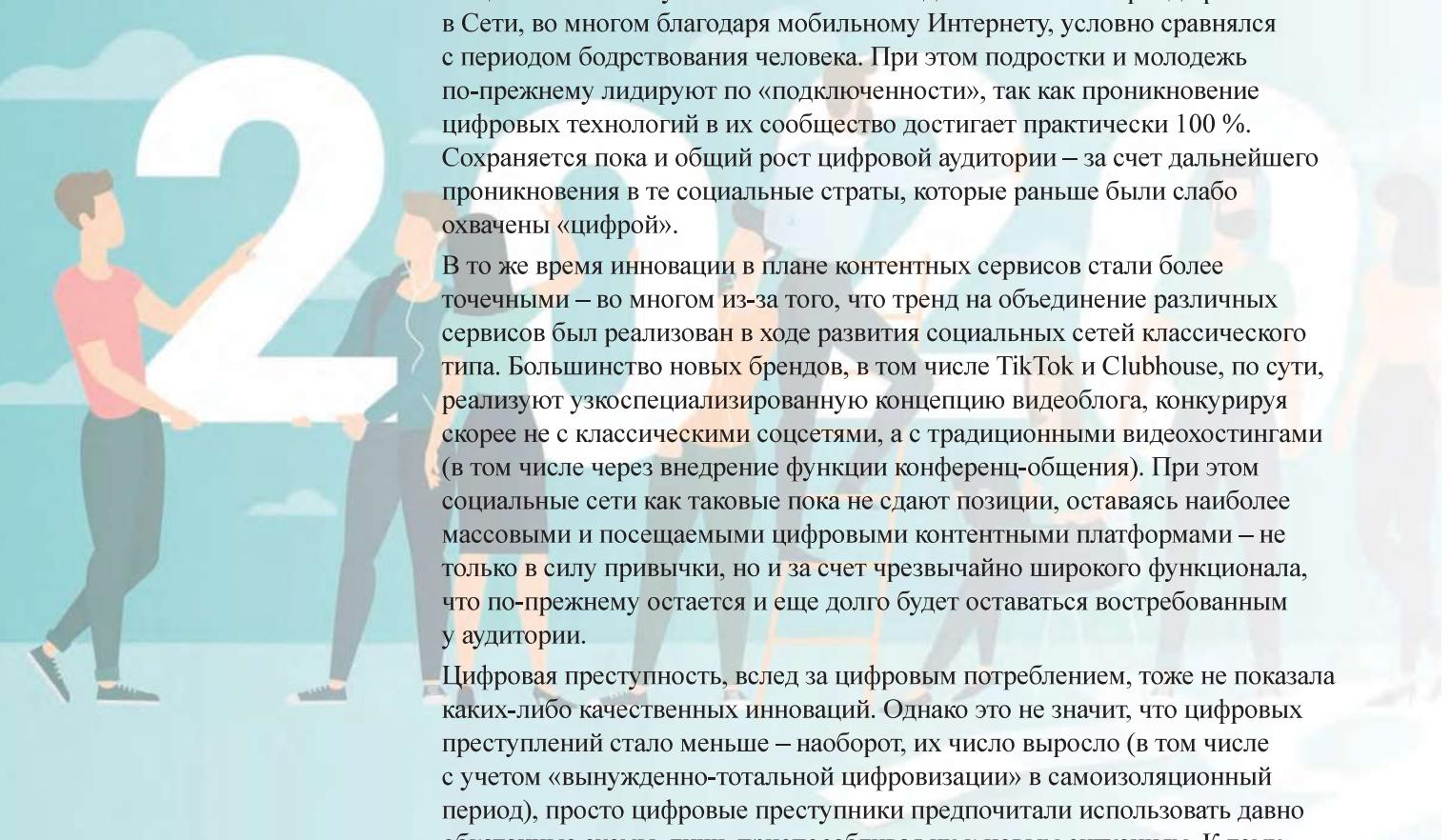




РЕЖИМ ОНЛАЙН



ЦИФРОВЫЕ ТРЕНДЫ 2020 ГОДА: «МОМЕНТЫ ИСТИНЫ»

Цифровая среда отличается от многих других отраслей общественной жизни и экономики своим быстрым развитием – как в технологическом плане, так и в социальном. Например, современное общество стало в буквальном смысле «подключенным»: период пребывания в Сети, во многом благодаря мобильному Интернету, условно сравнялся с периодом бодрствования человека. При этом подростки и молодежь по-прежнему лидируют по «подключенности», так как проникновение цифровых технологий в их сообщество достигает практически 100 %. Сохраняется пока и общий рост цифровой аудитории – за счет дальнейшего проникновения в те социальные страты, которые раньше были слабо охвачены «цифвой».

В то же время инновации в плане контентных сервисов стали более точечными – во многом из-за того, что тренд на объединение различных сервисов был реализован в ходе развития социальных сетей классического типа. Большинство новых брендов, в том числе TikTok и Clubhouse, по сути, реализуют узкоспециализированную концепцию видеоблога, конкурируя скорее не с классическими соцсетями, а с традиционными видеохостингами (в том числе через внедрение функции конференц-общения). При этом социальные сети как таковые пока не сдаают позиций, оставаясь наиболее массовыми и посещаемыми цифровыми контентными платформами – не только в силу привычки, но и за счет чрезвычайно широкого функционала, что по-прежнему остается и еще долго будет оставаться востребованным у аудитории.

Цифровая преступность, вслед за цифровым потреблением, тоже не показала каких-либо качественных инноваций. Однако это не значит, что цифровых преступлений стало меньше – наоборот, их число выросло (в том числе с учетом «вынужденно-тотальной цифровизации» в самоизоляционный период), просто цифровые преступники предпочитали использовать давно обкатанные схемы, лишь приспосабливая их к новым ситуациям. К тому же, 2020 год обострил проблему использования государством цифровых технологий во вред гражданам и впервые обозначил тему «самостоятельного контентного поведения» крупных цифровых сервисов.

Разумеется, на первом месте в рейтинге цифровых преступлений остается мошенничество. В ходе развития программно-технических защитных средств преступники быстро осознали, что самым слабым звеном защитной системы является человек, обычный пользователь, и манипуляция им позволит открыть дверь к денежным средствам, защищаемым соответствующими программами. Существенный «подарок» мошенникам сделали ограничения, в панике введенные в связи с COVID-19: инфоповод «отработали» на сто процентов. Если посмотреть глобально, то в чем-то сценарии жуликов были одинаковы, но в чем-то и отличались – преимущественно в силу социальной политики разных государств.

В тех странах, где граждане в условиях «схлопывания» экономики и потери дохода оказались брошены властями на произвол судьбы, люди старались добить какие-то деньги любой ценой – в том числе и в онлайне. Кто-то из них



УРВАН ПАРФЕНТЬЕВ,
координатор Центра
безопасного Интернета,
г. Москва
urvan@nedopusti.ru



пополнил ряды кибермошенников, а кто-то — жертв. Многие потеряли последнее в расцветших пышным цветом лотереях, тотализаторах и тому подобных механизмах отъема и увода денег. Бывало и так, что людям подбрасывалась информация о якобы положенных им выплатах — и жертвы теряли свои персональные данные, а то и напрямую деньги.

В тех же государствах, где госорганы проявили заботу о своих жителях и организовали раздачу денег, ситуация с кибермошенничеством оказалась не столь острой, хотя фальшивые сайты с предложением «дополнительных выплат», конечно, фигурировали и там.

Отдельную проблему составили приложения типа московского «Социального мониторинга»: жулики успешно «подсаживали» свои собственные программы под видом государственных, а также развлекались фальшивыми штрафами за якобы нарушения «ковидных» ограничений.

Проблема с безопасностью персональных данных если и находится на втором месте, то очень условно: охота за ними ведется не менее интенсивно, чем за прямыми деньгами. Контроль за персональными данными человека не только открывает путь к его финансам, но и позволяет контролировать самого человека — тайну его личной жизни или его репутацию. Цифровизация персональных данных способствует массовым их утечкам, и порой одна утечка может иметь сотни миллионов жертв. При этом стопроцентно надежного механизма защиты не существует: данные по всему миру утекают из банков, и из правоохранительных органов, несмотря ни на что. Особую опасность представляют в этом плане биометрические персональные данные, так как их компрометация носит пожизненный характер, ибо изменить лицо или отпечатки пальцев почти невозможно — это не буквенно-цифровой пароль или хотя бы паспорт. В этой связи стремление отдельных банков и, еще хуже, государств внедрять биометрическую идентификацию (например, так называемые «системы распознавания лиц») вызвало не просто протест, а самый натуральный ужас — сначала у специалистов в области инфобезопасности и правозащитников, а потому уже и в обществе. Уж слишком всё это напоминает печально известный мир антиутопии Оруэлла «1984» (кстати, один из российских разработчиков подобной системы для школ прямо назвал свое решение «Оруэлл»). В итоге моратории

на подобные системы уже введены или их планируется ввести в целом ряде штатов США и в Евросоюзе, подобное требование выдвинуто и в России ввиду гигантской общественной опасности предлагаемых решений, намного перевешивающей теоретическую пользу.

Проще говоря, биометрические данные собирать не надо — это очень опасно. Что, соответственно, ставит крест на любых системах «школьной безопасности», основанной на системах распознавания лиц и допуске по отпечаткам пальцев.

Опасений в плане биометрии добавила и технология диплейков — подмены лица, а то и фигуры в видеоизображении до уровня неотличимости обычным глазом. Изначально она разрабатывалась в интересах киноиндустрии — чтобы обходиться без дублеров (например, если надо снять ремейк какого-то старого фильма). Однако масштабирование технологии всегда означает удешевление и повышение ее доступности, что привело к тому, что «замена лиц» посредством технологий машинного обучения перекочевала в порноиндустрию.

А оттуда ее пытались заимствовать популярные цифровые сервисы для обычных пользователей — сначала в качестве опции «забавный курьез».

Правда, владельцы соцсетей не учли специфическую психологию своих юзеров: новую опцию тут же применили для киберунижения, причем, как правило, с порнографическим уклоном (точнее, для создания фальшивых сексуальных видео с лицом отвергнутых возлюбленных). Оправдаться и доказать, что это фейк, жертвы не могли: мысль о возможности качественной подделки видеоизображения тогда ни у кого не укладывалась в голове.

Следующими забили тревогу специалисты в сфере антитеррора, так как высококачественный диплейк «киношного» уровня вполне может использоваться для призывов к террористическим актам, массовым беспорядкам и свержению законной власти. Эту возможность описал еще Хайнlein 80 лет назад (например, вложить призыв в уста популярной в обществе личности, а то и самого главы государства). В ограниченной мере диплейки освоили и кибермошенники — фальсифицируя «лидеров мнений». Разумеется, из популярных цифровых сервисов все диплейк-приложения быстро исчезли, но «птица уже вылетела»: соответствующие



решения можно найти как в даркнете, так и в специфических местах «обычного» Интернета. Антидипфейки же находятся только в стадии разработки, так как опасность вредоносного использования искусственного интеллекта была изначально недооценена. И, к сожалению, пока немногочисленные сообщения о том, что приложение, распознающее дипфейк, уже сделано и работает, пока выглядят как выдача желаемого за действительное.

Единственное, с чем у злоумышленников стало сложно в период самоизоляции, — это продажа наркотиков, поэтому интенсивность торговли «веществами» заметно снизилась. Причина была весьма проста: здесь, в отличие от «чистых» онлайн-угроз, присутствует значимая офлайн-составляющая в виде доставки заказанного. На пустых, улицах городов «кладмен» (наркокурьер) был чрезвычайно заметен и почти стопроцентно привлекал внимание патрулей. Таким образом, риск становился недопустимым и грозил наркодилерам прекращением всего их бизнеса. В результате «антинаркотическая» категория оказалась чуть ли не единственной из контентных цифровых угроз, динамика по которой оказалась позитивной.

2020 год также подвел определенную черту под спорами, которые предметно шли чуть ли не два десятилетия: может ли «цифра» на определенном этапе своего развития полностью заменить офлайн? Коронавирусные ограничения создали непредставимые ранее условия для такого «стресс-теста». И результат оказался для многих сфер такой: «Да, может, но плохо и недолго». В первую очередь это коснулось онлайн-образования: к такой форме оказались не готовы ни учителя, ни ученики. Первые испытывали явные сложности с цифровой матчастью — выбором соответствующих приложений и организацией работы в них (безопасность таких уроков оказалась отдельным вопросом). Вторые — с дисциплиной, усвоением материала и даже с физической возможностью участвовать в онлайн-уроках, поскольку в семьях стационарный компьютер или ноутбук часто оказывался только один и его использовали родители для онлайн-работы. Уединиться для онлайн-урока детям тоже было негде, да и качество связи в отдельных регионах сказалось негативно (цифровой разрыв на практике оказался еще не преодолен). В итоге родительская общественность и часть педагогов стали с большим подозрением

относиться к цифровым экспериментам в образовании вообще, и именно поэтому столь массовым оказалось движение против проекта «Цифровая образовательная среда», так как многие сочли его принципиальным переводом образования из офлайна в онлайн и тут же припомнили весь негатив периода самоизоляции.

Однако бывает, что джинн цифровых угроз выпускается наружу под влиянием чисто политических аспектов. Самый яркий пример здесь — гипертрофированное внимание к так называемым «фейк новос» — фальшивым новостям, которое возникло в качестве реакции на неожиданную победу Трампа на президентских выборах 2016 года в США. Тогда в «пожарном порядке» на Западе были выпущены информационно-просветительские материалы про «фейк новос», которые демонстрировали явное непонимание и политизацию проблемы. Джинн же вырвался в 2020 году, под очередные американские президентские выборы: когда крупные цифровые контентные сервисы («прописанные», кстати, именно в США) стали произвольно трактовать свои собственные размытые правила и блокировать всё, что им по той или иной причине не нравится. Анализ блокировок неизбежно наводит наблюдателя на мысль, что некто пытается понять и уловить текущий политический тренд, то есть подстроиться под него в угоду гипотетическому новому мейнстриму. Так, например, блокировали аккаунты из некоторых «недружественных» государств, дошло и до блокировки самого Трампа (тогда еще действующего президента). Однако на этой волне случился кошмар из техноантиутопий: крупные цифровые сервисы, подобно «Скайнету», «осознали себя» и перешли к навязыванию собственной политики суверенным государствам. Самым ярким оказался пример противостояния Facebook и правительства Австралии — далеко не самой маленькой и весьма влиятельной в глобальном плане страны. Разумеется, такой фокус проходит далеко не всегда — например, при противостоянии с США, Евросоюзом или Китаем «фронда» даже глобального цифрового сервиса обречена на провал (по причине исключительной финансовой значимости этих рынков). Однако в других случаях всё бывает не столь радужно, что вновь обостряет вопрос о необходимости профильной конвенции об управлении Интернетом на уровне ООН.