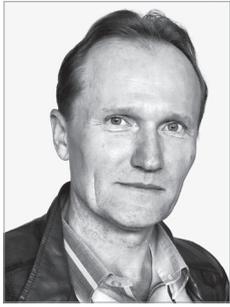


# КРИМИНАЛИСТИЧЕСКИЙ АСПЕКТ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В УСЛОВИЯХ ИНФОРМАТИЗАЦИИ И ЦИФРОВИЗАЦИИ ОБЩЕСТВА

УДК 343.98

**А.М.ХЛУС,**кандидат юридических наук, доцент,  
доцент кафедры криминалистики, докторант  
Белорусского государственного университета

hlus.home@mail.ru

## АННОТАЦИЯ

В статье рассматриваются общественные процессы информатизации и цифровизации. В связи с этим прогнозируются некоторые опасные тенденции в развитии современного общества. Содержание этих тенденций определяет роль криминалистической науки в системе мер ограничения проявлений их негативного воздействия на личность, общество и государство. Сделан вывод о необходимости развития прогностической и профилактической функций криминалистической науки, а также использования процессов информатизации и цифровизации общества с целью антикоррупционного воспитания граждан и профилактики коррупционных правонарушений.

**Ключевые слова:** информатизация, цифровизация, общество, информация, информационное пространство, криминалистика, прогнозирование, профилактика.

Современное общество характеризуется новым этапом развития. Происходит постепенный переход от информационного к цифровому обществу. Такой переход требует от научного сообщества пересмотра научных позиций, формирования новых подходов к исследованию теоретических и прикладных проблем. А в аспекте противодействия преступности необходимо использование всего позитивного, что связано с этими процессами, для профилактики преступности и предупреждения отдельных видов преступлений. Для понимания связи этих этапов с развитием современной преступности следует вначале рассмотреть их позитивные и негативные стороны.

Формированию информационного общества предшествует масштабное внедрение компьютерной техники, современных средств получения, обработки и передачи информации в различные сферы жизнедеятельности человека. Это повлекло за собой развитие информационной коммуникации, постоянно совершенствуемой на основе новых информационных технологий. Все это ориентировано на удовлетворение информационных потребностей и реализацию прав и законных интересов органов власти, организаций и граждан на основе создания и использования информационных ресурсов.

Положительной чертой информационного общества является процесс компьютеризации. Это создает условия для массового доступа к надежным источникам информации, а также предполагает преимущественную занятость работающих в сфере производства, хранения, переработки и ре-

лизации информации, особенно высшей ее формы – знаний.

Вследствие стремительного развития науки и техники происходит постепенный и поступательный переход в единое информационное пространство всего мирового сообщества. Следующим этапом в его развитии является цифровизация.

На фоне позитивных проявлений информационное общество имеет и отрицательную сторону. Не анализируя весь спектр негативных явлений, связанных с информатизацией общества, укажем на некоторые из них в аспекте рассматриваемой нами темы.

На личность человека может оказать отрицательное воздействие нежелательная информация, которая специально содержится либо умышленно «заброшена» третьими лицами в информационный контент.

Само по себе наличие информации и возможность доступа к ней – это благо для современного человека. Но о благе можно вести речь только в том случае, если информация носит позитивный (полезный) для него характер. Реальность же такова, что информация может быть как позитивной, так и негативной.

Негативная информация – это такие «сведения, которые целенаправленно оказывают воздействие на сознание человека, вызывают отрицательные эмоции и могут существенно влиять на психологическую структуру (свойства) его личности. Такая информация может являться основой для формирования у человека устойчивой ориентации на совершение преступлений и иных противоправных деяний» [1, с. 52].

Следовательно, доступ к информации деструктивного характера следует ограничивать, так как не все люди в равной степени устойчивы к восприятию негативных сведений. В связи с этим возникает необходимость обеспечения на государственном уровне безопасности пользования информацией. Причем эта безопасность должна

обеспечиваться во всех информационных ресурсах. Особенно это касается образовательных информационных ресурсов, сосредоточенных в интернете, где нередко размещено «огромное количество недостоверной, тенденциозной, идеологически вредной информации, порой выходящей за рамки этических норм» [2, с. 16]. Представляются недостаточными контроль и управление доступом субъектов системы образования (школьников и студентов) к образовательной информации в интернете. Главным здесь, по нашему мнению, должна быть «фильтрация» информации на сайтах, которой пользуется молодое поколение. Это достаточно сложный процесс, но в этом направлении должны приниматься соответствующие меры на государственном уровне.

Широкое распространение информации о негативных действиях людей может служить иницилирующим фактором для аналогичных деяний, совершаемых после ознакомления с ней. Современные средства массовой информации (далее – СМИ), в том числе и интернет, изобилуют примерами совершения различными категориями людей негативных деяний, среди которых преобладают правонарушения. С такой информацией знакомятся и психически неуравновешенные люди, испытывающие какие-либо жизненные трудности и ищущие выход из них. Оценка и неверные выводы о событии экстраполируются на личную ситуацию, выход из которой видится аналогичным образом. Как возможность выхода из трудной ситуации человек, имеющий деструктивные наклонности, совершает деяние, подобное тому, которое явилось публичной сенсацией.

В качестве примера можно рассмотреть ситуации, связанные с ложными сообщениями о минировании административных и иных зданий. СМИ, в том числе интернет, доводят до населения эту негативную информацию, которая, собственно, и является питательной средой для новых подобных деяний. Телефонного хулигана не пугает строгость уголовной ответственности. Он, по всей видимости, испытывает глубокое психологическое удовлетворение, осознавая (или даже наблюдая), что множество людей находятся в состоянии сильнейшего волнения и страха, вызванных его деянием. Для Российской Федерации это стало одной из серьезных проблем. Сообщается, что «массовые звонки о «минировании» учреждений и торговых центров охватили 75 из 85 регионов России. По оценке Федеральной службы безопасности, только в Москве ущерб от «минирований» составил 150 млн рублей. Всего было эвакуировано почти 2 млн человек из тысяч торговых центров, вокзалов и других объектов по стране. Ни в одном случае угроза взрывов не подтвердилась» [3].

Полагаем, что тиражируемая в СМИ и интернете информация об имеющих место в учебных заведениях США случаях вооруженных нападений школьников на своих педагогов и одноклассников спровоцировала подобные нападения и в нашей республике [4].

Информационная сфера – это «поле» для реализации различных технологий манипулирования сознанием пользователей информацией. В зависимости от целевой направленности эти технологии могут иметь различный характер: как откровенно враждебные для человека, разрушающие его личность, так и формирующие у него отрицательные качества (стяжательство, корысть и тому подобное).

В контексте этой проблемы вспоминается организованная в интернете игра для подростков «Синий кит», в результате которой имели место случаи суицидальных смертей детей, участвующих в этой игре. Общественность забила тревогу в связи с этой игрой после публикации под названием «Группы Смерти» в «Новой газете» 15 мая 2016 года. Журналисты утверждали, что с 2015 по начало 2016 года из-за участия в игре погибли около 130 детей.

Не анализируя в деталях технологию воздействия на личность данной игры, мы считаем подобные негативные проявления возможными. Свои убеждения подкрепим примерами реализации манипуляционных технологий, которые применяются на законных основаниях практически ежедневно и с ними каждый гражданин сталкивается не единожды. Например, сфера торговли сопровождается постоянным использованием манипуляций сознанием потребителей.

Способы манипулирования потребителями на грани мошенничества нами рассмотрены ранее. Они связаны с новым, ранее неизвестным способом реализации товаров, осуществляемой строго определенным образом – на так называемых «презентациях» [5, с. 31]. Действия «презентантов» вписываются в обычную схему мошенничества, представляют собой управляющее воздействие субъекта на объект.

В последнее время количество проводимых таким образом «презентаций» увеличилось. Причина такой ситуации кроется в следующем. Во-первых, манипулирование сознанием потребителя на грани мошенничества имеет высокий уровень организации, что, как следствие, не влечет за собой жалоб (претензий) со стороны потенциальных «жертв», которые в подавляющем большинстве случаев даже не в состоянии оценить те действия, которые в отношении них совершены. Во-вторых, если нет жалоб, то нет и реагирования правоохранителей, которые подобные ситуации рассматривают как дела частного обвинения.

Современное информационное пространство все чаще превращается в арену противоборства государств, вражда которых сначала достигает уровня информационной войны, а затем – кибервойны.

Информационная война представляет собой организованное на государственном уровне вмешательство в информационное пространство другого государства [6]. «Кибервойна – это действия, представляющие собой кибератаки одного или нескольких государств, направленные на проникновение в

компьютерную сеть государственных органов, иных критически важных объектов другого государства с целью нанесения ущерба или разрушения. Основными видами кибератак являются: вандализм (порча интернет-страниц, замена их содержания оскорбительными текстами и картинками); кибершпионаж (взлом серверов с целью сбора секретной информации); пропаганда (рассылка по интернет-сетям пропагандистских текстов); повреждение серверов (нарушение нормальной работы государственных компьютерных систем); информационно-психологическое воздействие на население (целью является создания паники, распространение тревожных слухов и дезинформации) и др.» [7, с. 33].

Создается основа для всеобщего контроля за населением в масштабах как отдельно взятых государств, так и мирового сообщества в целом. Данная глобальная проблема имеет конспирологический характер. Детально мы рассмотрели ее ранее [8, с. 41–51].

В информационном пространстве все больше совершается преступлений, что определяет тенденцию увеличения их удельного веса в объеме всей преступности.

Данное обстоятельство ставит перед криминалистической наукой задачу постоянного совершенствования имеющихся и разработки новых эффективных частных методик расследования компьютерных преступлений.

Выше мы обозначили некоторые проблемы, связанные с информатизацией общества. Для цифровизации, учитывая ее тесную связь с информатизацией, характерны те же проблемы, на которые мы уже обратили внимание.

Цифровизацию в настоящее время ученые рассматривают в узком и широком смысле. В узком смысле цифровизация – это преобразование аналоговой информации в цифровую форму. Дальнейшее использование такой «оцифрованной» информации возможно только в случае ее обратного преобразования в аналоговую. Положительным в вопросе цифровизации в узком смысле является возможность преобразования огромного массива обычной (аналоговой) информации в ее цифровую форму.

В широком смысле цифровизация представляет собой «современный общемировой тренд развития экономики и общества, который основан на преобразовании информации в цифровую форму и приводит к повышению эффективности экономики и улучшению жизни» [9, с. 46]. Такое представление цифровизации звучит весьма оптимистично и отражает только положительные стороны данного процесса. На его начальном этапе еще трудно судить о влиянии цифровизации на экономику государств. При этом остается без ответа вопрос о равных преимуществах цифровизации для государств с разным уровнем развития экономики.

Что касается «улучшения жизни» в связи с цифровизацией, то здесь опять же невозможно дать од-

нозначный ответ. С одной стороны, процессы цифровизации (а равно и информатизации как ее основы) расширяют возможности современного человека в получении и использовании разносторонней информации, приобретении услуг и товаров. Но с другой стороны, эта сфера представляет и опасности для человека. И здесь мы имеем в виду не только внешнее воздействие на человека.

Сама по себе цифровизация, как бы это нелогично ни выглядело, является ограничивающим фактором в развитии человека, что в итоге приводит его к страхам, постоянному стрессу и, как результат, психическим расстройствам. Не с этим ли связано появление в ряду человеческих зависимостей таких, как игромания, компьютерные игры, которые с точки зрения медицины трактуются как психические расстройства?

На данную проблему обратил внимание А.Г.Чернышев, который заметил, что «компьютерные игры не оставляют простора воображению» [10], так как все заранее спланировано их разработчиками.

Новые поколения людей обречены жить в условиях глобальной «цифры», и это неоспоримый факт. Но «цифровая» эпоха не меняет самого человека, «не может изменить генный код самого человеческого существа» [10], а меняет условия, в которых он вынужден жить. Не изменяются в связи цифровизацией общества традиционные приоритеты родового и социального человека.

Достижению многих деструктивных целей, в том числе и обозначенных, будет способствовать установление коррупционных отношений. И здесь надо иметь в виду не ту коррупцию, с которой борются правоохранительные органы на национальном уровне, а коррупцию международного уровня и ее определенную форму – политическую коррупцию [11, с. 78].

Важной в аспекте обозначенных проблем является роль криминалистической науки. По нашему мнению, криминалистика должна отказаться от обычного «следования» за произошедшим преступным событием, а должна его предсказывать и разрабатывать необходимые меры опережающего характера. Представляется, что в таких случаях криминалистике следует изменить свои функциональные приоритеты.

Криминалистическое прогнозирование должно осуществляться на этапе, предшествующем совершению преступного деяния. Такая возможность представляется в процессе осуществления экспертизы нормативных правовых актов, а также криминалистического анализа возникающих новых общественных отношений. В ходе экспертизы может быть создана модель криминальной деятельности, на основе которой определяются отражательные возможности элементов материальной структуры преступления, его последствия и меры, направленные на его предотвращение. Только на такой основе возможна под-

готовка обоснованных предложений об устранении выявленных в проектах правовых актов (правовых актах) недостатков, способствующих возникновению криминальных рисков.

Важное значение в аспекте противодействия преступной деятельности имеет криминалистическая профилактика. Такая функция криминалистики недостаточно разработана. Однако, на наш взгляд, в условиях информатизации и цифровизации общества такое направление криминалистики приобретает особую значимость.

Реализовать эту функцию криминалистики возможно в рамках криминалистического обеспечения раскрытия, расследования и предупреждения преступлений.

Обязательной составной частью криминалистического обеспечения является внедрение, то есть реализация, научных криминалистических разработок. Внедрение М.В.Субботина рассматривает в качестве самостоятельного и весьма важного этапа криминалистического обеспечения практической деятельности. Способы внедрения научных разработок М.В.Субботина разделила на три вида:

- 1) обучение;
- 2) издание научной литературы для самостоятельного изучения;
- 3) компьютеризация расследования (внедрение специализированных программ) [12, с. 79].

Указанные способы внедрения научных разработок не ориентированы на профилактику совершения преступлений. Их основное назначение – обеспечение практических работников криминалистическими знаниями, необходимыми для раскрытия и расследования преступлений.

На это же обращает внимание и Ю.П.Гармаев: он полагает обязательным уточнить перечень способов внедрения криминалистических разработок в практику.

Рассматривая обучение как способ внедрения методики расследования, Ю.П.Гармаев считает, что «необходимо расширять круг адресатов – конечных потребителей рекомендаций. Традиционные потребители – это следователи, иные представители стороны обвинения в уголовном процессе, судьи. Нетипичные, нетрадиционные потребители – это значительно более широкий круг лиц. Считаем очевидным, что соответствующие криминалистические и шире – межотраслевые разработки могут и должны быть адресованы не только их «традиционным конечным потребителям», но и потребителям нетипичным, прежде всего, потерпевшим и иным гражданам, относящимся к «группе риска» стать таковыми» [13, с. 31–32]. К такому мнению можно отнестись с осторожностью, если основываться только на понимании основного назначения методик расследования – обеспечении практической деятельности по раскрытию и расследованию преступлений. В таком случае возникает закономерный вопрос: зачем зна-

ния об этой методике «потерпевшим и иным гражданам, относящимся к «группе риска»? [13, с. 32]. Но если углубиться в понимание идеи, высказанной Ю.П.Гармаевым, то ее вполне можно принять в части «преобразования криминалистических разработок для профессионалов в рекомендации просветительского характера» [14, с. 48].

Мы же считаем, что в данном случае надо вести речь не о «просвещении» иных лиц (граждан), которое представляет собой «распространение знаний, образования» [15, с. 504], а о профилактике совершения с их стороны преступлений.

Далее, рассматривая методики расследования преступлений коррупционной направленности, Ю.П.Гармаев указывает на профилактику. Используя данный подход, необходимо, как считает Ю.П.Гармаев, учитывать важное методологическое правило: криминалистическая характеристика названных преступлений может формироваться и представляться в двух формах – «профессиональной» и «просветительской». Так, в рамках такой «процедуры преобразования» могут быть созданы рекомендации «О противодействии провокации, подстрекательству и иным незаконным методам борьбы с коррупцией; а также о том, как человеку не допустить вовлечения себя в эти противоправные деяния в типичных, хорошо знакомых каждому жизненных ситуациях» [14, с. 48–49].

Такие рекомендации представляются существенными для тех видов преступлений, где наличествует физическое лицо в качестве потерпевшего. Но это свойственно не каждому преступлению, предусмотренному Особенной частью Уголовного кодекса Республики Беларусь (далее – УК). В ряде случаев не оправданно говорить о подобных рекомендациях и в отношении методик группового характера. Придать «просветительский» характер всем методикам расследования преступлений коррупционной направленности не представляется возможным по причине их различий касательно объекта посягательства.

Например, для такого коррупционного преступления, как легализация средств, полученных преступным путем (ст. 235 УК), не является характерным наличие потерпевшего. Совсем иная ситуация складывается, если говорить о вымогательстве взятки (ч. 2 ст. 430 УК), когда в качестве объекта посягательства выступает конкретный гражданин.

«Преобразование» криминалистических разработок, по мнению Ю.П.Гармаева, должно иметь вид памяток, кратких пособий, видеофильмов, буклетов, адресуемых не только следователям и оперативным работникам, но и подозреваемым (обвиняемым), а также потерпевшим [14, с. 48]. Мы считаем, что сейчас информация может быть доведена (получена) и иным путем, например, посредством интернета.

Для практических работников весьма актуальными являются специальные программные продукты в виде приложений для мобильных телефонов, план-

шетных и стационарных компьютеров, ноутбуков. Их число в настоящее время весьма немногочисленно, но спрос на них растет.

Идея, высказанная Ю.П.Гармаевым, вызывает интерес, так как она ориентирована на предупреждение и профилактику преступлений.

На основе изложенного представляется возможным сделать некоторые выводы.

Процессы информатизации и цифровизации общества, наряду с положительным, содержат ряд негативных проявлений.

Наиболее опасными для благополучия как отдельных государств, так и мирового сообщества в целом являются следующие отрицательные проявления информатизации и цифровизации: широкий доступ к негативной информации, которая способствует деструктивным проявлениям психически неадекватных людей; расширение возможностей для реализации различных технологий манипулирования сознанием пользователей, информацией; противостояние государств на уровне информационной и кибервойн; контроль за населением в масштабах как отдельно взятых государств, так и мирового сообщества в целом; совершение преступлений общегосударственного характера.

Своевременное противодействие негативным проявлениям информатизации и цифровизации общества предполагает развитие прогностической и профилактической составляющих криминалистической науки.

Возрастающий уровень межгосударственной конкуренции в сфере развития информационных технологий, а также формирование национального информационного контента повлекут за собой увеличение количества и усложнения коррупционных отношений.

Процессы информатизации и цифровизации общества целесообразно использовать для антикоррупционного воспитания граждан и профилактики коррупционных правонарушений.

1. Хлус, А.М. Основы формирования деструктивного поведения личности и роль криминалистики в их познании / А.М.Хлус // Вестник КазНПУ имени Абая, серия «Юриспруденция». – 2015. – №1 (39). – С. 50–54.

2. Абламейко, С.В. Стратегия информатизации и информационная безопасность системы образования в условиях развития информационного общества / С.В.Абламейко, Ю.И.Воротницкий, Н.И.Листопад [Электронный ресурс]. – Режим доступа: <http://elib.bsu.by/bitstream/123456789/105304/4/12-17.pdf>. – Дата доступа: 27.05.2019.

3. В Москве из банка эвакуировали людей после сообщения о минировании [Электронный ресурс]. – Режим доступа: <https://ria.ru/20190210/1550651299.html>. – Дата доступа: 20.06.2019.

4. ЧП в Столбца: в результате нападения ученика в школе погибли учительница и школьник [Электронный ресурс]. – Режим доступа: <https://news.tut.by/society/625839.html>. – Дата доступа: 20.06.2019.

5. Хлус, А.М. Мошенничество или способ современной торговли? / А.М.Хлус // Законность и правопорядок. Правовой научно-практический журнал. – Минск, 2016. – №3. – С. 28–33.

6. Почепцов, Г.Г. Информационные войны: базовые параметры [Электронный ресурс]. – Режим доступа: [psyfactor.org/psyops/infowar9.htm](http://psyfactor.org/psyops/infowar9.htm). – Дата доступа: 12.04.2016.

7. Бабосов, Е.М. Учет особенностей кибервойны в организации и обеспечении национальной безопасности / Е.М.Бабосов // Криминалистическая структура преступлений против информационной безопасности / Информационная безопасность как составляющая национальной безопасности государства: материалы Междунар. науч.-практ. конф., Минск, 11–13 июля 2013 г.: в 3 т. / Ин-т нац. безопасности Респ. Беларусь; редкол.: С.Н.Князев (гл. ред.) [и др.]. – Минск, 2013. – Т. 1. – 174 с.

8. Хлус, А.М. Глобализация как причина коррупции и роль криминалистики в ее нейтрализации / А.М.Хлус // Вестник Карагандинского государственного университета. Серия «Право». – 2017. – №3 (87). – С. 41–51.

9. Халин, В.Г. Цифровизация и ее влияние на Российскую экономику и общество: преимущества, вызовы, угрозы и риски / В.Г.Халин, Г.В.Чернова // Управленческое консультирование. – 2018. – №10. – С. 46–62.

10. Чернышев, А.Г. Цифровизация и технологизация общественной жизни как социально-политическая проблема: сохранение идентичности и роль государства в условиях развития глобальных сетей [Электронный ресурс]. – Режим доступа: <https://cyberleninka.ru/article/v/tsifrovizatsiya-i-tehnologizatsiya-obshchestvennoy-zhizni-kak-sotsialno-politicheskaya-problema-sobranenie-identichnosti-i-rol>. – Дата доступа: 23.05.2019.

11. Хлус, А.М. Тенденции уголовного права и криминологии на современном этапе противодействия коррупции / А.М.Хлус // Вестник Карагандинского государственного университета. Серия «Право». – 2018. – №2 (90). – С. 70–80.

12. Субботина, М.В. Криминалистические проблемы расследования хищений чужого имущества: дис. ... д-ра юрид. наук / М.В.Субботина. – Волгоград, 2004. – С. 79.

13. Гармаев, Ю.П. Внедрение криминалистических методик расследования в практику: проблемы и пути их решения / Ю.П.Гармаев // Организационно-методические проблемы расследования: материалы Всерос. науч.-практ. конф.; отв. ред. В.Д.Зеленский. – Краснодар: КубГАУ, 2016. – С. 30–35.

14. Гармаев, Ю.П. Правовое просвещение в криминалистике / Ю.П.Гармаев // Криминалистические чтения на Байкале – 2015: материалы Междунар. науч.-практ. конф. / Вост.-Сиб. фил. ФГБОУВО «РГУП»; отв. ред. Д.А.Степаненко. – Иркутск, 2015. – С. 45–50.

15. Ожегов, С.И. Словарь русского языка: ок. 57 000 слов; под ред. чл.-корр. АН СССР Н.Ю.Шведовой. – 20-е изд., стереотип. – М.: Рус. яз., 1988. – 750 с.

*Материал поступил в редакцию 25.07.2019*

A.M.KHLUS

#### **Criminalistics aspect of anti-crime enforcement in the context of informatization and digitalization of society**

The article discusses the social processes of informatization and digitalization. In this regard, some dangerous trends in the development of contemporary society are being predicted. The content of these trends determine the role of criminalistics science in the system of measures to limit the manifestations of their negative impact on the individual, society and the state. The conclusion is drawn about the need to develop prognostic and preventive functions of criminalistics science, as well as to use the processes of informatization and digitalization of society with the aim of anti-corruption education of citizens and the prevention of corruption offenses.

**Keywords:** *informatization, digitalization, society, information, information space, criminalistics, forecasting, prevention measures.*

Рецензент: Б.В.АСАЕНОК, кандидат юридических наук, доцент, начальник цикла гражданско-правовых и уголовно-правовых дисциплин кафедры юридических дисциплин факультета внутренних войск Военной академии Республики Беларусь