ческими характеристиками: минимальное значение – 0,36; максимальное – 0,74; медиана − 0,46; среднее квадратическое отклонение – 0,1.

Методика оценки уровня криминализации регионов строится из предположения, что если видовой состав преступности между собой связан тесной корреляционной зависимостью, то преступность в представленном территориальном образовании представляет связную систему, имеет место самовоспроизводство и высокая криминализация населения.

В тройку территорий с выявленным максимальным средним коэффициентом корреляции на уровне 0,73 вошли Южный и Центральный ФО и г. Москва. Стоит отметить, что это достаточно высокое значение даже для усредненного показателя. Минимальные значения связности на уровне 0,36 обнаружены в Еврейской и Ненецком АО, Пермском крае. В середине списка с медианным значением оценки (0,46) находятся восемь территориальных образований, среди них Красноярский край, Новосибирская и Мурманская области. Ниже среднего показателя по России находятся 90 регионов.

Таким образом, развивая предлагаемый подход, можно проводить следующие оценки:

− в группах видовых показателей преступности;

− в группах категорий преступлений (небольшой тяжести, средней тяжести, тяжкие, особо тяжкие);

− в межгрупповых связях и так далее.

Большой интерес представляют частные оценки корреляционной зависимости между отдельными видами преступлений, но это уже будет следующий этап научного изыскания.

Для реализации практической значимости подобных исследований необходимо участие специалиста-криминолога, а предлагаемый инструментарий математической статистики способен осуществлять поддержку при принятии решений или опровержении выдвигаемых исследователем гипотез.

Комлев Ю.Ю.,

доктор социологических наук, профессор
Казанский юридический институт МВД России

Цифровизация и киберпреступность в мире постмодерна

Технологии радикально меняют жизнь человечества и отдельно взятого человека. Компьютеры и Интернет, социальные платформы и сети изменили общество постмодерна, в том числе криминальный мир.

Обобщение материалов интернет-исследований из англоязычных и отечественных источников с помощью метода качественного контент-анализа позволяет сделать ряд констатаций, дефиниций и обобщений[1]. Некоторые из них, наиболее существенные, состоят в следующем.

1. Цифровизация и общество постмодерна. В настоящее время большинство пользователей предпочитает выходить в Интернет с мобильных устройств. По оптимистическим прогнозам в 2020 г. количество пользователей Интернета достигнет отметки 5 млрд человек. За весьма короткое по историческим меркам время, благодаря компьютеризации и информационным технологиям, в центре которых Интернет, социум постмодерна приобрел зримые черты «цифрового общества».

Процесс цифровизации («перехода на цифру») можно определить в широком социологическом значении как широкомасштабное внедрение информационных цифровых технологий во все сферы социальной реальности, жизни и деятельности человека.

Цифровизация особенно наглядно и в первую очередь проявляет себя в экономической сфере. Поэтому нередко ее интерпретируют в узком смысле как процесс

[1] Комлев Ю.Ю. Цифровизация, сетевизация общества постмодерна и развитие цифровой криминологии и девиантологии // Вестник КЮИ МВД России. 2020. № 1.

перехода к цифровой экономике. Прежде всего, это развитие интернет-банкинга, интернет-торговли, интернет-рекламы, электронных платежей, электронного документооборота, online-услуг, интернета вещей, электронного доступа к государственным услугам. В число стран лидеров цифровой экономики по индексу цифровизации (digital evolution index) входят Норвегия, Швеция, Дания, Южная Корея, США. Россия в этом рейтинге находится на 39 месте, соседствуя с Китаем и Индией[1].

Цифровизация в России развивается стремительными темпами. Наиболее успешно это происходит в банковской сфере, в распространении интернет-торговли, в ТВ и мультимедиа, в образовании и медицине, в транспортных системах, в нефте- и газодобыче. По числу пользователей Интернетом Россия занимает 8 место в мире.

Закономерно, что вопросы развития цифровой экономики и других сфер бытия определены стратегией развития информационного общества в России на 2017-2030 гг., утвержденной Указом Президента РФ от 09 мая 2017 г. № 203[2]. Цифровизация в экономике и других сферах общества постмодерна – неотвратимый, но неоднозначный тренд. С одной стороны, она стимулирует позитивные социальные перемены. С другой стороны, цифровизация уже сегодня создает немало социальных проблем.

2. Киберпреступность – риски для цифровых пользователей и проблемы определения. Внедрение новых открытий, как это уже не раз бывало в истории, приносит не только благо, но и вред. Цифровизация создает невиданные ранее возможности для инновационной преступной активности в Интернете. Криминализация некоторых деяний в России, связанных с правонарушениями в компьютерной сфере, произошла только с принятием Уголовного кодекса Российской Федерации в 1996 г. (гл. 28). В 1997 г. были зарегистрированы 33 преступления, а в 2005 – 10 214, то есть их количество выросло за 9 лет в 310 раз[3].

На начальном этапе цифровизации наибольшую общественную опасность представляли:

− 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.

Высокие темпы повсеместного роста киберпреступности заставили признать в 2018 г. на Всемирном экономическом форуме в Давосе, что киберпреступность − это один из наиболее критических глобальных рисков современности. По одним экспертным оценкам, ежегодные потери мировой экономики в результате киберпреступлений достигают 500 млрд долларов[4]. По мнению других экспертов, финансовый ущерб от кибератак в мировой экономике составил в 2019 г. до 2 трлн долларов, в 2020 г. − до 3 трлн[5]. Причем и эти оценки весьма условны. По данным аналитиков Сбербанка, потери от киберпреступлений в 2017 г. во всех отраслях российской экономики оцениваются в 550-600 млрд рублей. В следующем году размеры ущерба, по мнению экспертов, приблизятся к 1 трлн рублей[6]. При этом в юридическом дискурсе, в уголовном законодательстве нет

[1] Что такое цифровая экономика? URL: http://www.fingramota.org/teoria-finansov/iterm2198-2198-chto-takoe-tsifrovaya-ekonomica (дата обращения: 26.10.2019).

[2] Администрация Президента России : официальный сайт. URL: http://www.kremlin.ru/acts/bank/41919 (дата обращения: 26.10.2019).

[3] Гилинский Я.И. Криминология: теория, история, эмпирическая база, социальный контроль. 2-е изд. перераб. и доп. СПб. : Юридический центр Пресс, 2009. С. 376.

[4] ВЭФ анонсировал создание Глобального центра кибербезопасности. URL: https://www.securitylab.ru/news/491033.php (дата обращения: 20.10.2019).

[5] МИД РФ: ущерб мировой экономике от киберпреступности в 2019 году может достичь $2. URL: https://www.tass.ru/politika/5551244 (дата обращения: 20.10.2019).

[6] Данные исследования Сбербанка и его дочерней компании Bi.Zone «Новые вызовы цифрового мира», посвященное современным киберугрозам и противодействию им. URL: https://www.roscongress.org (дата обращения: 28.10.2019).

однозначности относительно определения феномена киберпреступности.

На начальном этапе цифровизации (конец XX- первые годы XXI в.) интерес зарубежных исследователей 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[1]. Киберпреступность определяется в англоязычных работах предельно широко. Одно из рабочих определений киберпреступности в российской традиции, адекватное начальному этапу цифровизации, приводит профессор В.А. Номоконов. Оно состоит в том, что киберпреступность − это «совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных»[2]. Более поздние определения кибепреступности концентрируют внимание на компьютере как инструменте и одновременно как объекте преступления[3]. Примечательно, что во всех указанных трактовках киберпреступности отсутствует человек как жертва высокотехнологичного преступления. Между тем на современном этапе цифровизации, когда невероятно возросла доступность online-информации, у киберпреступников появилось значительно больше новых возможностей для совершения online-преступлений, прежде всего в отношении многочисленных частных пользователей Интернета и цифровых услуг. Так, по последним данным, 97% сетевых хищений у частных лиц совершается с помощью фишинга. С нашей точки зрения, рост нелегального обогащения в условиях сетевого обмена и обращения к различным ресурсам Интернета порожден новой специфической кибермотивацией преступников. Мотивация обогащения и адаптация в новых цифровых условиях происходит по инновационному типу (Р. Мертон). По данным департамента полиции Нью-Йорка, криминальный доход среднего киберпреступника в современном американском мегаполисе в семь раз превышает добычу обычного преступника. Кроме того, раскрываемость традиционных преступлений составляет в разные годы 40-60%, а киберпреступлений − всего 4%. Словом, киберпреступность – это высокодоходная и малорискованная криминальная деятельность, особенно в отношении частных пользователей.

Не случайно киберпреступники по всему миру стали атаковать не столько вычислительные машины и базы данных финансовых и других деловых организаций с помощью вирусов-шифровальщиков и внедрения вредоносных программ (supply chain-атак), сколько обычных людей – массовых пользователей цифровых услуг и сетевых ресурсов с помощью инновационных криминальных приемов. Типичным способом является рассылка киберпреступниками фишинговых сообщений (поддельных писем) интернет-пользователям с тем, чтобы войти к ним в доверие и совершить кибермошенничество.

Кроме того, в последние годы (2014-2019 гг.) происходит дифференция кибердевиантности и киберпреступности, растет ее общественная опасность. Это и online сексуальная эксплуатация детей и детская порнография, и кибер-секс-бизнес, кибер-секс-торговля людьми, и продажа наркотиков, и кибер-секс-туризм; различные формы кибернасилия, киберпреследования, киберзапугивания (кибersталкерство, кибербуллинг), домогательства, а также кибер-

[1] Stratton G, Powell A and Cameron R (2017) Crime and Justice in Digital Society: Towards a ‘Digital Criminology’ // International Journal for Crime, Justice and Social Democracy 6(2) : 17-33. URL: http://www.digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1233&context=facsch_lawrev (дата обращения: 28.10.2019).

[2] Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1(24). URL: https://www.cyberleninka.ru (дата обращения: 29.10.2019).

[3] Joseph Aghatise Cybercrime definition. URL: https://www.researchgate.net/publication/265350281_Cybercrime_definition (дата обращения: 29.10.2019).

терроризм и распространение инструкций по изготовлению взрывчатых веществ.

Стало очевидно, что новые формы и способы совершения киберпреступлений, другие проявления кибердевиантности, вызванные цифровизацией, интенсивными технологическими и социальными изменениями в обществе постмодерна, стали сложнее и разнообразнее. И все они в значительной мере или в конечном счете обращены прежде всего против сетевых пользователей. Отсюда, с девиантологической точки зрения, киберпреступность можно определить как множество проявлений негативной кибердевиантности, состоящих в нарушении уголовно-правовых запретов с использованием компьютеров, цифровых технологий и обращенных против компьютерных систем, социальных сетей и их пользователей.

3. Проблемы социального контроля в киберпространстве. Цифровизация, вооружая киберпреступников новыми технологическими возможностями, создает не только относительно высокую профитность для киберпреступников, но и относительную безопасность.

Система формального социального контроля сдержать волну цифровой криминализации социума не может. В Интернете практически заблокирована реализация классического принципа неотвратимости наказания в условиях несовершенного и запаздывающего законодательного регулирования в киберсфере, инертности правоприменительной практики, высокой степени анонимности злоумышленников и рядовых сетевых пользователей.

Цифровые технологии позволяют злоумышленникам оставаться анонимными, менять геолокацию, «взламывать» чужие аккаунты, тем самым скрывать информационные следы, что затрудняет расследование киберпреступлений.

Законодатели разных стран, реагируя на глобальные вызовы в цифровой социальной реальности, принимают законы, направленные против киберпреступлений, вводят и совершенствуют уголовную ответственность за их совершение. Однако консервативное уголовное законодательство с национальной юрисдикцией и тем более правоприменительная практика без развития международного сотрудничества в правовом регулировании отстают от требований дня, что порождает серьезные проблемы в сфере обеспечения кибербезопасности. Кроме того, эти проблемы обусловлены дефицитом подготовленных для правоохранительной системы кадров, недостаточно развитым взаимодействием между бизнесом и правоохранителями по вопросам безопасности в киберпространстве.

Обобщая отечественные и зарубежные источники, можно выделить несколько перспективных форм противодействия киберпреступлениям.

1. Совершенствование правового регулирования в цифровой сфере (необходимы своевременные изменения законодательных актов о связи, информационных технологиях, СМИ, социальных сетях и др.).

2. Поддержка рестриктивных практик и судебных решений по селективной блокировке информационных ресурсов, распространяющих запрещенную в России информацию, адресованную целевой молодежной аудитории при непременном сохранении связи Рунета с глобальной сетью (без существенного сокращения прав пользователей на получение информации, то есть цензуры).

3. Разработка технических средств и инструментов, позволяющих эффективно препятствовать совершению преступлений, защищать цифровые данные и раскрывать преступления.

4. Разработки специальной главы в УК РФ, посвященной противодействию киберпреступности в контексте международных правовых норм и соглашений, регулирующих глобальные риски киберпреступности.

5.Необходима целенаправленная работа с институтами социализации подростков и молодежи по повышению эффективности самоконтроля и формированию цифровой идентичности, неформального родительского социального контроля в целях снижения вероятности киберпреступного поведения в молодежной среде, вызванного мотивами гедонизма, наживы и обогащения.

В целом информационные технологии создают предпосылки для трансформации традиционных форм управления и обеспечения социального порядка, стимулиро-

вания работы над созданием и внедрением новых цифровых форм социального контроля и слежения за пользователями «мировой паутины», участниками сетевого общения. Однако цифровой мониторинг и другие практические аспекты совершенствования социального контроля в цифровом мире все еще недостаточно отрефлексированы в работах интернет-исследователей. Это удел новых, молодых сил в девиантологии и юриспруденции.

Тетерятников Н.Ю.,

кандидат юридических наук
Сибирский юридический институт МВД России (г. Красноярск)

«Виртуализация» преступности: киберугрозы современности

С первых лет третьего тысячелетия в России, как, впрочем, и во всем мире, наблюдается значительное (более чем на 70%)[1] уменьшение количества преступлений. Особенно насильственных. Это явление получило название великого спада преступности – great crime drop.

Причины столь резкого снижения преступной активности до конца так и не ясны. Один из факторов, который, безусловно, этому способствует, – увеличение времени, которое люди тратят на пребывание в информационных телекоммуникационных системах. Начиная от нахождения в социальных сетях, и до часов, ежедневно проводимых за компьютерными играми. То есть, заменяя действительность реальную на виртуальную, у человека элементарно остается меньше времени на то, чтобы совершать в повседневной жизни что бы то ни было, включая противоправные поступки.

Вместе с тем, в пику изложенному необходимо отметить, что, как указывают А. Кнорре и В. Кудрявцев, упомянутое «великое снижение преступности не затронуло две сферы: кражи мобильных телефонов и так называемые e-crimes – киберпреступления, связанные с компьютерами и компьютерными сетями»[2].

Несложно догадаться, что мобильные телефоны пользуются такой популярностью у преступников, поскольку на них наибольший общественный спрос как на самое распространенное в настоящее время средство доступа людей к телекоммуникационным системам, к той самой виртуальной реальности. Что касается киберпреступности, то это ничто иное как побочный, но в какой-то степени и закономерный эффект компьютеризации (а теперь еще и цифровизации) весьма значимой части жизни современного общества.

И если удешевление стоимости мобильных телефонов – это вопрос времени, что в перспективе неминуемо приведет и к снижению соответствующих краж, то сокращения уровня киберпреступности прогнозировать не приходится. Тем более что в настоящее время киберпреступность с постоянно увеличивающимся объемом причиняемого ущерба – это теневая многомиллиардная высокотехнологическая сфера, от противоправной деятельности авторов которой страдают и целые государства, и крупнейшие транснациональные корпорации, и отдельные учреждения, и обычные люди.

В связи с этим целесообразно рассмотреть основные виды киберугроз, с которыми все чаще и чаще приходится сталкиваться нашим современникам.

Одной из самых первых в истории человечества киберугроз, возникшей в 1980-х гг., стали компьютерные вирусы. Это специально созданные вредоносные программы, повреждающие либо уничтожающие пользовательскую информацию, а также препятствующие нормальной работе компьютерной техники.

Изначально большинство компьютерных вирусов не были предназначены для

[1] Великое снижение преступности // Ведомости : электронное периодическое издание. URL: https://www.vedomosti.ru/opinion/articles/2017/09/28/735650-velikoe-snizhenie (дата обращения: 25.01.2020).
[2] Там же.