Современные проблемы права, экономики и управления. Электронный журнал. – 2016. - № 2(3). – 474 с. – С. 292-299. – box@izuvpa.ru

УДК 343.98
ББК 67.52

НЕГАТИВНЫЕ ТЕНДЕНЦИИ ИНФОРМАЦИОННОГО ОБЩЕСТВА И РОЛЬ КРИМИНАЛИСТИКИ В ИХ НЕЙТРАЛИЗАЦИИ

Хлус Александр Михайлович,
кандидат юридических наук, доцент,
доцент кафедры криминалистики
Белорусского государственного университета,
г. Минск, Беларусь
hlus.home@mail.ru

NEGATIVE TRENDS OF THE INFORMATION SOCIETY AND THE ROLE CRIMINALISTICS IN THEIR NEUTRALIZATION

Khlus Alexander,
PhD, Associate Professor,
Associate Professor of Department of Criminalistics
Belarusian State University,
Minsk, Belarus, hlus.home@mail.ru

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.

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.

Ключевые слова: информационное общество, информация, криминалистика, нанотехнологии, универсальная электронная карта (УЭК).

Keywords: information society, information, criminalistics, nanotechnology, Universal Electronic Card (UEC).

Информационное общество представляет собой современный этап в развитии цивилизации. Его формированию предшествует внедрение компьютерной техники, современных средств получения, обработки и передачи информации в различных сферах жизнедеятельности человека.

Изобретение микропроцессорных технологий, появление и широкое применение персональных компьютеров повлекло за собой развитие информационной коммуникации, которая постоянно совершенствуется с появлением новых информационных технологий. Все это создало условия для удовлетворения информационных потребностей и реализации прав и законных интересов органов власти, организаций и граждан на основе создания и использования информационных ресурсов.

Отличительная особенность информационного общества состоит в том, что во всех сферах жизнедеятельности человека, общества и государства доминирующее положение занимают знания и информация. Информационно-коммуникационные технологии оказывают воздействие на образ жизни людей, их образование и работу, а также на взаимодействие государства и гражданского общества.

Развитие информационного общества для Беларуси является одним из приоритетных направлений, целями которого являются:

1) обеспечение устойчивого социально-экономического, политического и культурного развития страны;

2) улучшение качества жизни людей;

3) создание широких возможностей для удовлетворения потребностей и свободного развития личности и общества [1].

Стремительное развитие науки и техническое совершенствование способствует постепенному и поступательному переходу мирового сообщества в информационное общество, функционирующее в едином информационном пространстве. В развитии информационного общества, при всей внешней положительности рассматриваемых процессов, можно прогнозировать ряд тенденций опасных для человечества. Рассмотрение содержания этих тенденций позволяет определить роль криминалистической науки в системе мер, ограничивающих их негативное воздействие на личность, общество, государство.

Во-первых, формирование информационного общества превращает информационное пространство в арену противоборства государств. Высокая степень вражды превращает современное информационное пространство в военную арену. Вначале противостояние между государствами достигает уровня информационной войны, а затем - кибервойны.

Информационная война представляет собой организованное на государственном уровне вмешательство в информационное пространство другого государства [10]. 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. [2, 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.

Во-вторых, развитие информационного общества будет способствовать увеличению количества совершаемых в информационном пространстве преступлений. Это, в свою очередь, 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 др.

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».

В-третьих, все большее влияние на общество будут оказывать средства массовой информации со всем арсеналом телекоммуникационного воздействия на психику людей.

Для понимания степени воздействия средств массовой информации на общество необходимо рассмотреть особенности процесса формирования личности современного человека. Этот процесс непрерывный и длительный. 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, присущими конкретному индивидууму. В их числе можно назвать, например, наличие интеллекта, целеустремленность, уважительное (или негативное) отношение к другим людям, альтруизм, дисциплинированность и т.п.

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, и информационной сферы (среды), окружающей человека на протяжении всей его жизни.

В процессе жизнедеятельности человек воспринимает, оценивает и накапливает разноплановую информацию (сведения). При этом сформировавшаяся на определенном жизненном этапе личность способна меняться в результате оказываемого на нее информационного воздействия.

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 [3, с. 119]. Данная сфера нередко подвергается противоправному воздействию, что влечет за собой необходимость принятия адекватных мер, направленных на обеспечение ее безопасности.

В процессе жизнедеятельности человек получает информацию из различных источников. В их числе ближайшее окружение человека, т.е. тот социум, с которым он соприкасается. Еще более важным источником воздействия на личность являются средства массовой информации.

Под средством массовой информации (далее СМИ), согласно статье 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 Интернета.

Из перечисленных СМИ в настоящее время главным источником массированного агитационно-пропагандистского воздействия на сознание людей является глобальная система Интернет. В Интернете и в иных СМИ нередко распространяется информация, которая способна провоцировать совершение правонарушений, служит основой для развития негативных проявлений, например, ксенофобии, экстремизма. И, кроме того, содержание такой информации способствует формированию у отдельных личностей устойчивого деструктивного поведения [13, с. 50-54].

Следовательно, далеко не всякая 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 от нее человек должен быть защищен. Целевое назначение такого воздействия различно: запугивание, формирование устойчивого чувства страха и т.д.

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» [8, с. 483] в интересах тех, кто является организатором распространения определенной информации.

В век технологического прогресса современные люди не представляют свою жизнь без СМИ. Основное назначения 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. В тоже время она имеет и оборотную сторону. Все зависит от содержания и способов передачи информации, доведения ее до масс.

Вредоносная, негативного характера, информация являет собой информационные угрозы, которые исследователи подразделяют на информационный вандализм, криминал и терроризм [14, 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, где в офис сатирического журнала «Charli Hebdo» ворвались вооруженные люди и убили 12 человек. Поводом этому послужила опубликованная карикатура пророка Мухаммеда [4, с. 255-259].

Другой пример не связан с такими страшными последствиями, но указывает на стремление распространителей информации о частной жизни не столько скомпрометировать высшее должностное лицо, сколько опорочить действующую государственную власть, вызвать к ней недоверие. Так, высокопоставленный чиновник «уличен» в строительстве загородного коттеджа, оценочная стоимость которого составляет около 1 млн. долларов. Построить такой дом, находясь на государственной службе, невозможно. Изложенный в Интернете материал предполагает логический вывод о возможных злоупотреблениях должностного лица [6]. Такая информация требует проверки. Но, к сожалению, до сих пор, ни подтверждения, ни опровержения распространенной информации нет. Если она ложная, то честь чиновника и, в первую очередь, человека должна быть защищена. В противном случае у обывателя складывается негативное впечатление, переходящее в негативное отношение к органам государственной власти. В приведенном примере инициатива для защиты должностного лица должна исходить от государства, так как, затронув честь и достоинство человека, злоумышленник одновременно посягает на репутацию государства.

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 [11].

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 для них 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.

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. 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 [12, с. 71].

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

Для Республики Беларусь данная проблема не стоит остро. Но это только на сегодняшний день. Никто не может гарантировать, что в скором будущем она не обострится.

Показателен в этом вопросе пример Российской Федерации, где в 2010 году принят закон «Об организации предоставления населению государственных и муниципальных услуг». Согласно ст. 22 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 обеспечивающей 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 [7]. 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. При этом их заказ и оплата производится по принципу «не выходя из дома». Посредством УЭК можно: оплатить лекарства и услуги; приобрести билеты на все виды транспорта и пополнить транспортный электронный кошелек; купить полис КАСКО; оплатить штрафы и регистрацию транспортного средства (постановка на учет и снятие с учета); узнать состояние лицевого пенсионного счета; зарегистрировать брак и рождение ребенка; оплатить коммунальные услуги и налоги и т.д.

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 7.08. 2007 № 311 (далее «Стратегия»), согласно которой «внедрение нанотехнологий должно еще больше расширить глубину ее проникновения в повседневную жизнь населения» [9]. Безусловно, за прошедшие почти 10 лет с момента принятия «Стратегии» имеет 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: носит в кармане, в сумке и т.п. Но так не всегда будет происходить, так как человеку свойственна забывчивость (УЭК забыл дома, в ином месте), рассеянность, невнимательность (УЭК утеряна), умышленность действий (сознательно не взял с собой). Чтобы подобное исключить и обеспечить «постоянную связь индивидуума с глобальными управляющими» разработчики «Стратегии» предлагают иной способ.

При этом каждый «индивидуум» уже не считается человеком. 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-биобъекта, фактически превратив его в нанобиоробота, так как на него будет воздействовать посредством Интернет «глобальный управляющий».

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 др. Перечень таких лиц следует определить на уровне закона.

Куда предполагается внедрить электронное устройство (чип) становится понятным после дальнейшего ознакомления со «Стратегией».

Рассуждая о перспективном техническом развитии, разработчики «Стратегии» утверждают, что «широкое распространение получат встроенные беспроводные наноэлектронные устройства, обеспечивающие постоянный контакт человека с окружающей его интеллектуальной средой, получат распространение средства *прямого беспроводного контакта мозга человека с окружающими его предметами, транспортными средствами и другими людьми* (курсив наш – А.Х.). Тиражи такой продукции превысят миллиарды штук в год из-за ее повсеместного распространения».

В настоящее время Россия находится на третьем этапе (2016 - 2025 годы) развития «Стратегии», предусматривающем:

завоевание значимых позиций в ряде секторов мирового рынка электронной компонентной базы;

широкое внедрение достижений отечественных нанотехнологии, биоэлектроники и микросистемной техники в повседневную жизнь человека в сферах здравоохранения, образования, жилищно-коммунального хозяйства, транспорта и связи.

Какая 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 [5, 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 [5, с. 11].

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

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.

Традиционная криминалистика не в состоянии решить многие обозначенные проблемы. С учетом изложенного напрашивается вывод, что необходимо не только совершенствование процесса расследования разнообразных групп компьютерных преступлений, но и новая криминалистика – криминалистика сферы высоких технологий.

Список литературы

1. Абламейко, С.В., Анищенко В.В. Информационное общество в Беларуси: наука и образование: [Электронный ресурс] Режим доступа: www.bsu.by/Cache/pdf/451073.pdf. Дата доступа: 27.10.2016.

2. Бабосов, Е.М. Учет особенностей кибервойны в организации и обеспечении национальной 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. – С. 33.

3. Веруш, А. И. Национальная безопасность Республики Беларусь : курс лекций / А. И. Веруш. – Минск : Амалфея, 2012. – 204 с. – С. 119.

4. Козлик, И. Не чувствуешь грани – плати жизнью / Комсомольская правда. № 2. – 14-20 января 2015 г.

5. Криминалистика: учебное пособие /А.В. Дулов [и др.]; под ред. А.В. Дулова. – Минск: ИП «Экоперспектива», 1996. – 415 с. – С. 10-11.

6. Министр Щеткина завершает строительство коттеджа в Дроздах [Электронный ресурс] Режим доступа: nn.by?c=ar&land=ru. Дата доступа: 27.10.2016.

7. Об организации предоставления государственных и муниципальных услуг: Федеральный закон от 27.07.2010 № 210-ФЗ (ред. от 15.02.2016) [Электронный ресурс]

Режим доступа: /www.consultant.ru/document/ cons_dok_LAW_103023. Дата доступа: 05.04.2016.

8. Ожегов, С.И. Словарь русского языка: Ок. 57 000 слов/ Под ред. чл.-корр. АН СССР Н. Ю. Шведовой. – 20- изд., стереотип. М.: Рус. яз., 1988. – 750 с. – С. 493.

9. 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.

10. Почепцов, Г.Г. Информационные войны: базовые параметры. [Электронный ресурс] Режим доступа: psyfactor.org/psyops/infowar9.htm. Дата доступа: 27.10.2016.

11. Рак, Ю. Задержали интернет-мошенников, воровавших под маской МВД : [Электронный ресурс] Режим доступа: http://www.sb.by/proisshestviya/news/zaderzhali-internet-moshennikov-sobiravshikh-shtrafy-pod-maskoy-mvd.html. Дата доступа: 27.10.2016.

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

13. Хлус, А.М. Основы формирования деструктивного поведения личности и роль криминалистики в их познании / Вестник КазНПУ имени Абая, серия «Юриспруденция», № 1(39), 2015 – 94 с. – С. 50-54.

14. 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. – 320 с. – С. 87.

References

1. Ablamejko, S.V., Anishchenko V.V. Informacionnoeobshchestvo v Belarusi: nauka i obrazovanie: [EHlektronnyjresurs] Rezhimdostupa: www.bsu.by/Cache/pdf/451073.pdf. Datadostupa: 27.10.2016.

2. Babosov, E.M. Uchetosobennostejkibervojny v organizacii i obespecheniinacional'nojbezopasnosti / Informacionnayabezopasnost' kaksostavlyayushchayanacional'nojbezopasnostigosudarstva :materialyMezhdunar. nauch.-prakt. konf., Minsk, 11-13 iyulya 2013 goda : v 3 t. / In-t nac. bezopasnostiResp. Belarus' ;redkol. : S. N. Knyazev (gl. red.) [i dr.]. – Minsk, 2013. – T. 1. – 174 s. – S. 33.

3. Verush, A. I. Nacional'nayabezopasnost' RespublikiBelarus' :kurslekcij / A. I. Verush. – Minsk :Amalfeya, 2012. – 204 s. – S. 119.

4. Kozlik, I. Ne chuvstvuesh' grani – platizhizn'yu / Komsomol'skayapravda. № 2. – 14-20 yanvarya 2015 g.

5. Kriminalistika: uchebnoeposobie /A.V. Dulov [i dr.]; pod red. A.V. Dulova. – Minsk: IP «EHkoperspektiva», 1996. – 415 s. – S. 10-11.

6. Ministr SHCHetkina zavershaet stroitel'stvo kottedzha v Drozdah [EHlektronnyjresurs] Rezhimdostupa: nn.by?c=ar&land=ru. Data dostupa: 27.10.2016.

7. Ob organizaciipredostavleniyagosudarstvennyh i municipal'nyhuslug: Federal'nyjzakonot 27.07.2010 № 210-FZ (red. ot 15.02.2016) [EHlektronnyjresurs] Rezhimdostupa: /www.consultant.ru/document/ cons_dok_LAW_103023. Data dostupa: 05.04.2016.

8. Ozhegov, S.I. Slovar' russkogoyazyka: Ok. 57 000 slov/ Pod red.chl.-korr. AN SSSR N. YU. SHvedovoj. – 20- izd.,stereotip. M.: Rus. yaz., 1988. – 750 s. – S. 493.

9. Ob utverzhdeniiStrategiirazvitiyaehlektronnojpromyshlennostiRossiina period do 2025 goda: PrikazMinpromehnergoot 7.08.2007 № 311. [EHlektronnyjresurs] Rezhimdostupa: base.consultant.ru/cons/cgi/online/cgi?base=LAW;n=99457;reg=doc. Data dostupa: 06.04.2016.

10. Pochepcov, G.G. Informacionnyevojny: bazovyeparametry. [EHlektronnyjresurs] Rezhimdostupa: psyfactor.org/psyops/infowar9.htm. Data dostupa: 27.10.2016.

11. Rak, YU. Zaderzhali internet-moshennikov, vorovavshih pod maskojMVD : [EHlektronnyjresurs] Rezhimdostupa: http://www.sb.by/proisshestviya/news/zaderzhali-internet-moshennikov-sobiravshikh-shtrafy-pod-maskoy-mvd.html. Data dostupa: 27.10.2016.

12. Hlus, A.M. Kriminalisticheskoeizuchenielichnostiobvinyaemogo s cel'yuvyyavleniyaosnov ego destruktivnogopovedeniya // YUsticiyaBelarusi. – 2015. - № 9. – S. 70-73.

13. Hlus, A.M. Osnovyformirovaniyadestruktivnogopovedeniyalichnosti i rol' kriminalistiki v ihpoznanii / VestnikKazNPUimeni Abaya, seriya «YUrisprudenciya», № 1(39), 2015 – 94 s. – S. 50-54.

14. YUsupov, R.M., Osipov, V.YU. Informacionnyjvandalizm, kriminal i terrorizm.Problemyprotivodejstviya / Teoreticheskie i prikladnyeproblemyinformacionnojbezopasnosti: tez. dokl. Mezhdunar.nauch.-prakt. konf., (Minsk, 21 iyunya 2012 g.) / M-vovnutr. del Resp. Belarus', uchrezhdenieobrazovaniya «Akad. M-vavnutr.del Resp. Belarus'». – Minsk :Akad. MVD, 2012. – 320 s. – S. 87.