internal Affairs of Russia,
University of Management TISBI (Kazan)**

Digital technologies in the life of a modern person have led to not only positive, but also negative consequences. Among them, the greatest risks are posed by cybercrime, the growth rate of which is increasing every year. Despite the institutionalization of the cyberpolice service, the training of cyberpolice personnel for the internal affairs bodies remains extremely relevant. The purpose and objectives of the study are to justify the need to train cyberpolice officers within the framework of an interdisciplinary master's program, for example, with the profile "investigation of digital crimes"; assessing trends in the transformation of "old" and "new" digital forms of deviance; analyzing the development of cybercrime and cybervictimization, digital social control and its law enforcement institutions; integrating legal, behavioral and technological knowledge in an educational project. The statistical method and content analysis of scientific literature were used, some experience in training cyberpolice officers was summarized. The significance of the work lies in the formulation of a social problem, its understanding and justification of a solution. It is proposed to implement the training of cyber police officers in a departmental educational system, where a foundation of legal, deviantological research and knowledge has been formed with the involvement of specialists from the IT sphere and law enforcement practice.

Key words: digitalization, networking, cyberdeviance, cybercrime, cybervictimization, cyberpolice interdisciplinary master's program