ISSN 2524-2369 (Print)
ISSN 2524-2377 (Online)
УДК 316.422
https://doi.org/10.29235/2524-2369-2019-64-3-289-298

Поступила в редакцию 18.07.2018
Received 18.07.2018

**Е. М. Бабосов**

*Институт социологии Национальной академии наук Беларуси, Минск, Беларусь*

# ПРОТИВОРЕЧИВОСТЬ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ В СОВРЕМЕННОМ СЕТЕВОМ ОБЩЕСТВЕ

**Аннотация.** Выявлена амбивалентность конструктивной значимости социальных сетей и негативных способов их использования. Охарактеризовано негативное воздействие интернет-зависимости на здоровье, в первую очередь детей и подростков. Представлены примеры и типичные черты совершения в медийном пространстве интернет-хулиганства, кибермошенничества, интернет-хищений, секс-шантажа, совращения детей и подростков в интернете. Обращено внимание на возрастающую значимость формирования интернет-культуры, разработки и совершенствования законодательно-правовых установлений, ужесточающих наказания за злодеяния в киберпространстве.

**Ключевые слова:** амбивалентность использования информационно-коммуникационных систем, негативное воздействие интернет-зависимости на здоровье, интернет-хулиганство, кибермошенничество, интернет-хищения, секс-шантаж и совращение детей в интернете, роль законодательно-правовых установлений в пресечении киберпреступности

**Для цитирования.** Бабосов, Е. М. Противоречивость использования компьютерных технологий в современном сетевом обществе / Е. М. Бабосов // Вес. Нац. акад. навук Беларусі. Сер. гуманіт. навук. – 2019. – Т. 64, № 3. – С. 289–298. https://doi.org/10.29235/2524-2369-2019-64-3-289-298

**Ye. M. Babosov**

*Institute of Sociology of the National Academy of Sciences of Belarus, Minsk, Belarus*

## CONTRADICTORY USE OF COMPUTER TECHNOLOGY IN A MODERN NETWORK SOCIETY

**Abstract.** Ambivalence of constructive significance of social networks and negative ways of using them has been revealed. The fatality of long-term exposure and internet addiction to health, especially of children and adolescents, is characterized. Examples and typical features of committing internet hooliganism, cyber-fraud, cybercrime, blackmail of sexual nature, internet seduction of children and adolescents are presented. Attention to growing importance of formation of internet culture, development and improvement of legislative and legal provisions that toughen punishments for atrocities in cyberspace is drawn.

**Keywords:** ambivalence of use of information and communication systems, negative impact of internet addiction on health, internet hooliganism, cyber-fraud, cybercrime, internet sex blackmail and child abuse, role of legislative and legal provisions in suppressing cybercrime

**For citation.** Babosov Ye. M. Contradictory use of computer technology in a modern network society. *Vestsi Natsyyanal'nai akademii navuk Belarusi. Seryia humanitarnykh navuk = Proceedings of the National Academy of Sciences of Belarus. Humanitarian Series*, 2019, vol. 64, no. 3, pp. 289–298 (in Russian). https://doi.org/10.29235/2524-2369-2019-64-3-289-298

В большинстве стран мира, в том числе и в Беларуси, интенсивно развиваются сетевизация и цифровизация всех сфер жизнедеятельности людей. Высоко оценивая важную конструктивную значимость социальных сетей в жизнедеятельности индивидов, социальных, торговых, медицинских, научных, образовательных, социокультурных учреждений, предприятий и фирм, не следует оставлять вне зоны внимания и осмысления различные негативные побочные эффекты неконтролируемого использования информационно-коммуникационных структур.

Широкий круг пользователей социальных сетей высказывают озабоченность в связи с тем, что в медийном пространстве нередко осуществляется интернет-хулиганство, воплощающееся в оскорблениях, запугиваниях, преследованиях неугодных лиц, на месте которых может оказаться любой пользователь интернет-информации.

Проведенные белорусским центром системных бизнес-технологий САТИО (О.Н. Фаблинова и др.) исследования показали, что из более чем 1000 респондентов позитивно оценивают влияние

интернет-сетей на дружеские отношения в молодежной среде 22% респондентов, но в 1,7 раза больше – 38% – отрицательно, а в студенческих общностях удельный вес опрошенных, негативно оценивающих влияние сетей на дружеские отношения, возрастает до 43%.

Кроме того, многие исследователи (Д. В. Ярцев, О. А. Романов, Е. А. Нижний и др.) отмечают негативное воздействие чрезмерно интенсивного включения молодежи в интернет-общение, что влечет ослабление воспитательной функции семьи, формирование у молодых людей демонстративно-потребительского поведения.

Многолетними исследованиями установлено негативное длительное воздействие компьютерных устройств на центральную нервную систему детского организма, на интеллектуальное развитие малышей. Ребенок не получает сенсорных ощущений, вследствие чего утрачивается взаимосвязь между командами головного мозга и движениями рук, а в итоге плохо развивается мелкая моторика кистей. В результате постоянного использования мышки у ребенка начинают неметь и болеть пальцы правой руки (или левой, если он левша) – это так называемый туннельный синдром. Постоянное вглядывание в небольшие объекты на мониторе приводит к близорукости, а напряжение глаз – к высыханию слизистой и ее воспалению. Кроме того, регулярное применение планшетов и смартфонов вредно для позвоночника, который у детей очень податлив к искривлению [20].

Влиятельная британская газета «The Financial Times» в июне 2018 года сообщила о начале эпидемии онлайн-игромании, от которой особенно страдают молодые люди. Английские эксперты утверждают, что в последнее время счет интернет-зависимых людей пошел на миллиарды, в связи с чем медики с туманного Альбиона, поддержанные британскими депутатами, с тревогой заговорили о губительности азартных компьютерных игр для здоровья, в первую очередь для детей и подростков. Поэтому в средствах массовой информации, учреждениях образования и культуры необходимо чаще и доказательно убеждать молодежь реже заглядывать в экран смартфона и включаться в компьютерные игры, отдавая предпочтение живому общению со сверстниками и повседневным, интересным делам в реальном мире [16].

Примечательно, что основатель компании «Apple» Стив Джобс строго ограничивал для своих детей время, которое они затрачивают на использование айфонов и айпадов. Основатель «Twitter» Эван Уильямс разрешает своим детям пользоваться планшетами и смартфонами не более одного часа в день [9].

Втягивая ребенка в красочный, периодически изменяющийся игровой виртуальный мир, компьютер, в случае длительного привязывания к нему, отвлекает от реального окружающего мира, мешает полноценному общению с окружающими взрослыми и детьми, делает ребенка раздражительным и искажает его мировосприятие. В результате со временем у таких детей возникает игровая или интернет-зависимость, являющаяся своего рода социально-психологическим недугом. Поэтому санитарные нормы и правила Республики Беларусь не рекомендуют детям дошкольного и младшего школьного возраста использовать портативные гаджеты с высокочастотным электромагнитным излучением: смартфоны, планшеты, нетбуки, ноутбуки, электронные книги.

Во время учебной и воспитательной работы с детьми и подростками, в несколько меньшей степени с молодежью следует учитывать, что в условиях широкого распространения социальных сетей у современного молодого поколения формируется так называемое клиповое мышление. Для этого поколения восприятие информации, в отличие от представителей старших поколений, – не последовательное и не текстовое. Они видят картину цельной и воспринимают информацию по принципу клипа. Они не читают, не верят текстовым материалам и ищут ключевые моменты в них, поэтому скорость их ознакомления с новой информацией значительно выше. Они способны одновременно читать, посылать SMS-сообщения, звонить кому-нибудь. И таких людей в современном сетевом обществе требуется все больше. Но имеется здесь и обратная сторона медали – поверхностное освоение полученной информации, трудности в процессе ее анализирования, выработка потребительского отношения к информационным потокам. Для преодоления этих негативов специалисты советуют приучать молодежь читать произведения классиков, которые формируют и тренируют умение анализировать и создавать образы изображаемых героев самостоятельно [11].

В последнее время довольно частыми стали случаи использования социальных сетей в целях нарушения авторского права, зачастую без ведома автора или с нарушением условий договора, посредством плагиата происходит не просто заимствование безо всяких ссылок, но и присвоение чужого текста.

Широко распространившиеся в последние несколько лет в Минске и других городах Беларуси интернет-магазины также нередко используются недобросовестными работниками торговли, которые не соблюдают потребительские стандарты, нарушают законодательство о защите прав потребителей.

Виртуализация в сетевом обществе информационного пространства породила негативную тенденцию к обезличиванию журналистики, когда реальные создатели информационных сообществ прячутся за псевдонимами или за вымышленными фамилиями и в погоне за сенсациями искажают, а то и вовсе извращают излагаемые события.

Имеются также случаи, когда в социальных сетях распространяется недостоверная информация, порочащая честь и достоинство того или иного, чаще всего широко известного лица.

В виртуальную реальность все чаще перемещаются знакомства, переписка, покупки, услуги, игры. В ней находят разнообразные выражения правдоподобие, поддержка ближнего и даже дальнего, незнакомого человека, борьба за справедливость. Но в то же время в этом виде сетевые общение и взаимодействие нередко, а в последнее время все чаще, прививают и низменные чувства – обман, сладострастие, унижение знакомых и не очень знакомых людей (троллинг). Например, в феврале 2017 года сотрудники правоохранительных органов Беларуси начали разыскивать активного 18-летнего интернет-пользователя, являющегося интенсивно действующим троллингером. Он через «YouTube»-канал организовал живые эфиры – стримы, в которых транслировал по всему миру, как через «Skype» «раздевает» юных девушек. Молодой человек в формате видеообщения подсказывал своим моделям, какие предметы одежды надо снимать. За этим шоу следили 50 тысяч подписчиков. Почувствовав назревающее разоблачение и последующее уголовное наказание (в лучшем случае крупный штраф), этот сетевой «инноватор» подался в бега.

Но в интернет-сетях человека могут подстерегать и другие опасности. Группа авторитетных исследователей из Социологического института Копенгагенского университета, несколько лет изучавших феномен социальных сетей, недавно пришла к пугающему выводу: виртуальное общение наносит вполне реальный вред психике – она по природе своей отторгает подобный суррогат. Разговоры в соцсети ведь сводятся к простому обмену текстовыми сообщениями и условными индикаторами эмоций, смайликами, имеющими мало общего с подлинным выражением чувств, тогда как именно через их передачу посредством мимики, интонации, телодвижений человек получает едва ли не большую часть нужных сведений во время разговора. Потребность видеть и слышать собеседника заложена в человеке генетически. Длительные суррогатные разговоры в соцсетях для организма – нонсенс, который приводит к затяжным и зачастую тяжелым депрессиям, ощущению пустоты в жизни и ее бессмысленности. Нередко у интернет-зависимых людей, особенно юного и детского возраста, происходят не только негативные психические, но и физические изменения. Последние связаны с тем, что в некоторых областях головного мозга у таких людей оказывается пораженным белое вещество, отвечающее за самоконтроль, скорость принятия решений, общее эмоциональное состояние.

Исследования, проведенные в Техасском университете в Остине, показали, что чрезмерная приверженность к смартфонам ослабляет умственные способности своих владельцев, делает их психологически неустойчивыми, приводит к снижению их эрудированности.

Приведенные факты убеждают в том, что следует делать практические выводы из того, что крупные специалисты в области развития и изменения сетевых структур, а также врачи и учителя с тревогой говорят о возрастающем количестве попадания людей, в первую очередь молодых, особенно восприимчивых к новым информационным технологиям, в зависимость от использования компьютеров, смартфонов или планшетов.

В Санкт-Петербургском университете, в лаборатории когнитивных исследований под руководством профессора Т. В. Черниговской установлено, что память людей, живущих в цифровую эпоху, хуже памяти их бабушек и дедушек. У многих из них происходят такие болезненные

изменения, как нарушение концентрации, дефицит внимания. Одно дело – получить информацию, другое – понять ее. Доказано: если сканировать мозг интернет-зависимого человека, то получается та же картина, как у наркомана или алкоголика [17].

И проблема здесь заключается не только в том, что длительное «зависание» человека в соцсетях заставляет его затрачивать на такое занятие драгоценное время или оказывает вредоносное воздействие на зрение. Такое «зависание» может привести и к более серьезным отрицательным последствиям, связанным с тем, что интернет-зависимый человек гораздо чаще, чем другие люди, может воспринять негативные воздействия, идущие от мошенников и других социально-опасных людей. Поэтому необходимо оберегать нашу молодежь, начиная с детского возраста, от чрезмерно активного и длительного пребывания в интернет-пространстве.

Сегодня вполне правомерно говорят о молодежи как о «поколении сети», ведь она ежедневно включается в мощные и разнообразные информационные потоки при помощи интернета. Поэтому очень важно вырабатывать у молодого человека и в семье, и в школе, и в трудовом коллективе способность выборочно воспринимать эти потоки, внимательно усваивать то, что соответствует культуре нашего народа, внутренним установкам нравственной и гражданско развитой личности. В таком случае молодой человек (и не только молодой) становится внутренне способным отделить правду от лжи, сопротивляться искушениям, будет использовать социальные сети во благо, но не во зло. Такая жизненная позиция означает, что человек достаточно открыт к восприятию того, что несет ему современный мир, но сохраняет свою личностную самость, национальную, духовную, культурную самобытность. Нужно не только сохранять, но и защищать свою духовно-нравственную самостоятельность, культурную самобытность и сопротивляться информационной агрессии. Одновременно и в органической взаимосвязи с этим необходимо улучшить, в первую очередь в учебных заведениях, формирование и активное развитие интернет-культуры.

Наряду с этим и властным структурам страны следует принимать эффективные меры по очистке социальных сетей от бескультурья и бездуховности и усиливать противодействие информационным атакам, ведущимся в сетевых потоках против нашей страны и ее государственного строя, нашего народа и нашей культуры.

Противоречивость и амбивалентность в использовании компьютерных систем в современном сетевом обществе порождает еще несколько сложных и трудно разрешаемых проблем в социальных взаимодействиях. Одна из них заключается в том, что возрастающая масштабируемость применения информационно-коммуникационных технологий практически во всех сферах общества не только увеличивает возможности конструктивного разрешения многих задач в различных сферах жизнедеятельности человека, но одновременно порождает у девиантно ориентированных индивидов и состоящих из них групп использовать компьютерные технологии в социальных преступных целях. Причем по мере расширения числа пользователей компьютерных сетей возрастает количество преступлений в сетевых структурах. Следует также иметь в виду три весьма существенных обстоятельства. Во-первых, практически невозможно обеспечить безопасность интернета в одной отдельно взятой стране, поскольку современные киберугрозы транснациональны, для них не существует ни географических, ни политических, ни темпоральных границ. Во-вторых, такие угрозы характеризуются высокой степенью интенсивности, их раскрываемость едва превышает половину их общего количества. В-третьих, киберпреступность многолика, и довольно часто возникают и быстро распространяются все новые ее виды.

Стремительное развитие сетевых систем сопровождается возрастающей активизацией разнообразных видов преступлений в киберпространстве. Главным объектом деструктивных кибернетических воздействий становится банковско-финансовая сфера. По данным Национального банка России, объем криминальных операций в российских автоматизированных системах дистанционного банковского обслуживания, который в 2014 году составил около 1,6 тыс., в 2016 году вырос до более 7 тыс. Общий объем ущерба российской экономике от киберпреступлений – около 400 млрд руб., что составляет 0,5% ВВП Российской Федерации, и в 3,3 раза превышает все расходы страны на жилищно-коммунальное хозяйство, в 1,02 раза – расходы на здравоохранение [12].

На встрече генеральных прокуроров стран БРИКС в августе 2017 года генеральный прокурор Российской Федерации Ю. Чайка сообщил, что количество киберпреступлений в России с 11 тыс. в 2013 году увеличилось до 66 тыс. в 2016 году, т. е. в шесть раз. Значительный их рост наблюдался и в 2017 году (+26%, 40 тыс.). Ущерб от таких преступлений за первую половину 2017 года превысил 18 млн долларов США. МВД и «Group-IB» ликвидировали группировку, укравшую 50 млн рублей с помощью трояна. В мае 2017 года в нескольких городах России задержаны два десятка киберпреступников, которые с помощью вредоносного ПО для мобильных устройств похитили более 50 млн руб. Авиакосмическая отрасль России привлекает растущий интерес кибершпионов. В феврале 2017 года стало известно о том, что китайские хакеры стали интенсивно атаковать авиакосмические компании России и Беларуси. Такой вывод сделали эксперты компании «Proofpoint», отслеживающие деятельность группировки, ранее замеченной в атаках на правительственные структуры и коммерческие компании по всему миру.

Специалисты компании «Avast» отмечают, что во втором квартале 2017 года число мобильных кибератак в России выросло почти на 40 %. Три самые распространенные из них, по мнению «Avast», выглядят следующим образом:

1) *перехватчики root-доступа* (22,8 %). Перехватчики создают запрос на root-доступ или получают его с помощью эксплоистов. Эти вредоносные программы контролируют устройство, шпионят за пользователем и похищают различные данные;

2) *загрузчики* (22,76 %). Загрузчики или дропперы используют методы социальной инженерии, чтобы обманом вынудить жертву установить дополнительные вредоносные приложения. Дропперы также используются для отображения полноэкранных рекламных объявлений даже вне приложений. Такая реклама не просто раздражает пользователей, но и зачастую перенаправляет их на вредоносные сайты;

3) *фейковые приложения* (6,97 %). Поддельные приложения, которые выдаются за подлинные, чтобы увеличить число скачиваний и показывать пользователям рекламу [18].

Об актуальности и важности исследования киберпреступности и определения путей и средств противодействия ей свидетельствует социодинамика компьютерной преступности на протяжении последних лет в Беларуси. В течение 2012–2017 гг. она возросла с 2040 до 3099 случаев преступных злодеяний.

В нашей стране количество выявленных киберпреступлений в 2017 году по сравнению с 2016 годом возросло на 25,4 % – с 2471 до 3099. Увеличение количества киберпреступлений в 2017 году в сопоставлении с 2016 годом произошло за счет прироста преступлений против информационной безопасности на 20,2 % (с 651 до 781). Количество фактов несанкционного доступа к компьютерной информации возросло на 152,9 % (с 258 до 462). Распространен так называемый фишинг – разновидность сетевого мошенничества, состоящая в том, что киберпреступник заманивает пользователей на фальшивые сети, где получает доступ к данным платежных карт с целью хищения у них денег. А жертвами таких киберзлодеяний становятся клиенты банков и электронных платежных систем[1].

В последнее время в Беларуси киберпреступники все более масштабно используют вредоносные программы-включатели, которые шифруют размещаемые в социальных сетях данные, а затем требуют выкуп за расшифровку. Наряду с этим в интернет-пространстве довольно часто совершаются преступления против конфиденциальности, целостности и доступности компьютерных данных, а также преступления, связанные с нарушением авторских прав. Одним из активно используемых трендов является распространение вредоносных вирусов, основанных на программе «Trojan.Winlock». Она блокирует операционную систему компьютера, а его владельцу предлагается перевести деньги на электронный кошелек в качестве оплаты за разблокирование. Довольно часто в киберпространстве Беларуси осуществляются хищения с использованием банковских карточек.

Основные особенности киберпреступности в Беларуси состоят в том, что, во-первых, три четверти их связаны с хищениями, во-вторых, масштабы компьютерной преступности возрастают.

[1] Официальный сайт Министерства внутренних дел Республики Беларусь [Электронный ресурс] / МВД Республики Беларусь. – Минск, 2017. – Режим доступа: htttps: //www.mvd.gov.by. – Дата доступа: 09.08.2017.

Как сообщил В. Зайцев, заместитель начальника управления по раскрытию преступлений в сфере высоких технологий МВД, количество выявленных преступлений в сфере высоких технологий в 2017 году по сравнению с 2016 годом увеличилось на 25,4%. Почти три четверти злодеяний связаны с хищениями путем использования компьютерной техники [7]. В 2017 году сотрудники подразделений по раскрытию преступлений в сфере высоких технологий криминальной милиции Министерства внутренних дел Беларуси установили 1052 причастных к киберзлодеяниям гражданина, что на 86 человек больше, чем в 2016 году. К уголовной ответственности привлечено 956 лиц, в том числе 294 имеющих судимость, 683 нигде не работающих и не учащихся, 34 несовершеннолетних. Сумма ущерба от противоправных действий в виртуальном пространстве в 2017 году составила 3,2 млн белорусских рублей [6].

Следует иметь в виду, что преступления в сетевых системах чаще совершаются не одиночками, а транснациональными группами. Так, например, такая группа, в состав которой входило четверо граждан Беларуси, совместно с соучастниками из других стран совершила хищения на сумму 18 млн долларов у более чем 260 тыс. граждан различных государств. Раскрытие подобного рода киберпреступлений может оказаться успешным только в том случае, когда происходит в тесном взаимодействии с коллегами из других государств [1].

В последнее время хакерским атакам все чаще стали подвергаться вслед за компьютерами владельцы смартфонов и планшетов. Наибольшую опасность для смартфонов со стороны киберпреступников представляет вход в медийное пространство через беспарольный «Wi-Fi», представляющий один из основных каналов для хакерских атак. Нередко через мобильную сеть на сайтах предлагается доступ к скачиванию и просмотру прилично именуемого «взрослого видеоконтента». Наиболее предпочитаемыми для киберпреступников становятся такие преступления, которые ориентированы на получение выкупа. Становящиеся все более крупномасштабными и многообразными информационно-коммуникационные сетевые структуры используются преступными лицами и их группами для распространения порнографии, наркотиков, вовлечения недовольных деятельностью управленческих структур в экстремистские действия.

Недавно в Беларуси появился и набирает обороты новый вид киберпреступности – секс-шантаж. В 2016 году в милицию обратился 41 человек, которым угрожали, что откровенное видео с их участием увидят другие пользователи, если не перечислить злоумышленникам деньги. А в 2017 году жертв стало в 2,5 раза больше, причем все пострадавшие – мужчины – жители Минска. В МВД это объясняют более свободными нравами жителей крупных городов и преобладанием минчан в интернете. Оперативники считают, что на деле жертв стало гораздо больше, но люди стыдятся обращаться по такому поводу в милицию. Злоумышленники работают по нехитрой схеме: заводят в соцсетях фейковые страницы, как правило, от лица девушек, находят потенциальных жертв и начинают переписку на откровенные темы. Дальше девушка предлагает продолжить общение в видеочате. Затем сценарий развивается по-разному: например, девушка может оголить грудь или станцевать эротический танец, а потом просит раздеться и мужчину. Видео с виртуальным сексом злоумышленники записывают, а потом начинается шантаж [5].

Летом 2017 года обширный резонанс получило уголовное дело кибермошенника, который от лица подкупленных им девушек предлагал пользователям канала «Skype» виртуальный секс, а затем требовал от поддавшихся на его предложения клиентов 100 долларов за неразглашение записей. Количество сексуальных домогательств посредством социальных сетей возрастает. В июне 2017 года суд вынес приговор брестскому жителю, который знакомился при помощи компьютера со школьницами, вел с ними интенсивную переписку и постепенно подталкивал к близости. Значительную часть из трех сотен совершающихся в республике в течение года преступлений против несовершеннолетних составляют совращения через социальные сети. Если одни злоумышленники охотятся за откровенными фотографиями детей, другие добиваются реальных встреч и вытекающих из них отношений, третьи, получив фотографии или видеокадры, продают их. Но наиболее циничны и омерзительны те, которые, получив доступ к несовершеннолетнему человеку, склоняют его к проституции [3]. Считается, что первый платный сайт, где нужно платить за просмотр порносюжетов, запустила в сеть порноактриса Дэнни Аше в 1995 году. К 1999 году порносайты заработали в онлайне 1,3 млрд долларов, в 2006 году – 2,8 млрд, а к 2020 году, по

утверждению экспертов, объем секс-индустрии достигнет 20 млрд долларов. В настоящее время третью часть трафика в интернете дают порносайты. У одного из самых крупных порносайтов в мире «Xvideos» около 5 миллиардов просмотров в месяц – втрое больше, чем у любого новостного ресурса, блога или медиахолдинга [13]. На таких сайтах несложно найти и секс с несовершеннолетними, и сцены развращения детей, и сцены насилия. А они в свою очередь провоцируют насилие и в реальной жизни [14]. Маньяки и прочие извращенцы научились умело пользоваться социальными сетями, растлевая неискушенных девушек, временами выманивая жертв на общение в реальности [21].

Серьезную озабоченность сотрудников МВД и учреждений образований получает распространение в последние годы так называемого груминга – преступных действий по совращению детей в интернете. Например, в Минской школе-интернате № 7 двое сотрудников задержаны по подозрению в педофилии, а из 108 детей, которые содержались там, не менее трети подвергались сексуальному или физическому насилию. За два первых месяца 2018 года от сексуального насилия в Минске пострадали 115 детей – это в два раза больше, чем в 2017 году. Поэтому в МВД считают, что необходимо введение уголовной ответственности за хранение детской порнографии, груминг [21]. Милицейская статистика свидетельствует, что за последние 5 лет количество преступлений против половой неприкосновенности и свободы подростков увеличилось в 15 раз: в 2017 году в Беларуси дети подвергались насилию 581 раз, что на 84,4% выше показателей 2016 года. Но в милицейскую статистику попадают лишь те случаи, которые завершились приговором суда. Конечно, масштабы проблемы гораздо серьезнее. Понятно, что она требует решения с помощью совместных действий органов МВД, учебных заведений, комиссий различных уровней местных властей по делам несовершеннолетних, родителей, широкой общественности [19].

Одними запрещающими мерами нарастающую волну цифровизации порносекса снизить, а тем более приостановить, не удастся. Здесь необходимо в учебных заведениях, средствах массовой информации, общественных организациях, прежде всего, детских и молодежных, активизировать, сделать более привлекательными воспитание семейных ценностей, уважение к женщине, институту брака.

Ширится в Беларуси еще одна новая разновидность киберпреступлений – хищение денег абонентов сотовой связи с помощью мобильного банкинга на смартфоне. «Несмотря на то что данный вид хищений появился в конце прошлого года, буквально через месяц сотрудники подразделений по раскрытию преступлений в сфере высоких технологий уже провели задержания причастных к этому лиц. Двое мужчин по предварительному сговору занимались такой деятельностью в Могилеве и Минске. Еще один гражданин промышлял подобным на территории Минской области. Возбуждены уголовные дела по ст. 212 УК Беларуси (хищение путем использования компьютерной техники). Есть основания полагать, что эпизодов было гораздо больше. Пока же общая сумма ущерба составляет более 2 тыс.», – отметил заместитель начальника управления по раскрытию преступлений в сфере высоких технологий криминальной милиции МВД В. Зайцев. Он подчеркнул, что злоумышленники ищут жертв в общественных местах, а иногда просто просят телефон у знакомых якобы для того, чтобы позвонить. «Когда аппарат попадает в руки афериста, он делает вид, что набирает номер, а на самом деле при помощи USSD-запроса или выхода в интернет активирует предоставляемую некоторыми операторами сотовой связи услугу мобильного банкинга. Она позволяет осуществить платежные операции с лицевого счета абонента и получить у оператора сотовой связи лимитированный микрозайм. Сумма, поступившая хозяину гаджета, в несколько касаний переводится на российские абонентские номера или банковские счета. Туда же могут уйти и средства с баланса мобильного телефона. Все это занимает буквально пару минут, – отметил В. Зайцев. – В результате граждане остаются без денег, вынуждены погашать микрозайм вместе с процентами и вносить абонентскую плату за использование мобильного банкинга». Многие не сразу понимают, что стали жертвой злоумышленников, и лишь спустя некоторое время замечают, что с их счетов списывается слишком большая сумма. В МВД подчеркивают, что обезопасить себя от подобных преступлений довольно просто. Достаточно не передавать свой телефон другим людям, даже знакомым, и установить на него блокировку [8].

Затруднения в раскрытии злонамеренных действий преступного характера возникают зачастую вследствие того, что далеко не все, кто сталкивается с такими явлениями, обращаются в правоохранительные органы. Кто-то из потерпевших не хочет афишировать свою беспечность и доверчивость, кто-то не хочет ввязываться в оперативно-следственный процесс. Кто-то, проявляя жалость и сочувствие к людям, просящих о помощи, не желает быть в глазах пользователей интернета бездушным эгоистом. А кто-то испытывает такую сильную привязанность к легким деньгам, что легко поддается на обманные обещания интернет-мошенников. Но что самое удивительное в такого рода историях – доверчивость интернет-пользователей, которые сами попадают в руки виртуальных мошенников.

Масштабы киберпреступности в различных регионах Беларуси развертываются с разными скоростями и различной интенсивностью. Об этом свидетельствуют официальные данные Министерства внутренних дел страны. Наибольшим размахом такие преступления характеризуются в самых крупных городах республики – Минске и Гомеле, меньше всего их выявлено в Гродненской и Могилевской областях.

Если сопоставить регионы страны по абсолютной численности возрастающей или снижающейся киберпреступности за период с 2011 по 2016 год включительно, то наиболее внушительный рост преступности в сфере высоких технологий за этот период зафиксирован в городе Минске (увеличился на 386 преступлений), Гомельской (на 211 преступлений) и Витебской (114 преступлений) областях, а самый небольшой рост таких преступлений выявлен в Могилевской области. Если общую панораму социодинамики киберпреступности в регионах Беларуси выразить в процентных соотношениях, то исследуемая картина приобретает существенно иной вид. Наиболее быстрыми темпами в рассматриваемый период злоумышленные действия в сетевых структурах нарастали в столице республики, а также в Витебской и Минской областях. Наименьшим увеличением характеризуется приращение преступности в информационно-коммуникационной сфере белорусского общества на территории Могилевщины и Гродненщины.

В обширном реестре различных видов компьютерной преступности правоохранительные органы обычно выделяют два наиболее распространенных из них: а) хищения путем использования компьютеров; б) преступления против информационной безопасности.

Одной из наиболее распространенных разновидностей сетевого мошенничества, приводящего к денежным хищениям, становится изготовление, сбыт и противоправное использование поддельных кредитных или расчетных карт, в результате чего происходит преступное нарушение имущественных прав и интересов граждан – пользователей интернета. В какой бы форме ни совершалось мошенничество с использованием банковских карт, обязательно в действиях преступника содержится элемент обмана. Использует ли он поддельную карту, подбирает ли код, выдает ли себя за подлинного владельца карты – он кого-то вводит в заблуждение, обманывает для достижения своих интересов: получения денежных средств либо товаров в торговых сетях [2].

Чаще всего крупные хищения и вымогательства, осуществляемые кибермошенниками, приобретают широкий общественный резонанс. Например, в августе 2017 года неизвестный хакер взломал аккаунт минского Комаровского рынка в сети «Instagram» и потребовал выкуп в 15000 российских рублей. Еще более масштабная киберафера была организована киберпреступниками почти в то же время, когда виртуальные дельцы, прикрывающиеся псевдонимом «Mr Smith», заявили о получении доступа к популярному телесериалу «Игра престолов» и пожелали многомиллионный выкуп, а в случае отказа угрожали обнародовать сценарии фильмов и сериалов и связанную с ними служебную информацию.

В марте 2018 года в суде Центрального района г. Минска началось слушание громкого уголовного дела в отношении двух минчанок, которые обвиняются в кибермошенничестве, совершенном в особо крупном размере. Создав в социальных сетях группу под названием «Маргаритка», они предлагали купить товары по ценам гораздо ниже рыночных, при этом заказчикам ничего не поставляли. Потерпевшими от этих злодеяний признаны более 1200 человек, а нанесенный мошенницами ущерб чрезмерно доверчивым людям превысил 900 тыс. долларов[1].

[1] Ломановская, Д. Более 1200 потерпевших, ущерб в 900 тысяч долларов : «уже не надеемся, что деньги вернут» / Д. Ломановсская // Комсомольская правда в Белоруссии. – 2018. – 6 апр. – № 66(4728). – С. 6.

С учетом нарастающих масштабов роста киберпреступлений в Беларуси ведется активная работа над текстом закона, который ужесточит наказание за злодеяния в сфере кибермошенничества, киберобробмана, киберворовства и существенно сузит эту сферу. Кроме того, Беларусь, строящая IT-страну, готовится внести на рассмотрение Парламентской ассамблеи ОБСЕ резолюцию по пресечении киберпреступности [15]. В конце июля 2018 года на заседаниях 27-й сессии ПАОБСЕ белорусские парламентарии инициировали проект резолюции «Продвижение цифровой экономики в интересах обеспечения экономического роста на пространстве ОБСЕ». Этот проект получил единогласную поддержку членов Постоянного комитета ПАОБСЕ [10]. Тем самым существенно расширится ареал законодательных установлений, регулирующих и повышающих действенность мероприятий по пресечению различных видов преступлений, совершаемых с применением компьютерных технологий.

## Список использованных источников

1. Безопасность в сети [Электронный ресурс] // БЕЛТА. – Режим доступа: http://www.belta.by/onlineconference/view/bezopasnost-v-sety-praktika-borby-s-kiberprestuplenijami-906. – Дата доступа: 18.03.2018.

2. Воронцова, С. В. Киберпреступность: проблемы квалификации преступных деяний / С. В. Воронцова // Рос. юстиция. – 2011. – № 2. – С. 14–15.

3. Гладкая, Л. Ловушки из сети / Л. Гладкая // СБ. Беларусь сегодня. – 2017. – 11 авг.

4. Головенькин, А. Клубничка востребована / А. Головенькин / Комсомол. правда в Белоруссии. – 2018. – 10 янв.

5. Дробыш, А. Больше 100 мужчин стали жертвами вымогателей, занимаясь виртуальным сексом / А. Дробыш // Комсомол. правда в Белоруссии. – 2018. – 28 янв.

6. Дробыш, А. В Беларуси на 25% выросло количество преступлений в сфере высоких технологий [Электронный ресурс] / А. Дробыш // БЕЛТА. – Режим доступа: htttps://www.belta.by/society/view/pochti-75-kiberprestuplenij-v-belarusi-svjazany-s-hischenijami-288005. – Дата доступа: 06.03.2018.

7. Жур, Я. Совет: модем нужно отключать : [СК и МВД рассказали о киберпреступлениях в 2017 г.] / Я. Жур // СБ. Беларусь сегодня. – 2018. – 6 февр.

8. Зайцев, В. В Беларуси задержаны злоумышленники, похищавшие деньги через мобильный банкинг [Электронный ресурс] / В. Зайцев // БЕЛТА. – Режим доступа: https://www.belta.by/incident/view/v-belarusi-zaderzhany-zloumyshlenniki-pohischavshie-dengi-cherez-mobilnyj-banking-289097-2018/. – Дата доступа: 09.03.2018.

9. Иванович, Е. Почему Стив Джобс не разрешал своим детям айфоны? / Е. Иванович // Здоровье и успех. – 2016. – № 2. – С. 16.

10. Васильева, Н. Инициатива Минска в повестке дня ОБСЕ / В. Васильева // СБ. Беларусь сегодня. – 2018. – 20 июля.

11. Клиповое мышление и наш интеллект // Здоровье и успех. – 2016. – № 11. – С. 14–15.

12. Кузнецов, С. К. Противодействие угрозам кибербезопасности банковско-финансовой сферы Российской Федерации / С. К. Кузнецов, С. К. Лебедь, С. В. Шеремет // Вестн. акад. воен. наук. – 2017. – № 2 (59). – С. 41–45.

13. Михайлова, А. Они переходят моральные и уголовные границы / А. Михайлова // Комсомол. правда в Белоруссии. – 2018. – 10 янв.

14. Михнус, А. Цифровой секс может вытеснить реальный / А. Михнус // Комсомол. правда в Белоруссии. – 2018. – 10 янв.

15. Нестеров, А. Хакеры входят без стука / А. Нестеров // СБ. Беларусь сегодня. – 2018. – 18 марта.

16. Попова, В. Играет гормон / В. Попова // СБ. Беларусь сегодня. – 2018. – 30 июня.

17. Послянова, А. Соцсети превращают нас в тупиц / А. Послянова // Комсомол. правда в Белоруссии. – 2017. – 25 мая.

18. Самодаев, Н. Киберпреступность и киберконфликты в России [Электронный ресурс] / Н. Самодаев // D-russia.ru. – Режим доступа: http://d-russia.ru/ugrozhayushhhaya-statistika-rosta-kiberprestupnosti-v-mire.html. – Дата доступа: 11.09.2017.

19. Тельтевская, Ю. Дети под угрозой / Ю. Тельтевская // Аргументы и факты в Белоруссии. – 2018. – 20 марта. – С. 9.

20. Хрыщанович, В. Чем грозит игровая и интернет-зависимость у детей / В. Хрыщанович // СБ. Беларусь сегодня. – 2017. – 14 сент.

21. Шилак, О. МВД: «Не менее трети воспитанников школ-интерната подверглись сексуальному насилию» / О. Шилак // Комсомол. правда в Белоруссии. – 2018. – 15 марта.

## References

1. *Network security.* BelTA. Available at: http://www.belta.by/onlineconference/view/bezopasnost-v-sety-praktika-borby-s-kiberprestuplenijami-906 (accessed 18.03.2018) (in Russian).

2. Vorontsova S. V. Cybercrime: problems of qualification of criminal acts. *Rossiiskaya yustitsiya* [Russian justice], 2011, no. 2, працырр. 14–15 (in Russian).

3. Gladkaja L. Traps from the net. *SB. Belarus' segodnya* [SB. Belarus today], 2017, 11 august. (in Russian).

4. Goloven'kin A. Strawberry demand. *Komsomol'skaya pravda v Belorussii* [Komsomolskaya Pravda in Belarus], 2018, 10 January. (in Russian).

5. Drobysh A. More than 100 men became victims of extortionists, engaging in virtual sex. *Komsomol'skaya pravda v Belorussii* [Komsomolskaya Pravda in Belarus], 2018, 28 January. (in Russian).

6. Drobysh A. In Belarus, the number of high-tech crimes has increased by 25%. *BelTA*. Available at: https://www.belta.by/society/view/pochti-75-kiberprestuplenij-v-belarusi-svjazany-s-hischenijami-288005 (accessed 03.06.2018).

7. Zhur Ya. Tip: you need to disable the modem. *SB. Belarus' segodnya* [SB. Belarus today], 2018, 6 February. (in Russian).

8. Zaitsev V. In Belarus, attackers who stole money through mobile banking were detained. *BelTA*. Available at: https://www.belta.by/incident/view/v-belarusi-zaderzhany-zloumyshlenniki-pohischavshie-dengi-cherez-mobilnyj-banking-289097-2018/ (accessed 03.09.2018) (in Russian).

9. Ivanovich E. Why Steve Jobs did not allow iPhones to his children? *Zdorov'e i uspekh* [Health and Success], 2016, no. 2, pp. 16 (in Russian).

10. Vasil'eva N. The Minsk initiative on the agenda of the OSCE. *SB. Belarus' segodnya* [SB. Belarus today], 2018, 20 July. (in Russian).

11. Clip thinking and our intellect. *Zdorov'e i uspekh* [Health and Success], 2016, no. 11, pp. 14–15 (in Russian).

12. Kuznetsov S. K., Lebed' S. K., Sheremet S. V. Conrtadiction to the threats of the cybersecurity of the bank-financvial sphere of the Rissian Federation. *Vestnik akademii voennykh nauk* [Bulletin of the Academy of Military Sciences], 2017, no. 2 (59), pp. 41–45 (in Russian).

13. Mikhailova A. They cross the moral and criminal boundaries. *Komsomol'skaya pravda v Belorussii* [Komsomolskaya Pravda in Belarus], 2018, 10 January. (in Russian).

14. Mikhnus A. Digital sex can supplant real. *Komsomol'skaya pravda v Belorussii* [Komsomolskaya Pravda in Belarus], 2018, 10 January. (in Russian).

15. Nesterov A. Hackers enter without knocking. *SB. Belarus' segodnya* [SB. Belarus today], 2018, 18 March. (in Russian).

16. Popova V. Plays hormone. *SB. Belarus' segodnya* [SB. Belarus today], 2018, 30 June. (in Russian).

17. Poslyanova A. Social networks make us stupid. *Komsomol'skaya pravda v Belorussii* [Komsomolskaya Pravda in Belarus], 2017, 25 May. (in Russian).

18. Samodaev N. Cybercrime and cyber conflict in Russia. *D-russia.ru* Available at: http://d-russia.ru/ugrozhayushhhaya-statistika-rosta-kiberprestupnosti-v-mire.html (accessed 11.09.2017) (in Russian).

19. Tel'tevskaya Yu. Children Under Threat. *Argumenty i fakty v Belorussii* [Arguments and Facts in Belarus], 2018, 20 March, pp. 9 (in Russian).

20. Khryshchanovich V. What threatens gaming and Internet addiction in children. *SB. Belarus' segodnya* [SB. Belarus today], 2017, 14 September. (in Russian).

21. Shilak O. Ministry of Internal Affairs: "At least one third of boarding school pupils were sexually abused". *Komsomol'skaya pravda v Belorussii* [Komsomolskaya Pravda in Belarus], 2018, 15 March. (in Russian).

## Информация об авторе

**Бабосов Евгений Михайлович** – академик, доктор философских наук, профессор, заведующий отделом. Институт социологии, Национальная академия наук Беларуси (ул. Сурганова, 1, корп. 2, 220072, Минск, Республика Беларусь). E-mail: Isst@socio.bas-net.by

## Information about the author

**Yevgeni M. Babosov** – Academician, D. Sc. (Philos.), Professor, Head of the Department. Institute of Sociology of the National Academy of Sciences of Belarus (1 Surganov Str., Bldg 2, Minsk 220072, Belarus). E-mail: Isst@socio.bas-net.by.