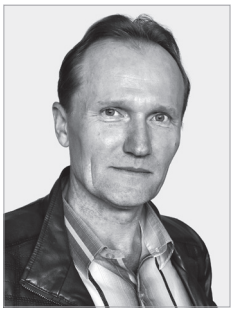

КРИМИНАЛИСТИЧЕСКАЯ НАУКА В УСЛОВИЯХ ФОРМИРОВАНИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Александр ХЛУС,
кандидат юридических наук, доцент,
доцент кафедры криминалистики юридического факультета
Белорусского государственного университета

АННОТАЦИЯ

В статье определяется содержание опасных тенденций в развитии информационного общества и роль криминалистической науки в системе мер ограничения их негативного воздействия на личность, общество и государство.

ANNOTATION

The article defines the content of the dangerous trends in the development of the information society and the role of forensic science in the system of measures to limit their negative impact on the individual, society and state.

Стремительное развитие науки и техники способствует постепенному и поступательному переходу всего мирового сообщества к информационному обществу, функционирующему в едином информационном пространстве.

Криминалистическая наука в начале третьего тысячелетия оказалась в переходном состоянии, когда происходит осознание необходимости нового знания, формируются новые научные парадигмы. Это обусловлено переходом от индустриального к информационному обществу. Такой переход требует от научного сообщества пересмотра многих научных позиций, формирования новых подходов к исследованию теоретических и прикладных проблем.

Для нашего государства развитие информационного общества – одно из приоритетных направлений, целями которого являются обеспечение устойчивого социально-экономического, политического и культурного развития страны, улучшение качества жизни людей, создание широких возможностей для удовлетворения потребностей и свободного развития личности и общества [1].

В связи с постепенным переходом мирового сообщества в информационное общество прогнозируются некоторые опасные тенденции в развитии информационного общества, в числе которых можно назвать следующие:

1) активизация влияния средств массовой информации на общество посредством использования разнообразных средств воздействия на психику людей;

2) активное использование современных информационных технологий для вторжения в частную жизнь людей и в деятельность организаций;

3) разработка и использование современных технологий для организации всеобщего контроля за населением как отдельно взятых государств, так и мирового сообщества в целом;

4) превращение информационного пространства в арену противоборства государств, вражда которых достигает уровня информационной войны;

5) значительное увеличение совершения в информационном пространстве преступлений.

Рассмотрим содержание этих тенденций и определим роль криминалистической науки в системе мер ограничения проявлений их негативного воздействия на личность, общество, государство.

Во-первых, все большее влияние на общество будут оказывать средства массовой информации (далее – СМИ) со всем арсеналом телекоммуникационного воздействия на психику людей.

Для понимания влияния СМИ на общество необходимо рассмотреть особенности процесса формирования личности современного человека. На него оказывают влияние различные факторы, которые условно можно разделить на две группы: внутренние и внешние.

Внутренние факторы связаны с природными личностными качествами и свойствами конкретного индивидуума.

В качестве внешних факторов рассматривается сложившаяся в обществе система мер воспитательного характера. Данная система складывается из внутрисемейного и организованного в рамках государственных образовательных учреждений воспитания, а также информационной сферы (среды).

Степень влияния на личность указанных выше факторов различна. Но в современных условиях существенное и определяющее значение для становления личности имеет информационная сфера (среда). Она представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений [2, с. 119].

Данная сфера нередко подвергается противоправному воздействию, что влечет за собой необходимость принятия адекватных мер, направленных на обеспечение ее безопасности.

Важным источником воздействия на личность являются СМИ.

Под СМИ согласно ст. 1 Закона Республики Беларусь от 17 июля 2008 года «О средствах массовой информации» понимается форма периодического распространения массовой информации с использованием печати, вещания теле- или радиопрограммы, глобальной компьютерной сети Интернет.

В настоящее время главным источником массированного агитационно-пропагандистского воздействия на сознание людей является глобальная система Интернет. В Интернете нередко распространяется информация, которая способна провоцировать совершение правонарушений, служит основой для развития негативных проявлений, например, ксенофобии, экстремизма. Кроме того, содержание такой информации способствует формированию у отдельных личностей устойчивого деструктивного поведения [3, с. 50–54].

Следовательно, далеко не вся информация, с которой человеку приходится сталкиваться, приносит ему пользу. При этом информация может быть не только бесполезной, но и вредной. Вредная по своему содержанию информация не направлена на удовлетворение потребностей человека. Она является средством негативного воздействия, и в этом случае человек от нее должен быть защищен. Целевое назначение такого воздействия различно: запугивание, формирование устойчивого чувства страха и так далее.

Действия лиц, заинтересованных в распространении негативной информации, представляют собой различные технологии скрытого управляющего воздействия. В результате такого воздействия человек может оказаться в ситуации принуждения, когда он не свободен в выборе своих действий. Принудить – значит «заставить что-нибудь сделать» [4, с. 483] в интересах тех, кто является организатором распространения определенной информации.

В век технологического прогресса современные люди не представляют свою жизнь без СМИ. Основное назначение этих средств – доведение информации до широких слоев населения как внутри государства, так и за его пределами. Но это является хорошим делом при условии, что информация носит объективный и позитивный характер. Все зависит от содержания и способов представления информации, доведения ее до масс.

Вредоносная, негативного характера информация представляет собой информационные угрозы, которые исследователи подразделяют на информационный вандализм, криминал и терроризм [5, с. 87].

Проявления информационного вандализма связаны с распространением недостоверных порочащих фактов, некорректными высказываниями, неосторожными либо умышленными публикациями карикатур популярных личностей. Внешняя безобидность информационного вандализма может иметь серьезные последствия, связанные с разрушением информационной среды и совершением преступлений. Например, об этом свидетельствуют события, произошедшие во Франции 7 января 2015 года, когда в офис сатирического журнала «Charli Hebdo» ворвались вооруженные люди и убили 12 человек. Поводом этому послужила опубликованная карикатура пророка Мухаммеда [6, с. 255–259].

Информационный криминал может быть связан с хулиганским мотивом, но преимущественно имеет корыстную цель. Так, например, группа мошенников, используя вредоносный код, блокировала браузеры пользователей Интернета. Затем демонстрировалась пользователю страница, где от имени правоохранительных органов (МВД, прокуратуры и других) мошенники требовали заплатить штраф за просмотр и хранение порнографии. В результате этого были обмануты около 380 белорусов [7].

Информационный терроризм нередко направлен на принуждение к реализации политических, экономических, религиозных и других целей. К большому сожалению, СМИ не анализируют возможность негативных последствий распространения определенного рода информации. Они также не несут ответственности за те реальные последствия, которые вызваны распространенной информацией.

Закон о СМИ устанавливает ответственность за недостоверную информацию. Но даже достоверная информация не всегда является полезной для общественного сознания. Дело в том, что ее распространение может оказать содействие преступной деятельности, например, способствуют нагнетанию страха в связи с совершением террористического акта. Для понимания этого необходимо рассмотреть сущностное содержание терроризма.

Как явление терроризм включает в себя несколько взаимосвязанных элементов: 1) идеологию терроризма (теории, концепции, идейно-политические платформы), имеющую определенную целевую направленность; 2) террористическое структурное образование (международные или национальные террористические организации, религиозные и другие общественные организации, организованная преступность и так далее); 3) террористическую деятельность (практика совершения преступлений и иных противоправных действий террористической направленности). Терроризм (от лат. *terror* – страх, ужас) – это прежде всего устрашение людей посредством осуществляемого насилия. При этом для терроризма характерно наличие двух целей. Одна из них основная, связанная с идеологической

концепцией, а вторая вспомогательная – запугать властные структуры, общественность и добиться от них реализации основной цели. Логичен вывод, что в достижении вспомогательной цели террористам способствуют СМИ (газеты, радио, телевидение), которые часто нагнетают страх в обществе, к чему и стремятся преступники, совершая насильственные преступления.

В Советском Союзе не было терроризма в нынешнем его понимании. Объясняется это несколькими причинами. Во-первых, государство окутывало подобные события плотной завесой секретности, что обеспечивало спокойствие граждан и не являлось «примером» для других. Во-вторых, завеса секретности исключала возможность достижения целей террористического акта. Советские СМИ не брали интервью у преступников и не транслировали сцены насилия. Что же происходит сегодня? Например, телевидение можно рассматривать как соучастника террористов. Оно вдумчиво и творчески делает именно то, что требуется террористам. Настало новое время – время «экранного терроризма» [3, с. 52].

Следовательно, можно сделать вывод, что СМИ играют ключевую роль в формировании и обеспечении состояния информационной безопасности.

Важным направлением в обеспечении информационной безопасности является своевременное предупреждение возникновения информационных угроз. Выявление их источников и принятие соответствующих мер, направленных на недопущение совершения противоправных действий в будущем, возможно в процессе расследования преступлений при изучении личности обвиняемого. В этих целях в ходе расследования целесообразно использовать разработанный в криминалистике метод субъектно-функционального анализа. Данный метод предполагает исследование функций, осуществляемых для достижения преступного результата. В процессе анализа исследуются сознательные волевые действия, проявления функций человека в наступивших вредных последствиях преступления.

Субъектно-функциональный анализ также обеспечивает возможность выявления всего, что послужило основанием для формирования конкретных свойств (качеств) личности обвиняемого и в итоге определило мотивацию и направленность криминального умысла [9, с. 71].

Во-вторых, информационные технологии все активнее будут использоваться для вторжения в частную жизнь людей и в деятельность организаций.

Компьютерная техника, мобильные средства связи, их программное обеспечение, телекоммуникационные системы, информационные технологии охватывают все сферы жизнедеятельности современного человека, в том числе и его личную жизнь. Право на личную жизнь многогранно. Оно объединяет следующие самостоятельные права: сохранять в тайне, никому не сообщать информацию о себе; в некоторых случаях сохранять свою личность в тайне; вести беседу таким образом, чтобы она не стала достоянием посторонних лиц; тайно встречаться с некоторыми людьми, не афишируя свое общение с ними; оставаться наедине с собой; жить так, чтобы не привлекать к себе внимание других людей.

Реализация перечисленных прав во многих случаях затруднена.

В-третьих, создается основа для всеобщего контроля за населением в масштабах как отдельно взятых государств, так и мирового сообщества в целом.

Показателен в этом вопросе пример Российской Федерации, где принят Федеральный закон от 27 июля 2010 года №210-ФЗ «Об организации предоставления населению государственных и муниципальных услуг». Согласно ст. 22 данного Закона гражданам Российской Федерации на основе их заявления выдается универсальная электронная карта (далее – УЭК). Данная карта представляет собой материальный носитель, содержащий визуальную (графическую) и электронную (машиносчитываемую) информацию о пользователе картой и обеспечивающий доступ к информации о пользователе картой, используемой для удостоверения прав пользователя картой на получение государственных и муниципальных услуг, иных услуг, в том числе для совершения юридически значимых действий. Фактически УЭК является идентификационным и платежным средством. УЭК заменяет медицинский полис и страховое пенсионное свидетельство, объединяет одновременно банковскую карту, электронный кошелек, электронную подпись и проездной билет. В предусмотренных случаях УЭК является документом, удостоверяющим личность и иные права гражданина. Она позволяет оплачивать государственные и муниципальные услуги.

Все изложенное для непосвященного человека покажется положительным. Но, как и у любой медали, здесь также имеется обратная сторона. Дело в том, что введение УЭК, по мнению ее противников, может явиться только первым этапом на пути к достижению глобальной цели – тотальный контроль за населением земного шара. Такая мысль может показаться абсурдной, если не обратить внимания на иные принятые и до сих пор действующие нормативные правовые акты.

В первую очередь особого внимания требует Стратегия развития электронной промышленности России на период до 2025 года от 7 августа 2007 года №311 (далее – Стратегия), согласно которой «внедрение нанотехнологий должно еще больше расширить глубину ее проникновения в повседневную жизнь населения» [10]. Безусловно, за прошедшие почти 10 лет с момента принятия Стратегии имеет место невиданный ранее скачок

в техническом прогрессе. Разработка и внедрение УЭК является тому подтверждением. Техническое совершенство само по себе является положительным фактором в развитии человечества. Проблема кроется в ином. Как сказано в Стратегии, «должна быть обеспечена постоянная связь каждого индивидуума с глобальными информационно-управляющими типа Интернет». Как же ее можно обеспечить? Данную проблему УЭК может решать при условии постоянного ее нахождения у владельца (ношение в кармане, сумке и так далее). Но так не всегда будет происходить, так как человеку свойственна забывчивость, рассеянность, невнимательность, умышленность действий. Чтобы подобное исключить и обеспечить «постоянную связь индивидуума с глобальными управляющими», разработчики Стратегии предлагают иной способ.

Люди в Стратегии названы биообъектами, с которыми наноэлектроника будет интегрироваться и «обеспечивать непрерывный контроль за поддержанием их жизнедеятельности, улучшением качества жизни, и таким образом сокращать социальные расходы государства». Получается, что тот чип, который имеется в УЭК, предполагается внедрить в тело человека.

Идея массового внедрения электронных устройств в организм человека не может быть поддержана, так как это исключает свободу и равенство между людьми и в итоге приведет к ограничению государственного суверенитета. Вместе с тем идентификационные свойства внедряемых электронных устройств могут быть использованы в правоохранительной практике. По решению суда электронные устройства на определенный срок следовало бы применять в отношении определенной категории лиц, представляющих опасность для общества и государства. Речь идет о рецидивистах, лицах, совершивших тяжкие и особо тяжкие преступления, отбывающих наказание за уголовные преступления вплоть до снятия судимости, и других. Перечень таких лиц следует определить на уровне закона.

Какова роль криминалистической науки в период реализации такой государственной программы? 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.

Функции криминалистической науки представляют собой определенные направления и содержание ее исследований. В теории криминалистики выделяют следующие функции криминалистики: 1) познавательную; 2) прогностическую; 3) преобразовательную; 4) синтезирующую; 5) организующую; 6) функцию создания технических, тактических и методических основ расследования; 7) функцию аккумуляции знаний других наук, которые могут быть использованы в процессе расследования [11, с. 10–11].

Перечисленные функции криминалистики взаимосвязаны, но имеют различное значение для практической деятельности по расследованию. Учитывая «сервисный» характер криминалистики, доминирующую роль играют функции, призванные обеспечивать процесс расследования преступлений. Синтезирующая функция значима для научной деятельности. Она способствует формированию результатов научных исследований в законченные научные теории. В меньшей степени имеет отношение к практике расследования и прогнозирующая функция.

Считается, что криминалистика должна не только изучать явления, но и иметь возможность прогнозировать их дальнейшее развитие. Содержание прогностической функции в криминалистике проявляется двояко: прогнозирование преступления (его последствий) и прогнозирование деятельности по расследованию [11, с. 11].

В первом случае прогнозирование направлено на установление связей между объектами, субъектами, их взаимодействий, последствий, поведение преступника после совершения преступления и так далее.

Во втором случае оно обеспечивает деятельность следователя по познанию прошлого преступного события, реализацию взаимоотношений в ходе расследования.

Такой подход к реализации прогностической функции криминалистики, по нашему мнению, не в полной мере раскрывает ее содержание и направленность. Криминалистическое прогнозирование должно осуществляться на этапе, предшествующем совершению преступного деяния. Такая возможность представляется в процессе осуществления экспертизы нормативных правовых актов, а также криминалистического анализа стремительно 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 подготовка обоснованных предложений об устранении выявленных в проектах правовых актов (правовых актах) недостатков, способствующих возникновению криминальных рисков.

В-четвертых, современное информационное пространство все чаще превращается в арену противоборства государств, вражда которых вначале достигает уровня информационной войны, а затем – кибервойны.

Информационная война представляет собой организованное на государственном уровне вмеша-

тельство в информационное пространство другого государства [12]. 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 иллюстрациями); 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 создание паники, распространение тревожных слухов и дезинформации) и другие [13, с. 33]. В кибервойне невозможно определить не только участников, время ее начала и завершения, но и трудно доказать во многих случаях сам факт применения разрушительного кибероружия. Сложным также является определение, имела место организованная на государственном уровне кибератака или действовала группа, преследующая собственные преступные цели. Решение этой проблемы предполагает потребность в эффективных методах, разработка которых должна основываться на криминалистических знаниях.

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

Формирование мирового информационного общества связано с расширением преступного интереса в информационной сфере. Уже сейчас имеет место тенденция ежегодного увеличения так называемых компьютерных преступлений. Можно с уверенностью прогнозировать в ближайшем будущем значительный рост преступлений, совершаемых в информационном пространстве. Данное обстоятельство ставит перед криминалистической наукой задачу постоянного совершенствования имеющихся и разработки новых эффективных частных методик расследования компьютерных преступлений: преступлений против целостности и доступности компьютерных данных и систем; преступлений, связанных с содержанием информации; преступлений, связанных с использованием компьютерных, телекоммуникационных средств, и других.

Все эти методики должны учитывать ряд проблемных особенностей совершения компьютерных преступлений: во-первых, высокую квалификацию лиц, совершающих такие преступления; во-вторых, их умение профессионально скрывать следы преступления; в-третьих, пространственное различие места совершения преступных действий и места непосредственного причинения вреда (нередко преступник находится под юрисдикцией другого государства); в-четвертых, специфику следов отражения компьютерного преступления, которые выходят за рамки традиционного понятия «след в криминалистике».

Традиционная криминалистика не в состоянии решить многие обозначенные проблемы. С учетом изложенного напрашивается вывод о том, что для расследования разнообразных групп компьютерных преступлений требуются не только новые методики, но и новая криминалистика – информационная криминалистика.

1. Абламейко, С.В. Информационное общество в Беларуси: наука и образование [Электронный ресурс] / С.В.Абламейко, В.В.Анищенко. – Режим доступа: www.bsu.by/Cache/pdf/451073.pdf. – Дата доступа: 21.03.2016.

2. Веруш, А.И. Национальная безопасность Республики Беларусь: курс лекций / А.И.Веруш. – Минск: Амалфея, 2012. – 204 с.

3. Хлус, А.М. Основы формирования деструктивного поведения личности и роль криминалистики в их познании / А.М.Хлус // Вестник КазНПУ имени Абая. – Серия «Юриспруденция». – №1 (39). – 2015 – 94 с.

4. 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.

5. Юсупов, Р.М., Осипов, В.Ю. Информационный вандализм, криминал и терроризм. Проблемы противодействия // Теоретические и прикладные проблемы информационной безопасности: тез. докл. Междунар. науч.-практ. конф. (Минск, 21 июня 2012 г.) / М-во внутр. дел Респ. Беларусь, учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь». – Минск: Акад. МВД, 2012. – С. 87–90.

6. Козлик, И. Не чувствуешь грани – плати жизнью / И.Козлик // Комсомольская правда. – 2015. – №2 (14–20 января).

7. Рак, Ю. Задержали интернет-мошенников, воровавших под маской МВД [Электронный ресурс] / Ю.Рак. – Режим доступа: http://www.sb.by/proisshestviya/news/zaderzhali-internet-moshennikov-sobiravshikh-shtrafy-pod-maskoy-mvd.html. – Дата доступа: 04.02.2016.

8. Раззаков, Ф.И. Век террора / Ф.И.Раззаков. – М.: ЗАО Издво ЭКСМО, 1997. – 432 с.

9. Хлус, А.М. Криминалистическое изучение личности обвиняемого с целью выявления основ его деструктивного поведения / А.М.Хлус // Юстиция Беларуси. – 2015. – №9. – С. 70–73.

10. Об утверждении Стратегии развития электронной промышленности России на период до 2025 года: Приказ Минпромэнерго от 7.08.2007 №311 [Электронный ресурс]. – Режим доступа: base.consultant.ru/cons/cgi/online/cgi?base=LAW;n=99457;reg=doc. – Дата доступа: 06.04.2016.

11. Криминалистика: учебное пособие /А.В.Дулов [и др.]; под ред. А.В.Дулова. – Минск: ИП «Экоперспектива», 1996. – С. 10–11.

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

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

Материал поступил в редакцию 18.04.2016