Н.Г. Муратова, И.О. Антонов

ТЕХНОЛОГИЯ ДОКАЗЫВАНИЯ ТРАНСНАЦИОНАЛЬНОГО КИБЕРМОШЕННИЧЕСТВА

В статье исследованы наиболее значимые аспекты технологии доказывания по уголовным делам о транснациональных кибермошенничествах. Выделены и описаны факторы, оказывающие существенное влияние на эффективность технологии доказывания по уголовным делам данной категории. Показано значение для эффективности доказывания транснационального кибермошенничества: 1) адекватной существующим угрозам процессуальной регламентации деятельности правоохранительных органов; 2) организации рационального взаимодействия на всех уровнях государственных органов и негосударственных организаций, специализирующихся на борьбе с транснациональной киберпреступностью; 3) грамотной непроцессуальной и процессуальной деятельности по выявлению следов кибермошенничества в Интернете.

Ключевые слова: киберпреступления; кибермошенничество; доказывание; расследование; международное сотрудничество; оперативно-розыскная деятельность; транснациональная преступность; Интернет.

Проблема эффективного противодействия криминальным посягательствам в глобальных компьютерных сетях как никогда актуальна для современной криминалистической науки. Помимо несомненного позитивного вклада в развитие цивилизации Интернет расширил и возможности для совершения криминальных посягательств, в том числе транснациональных. С ростом количества пользователей информационно-телекоммуникационных сетей расширяется потенциальный круг тех, кто может стать жертвой киберпреступников, включая и кибермошенников. В этой связи нельзя не отметить, что, по оценкам Минкомсвязи России, среди стран Европы Российская Федерация вышла на первое место по числу пользователей Интернета, а также занимает лидирующие позиции по числу доменов второго уровня в национальных интернет-зонах. Кроме того, немаловажным является и то, что процесс роста продолжается – в России фиксируется заметная положительная динамика по росту количества пользователей Сети среди россиян [15].

В связи с этим особое место в криминалистическом обеспечении деятельности правоохранительных органов приобретает методика расследования так называемых киберпреступлений («компьютерные преступления», «преступления в сфере высоких технологий», «информационные преступления»), важнейшей особенностью которых считается использование сетей компьютера для совершения преступления в виртуальном пространстве [11, с. 339]. Среди киберпреступлений одними из наиболее часто встречающихся являются различные варианты криминального обмана. По оценкам МВД России, именно мошенничества являются самыми распространенными преступлениями в IT-среде, и их количество растет с каждым годом [4].

В 2012 г. согласно данным, предоставленным Бюро специальных технических мероприятий МВД России, в РФ было выявлено на 70% больше самых массовых и прибыльных видов киберпреступлений – мошенничеств и краж денежных средств со счетов граждан и организаций, чем в предыдущем году [6].

Криминальный обман в киберпространстве весьма разнообразен. В Сети можно встретить практически все классические способы мошеннических посягательств. Например, благодаря ресурсам Интернета злоупотребления в сфере благотворительности приобрели трансграничный масштаб и перешли в разряд одного из самых распространенных видов онлайн-мошенничества [19]. Новые варианты проведения досуга современного человека также не остаются вне поля зрения мошенников. Сравнительно новой разновидностью преступлений данного вида можно считать мошеннические действия с аккаунтами игроков в онлайновые игры [2].

Одними из самых распространенных и известных считаются мошеннические действия в сфере интернет-торговли. Фактически преступники смогли перенести традиционные для мошенничества сценарии криминального обмана в виртуальную среду, чтобы иметь возможность незаконно обогащаться за чужой счет. Трудно не согласиться с выводом о том, что мошенничать пытались со всеми когда-либо изобретенными коммерческими системами и в этой связи электронная торговля не будет ничем отличаться от них, не изменятся и методы преступников [22, с. 32].

Проблемы противодействия транснациональной преступности не могли не найти отражения в решениях, принятых самыми различными международными организациями. Например, XI Конгресс ООН по предупреждению преступности и уголовному правосудию (Бангкок, 18–25 апреля 2005 г.) обратил особое внимание на совершенствование законодательства и разработку и реализацию единой системы общесоциальных и специальных мер борьбы с транснациональной преступностью [23, с. 8–9].

Кроме того, во время работы Конгресса на семинаре-практикуме № 5 «Меры по борьбе против экономических преступлений, включая отмывание денег» говорилось о значении борьбы с хищениями личных данных как инструменте для совершения преступления в будущем или как фактическом использовании личной информации с целью совершения преступления (кража кошельков, документов, почтовых отправлений, кредитных карточек, несанкционированное копирование электронно-цифровых данных, получение личной информации об умершем, получение базовой информации о лице из интернет-ресурсов, получение личной информации от коррумпированных сотрудников государственных учреждений и частных компаний с целью изготовления поддельных документов), так как в законодательстве большинства государств не предусмотрено такое преступление, как «хищение личных данных» [23, с. 110].

Российский законодатель также отреагировал на актуальные тенденции развития киберпреступности в мире и внес изменения в действующее законодательство. В частности, в последние годы в этой связи претерпел изменения Уголовный кодекс Российской Федерации. Была усилена уголовная ответственность по ст.ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» и 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ». Были выделены в самостоятельные составы такие разновидности криминального обмана, как мошенничество с использованием платежных карт (ст. 159.3 УК РФ) и мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ).

В последнее время в уголовно-процессуальной науке, теории доказывания и криминалистике все более востребованным становится термин «технология». Он

используется в самых различных контекстах. Что касается вопросов расследования преступлений, то для примера здесь можно назвать наиболее часто встречающиеся сочетания – «технология расследования», «криминалистическая технология», «технология доказывания», «технология преодоления трудностей расследования», «технологии в области фиксации информации». Востребованность термина «технология» можно объяснить высокой сложностью деятельности по осуществлению уголовного судопроизводства, в которой можно выделить помимо интенционального, методического, операционального аспектов и технологический аспект. Технологический аспект во всех значениях этого слова еще более заметен, когда речь идет о киберпреступлениях. В теории доказывания, согласно позиции, которая выглядит, на наш взгляд, достаточно обоснованно, под технологией доказывания можно понимать прежде всего построение, динамическое развитие и обоснование следственных версий в процессе доказывания [16].

В рамках одной статьи невозможно остановиться подробно на всех составляющих технологии доказывания транснационального кибермошенничества, мы лишь проанализируем те, которые, на наш взгляд, можно назвать ключевыми.

При осуществлении доказывания по уголовным делам о кибермошенничестве субъекты предварительного расследования сталкиваются с целым рядом сложностей самого различного порядка.

Эти сложности во многом предопределяются выявленными тенденциями современной киберпреступности, важнейшими из которых можно назвать: 1) рост преступлений корыстной направленности среди криминальных деяний данного вида. Как отмечают в МВД России, если раньше киберпреступность нередко была результатом бравирования, хвастовства, то в настоящее время в действиях киберпреступников совершенно определенно виден корыстный мотив [20]; 2) увеличение размера нанесенного материального ущерба. Так, по итогам исследования, проведенного Институтом Понемон (*Ponemon Institute*), в результате вторжений с помощью вредоносных программ крупные бизнес-структуры ежегодно теряют примерно по 6 млн долларов США, причем, каждая из них ежемесячно подвергается в среднем 72 успешным для киберпреступников атакам [18, с. 30]. В поле внимания киберпреступников находятся и обычные пользователи. По данным исследования *Norton by Symantec*, число жертв среди россиян в 2012 г. превысило 31 млн. человек, а сумма нанесенного ущерба находится в пределах 2 млрд долларов [1]; 3) рост в киберпространстве количества криминальных деяний, совершенных организованными преступными формированиями; 4) высокий уровень латентности кибермошенничества. Так, по некоторым оценкам, лишь 10–12% киберпреступлений становятся достоянием гласности [11, с. 340]. Согласно опубликованным данным, правоохранительным органам становится известно только 10–15% случаев от реального числа мошенничеств с использованием банковских карт [14, с. 3].

Как и в любой другой технологии, в технологии доказывания кибермошенничества определяющими являются характеристики субъекта, ее реализующего. Учитывая специфику современного кибермошенничества, можно в связи с этим предположить, что технологию доказывания данных составов преступления может успешно реализовать только такой субъект доказывания, который, во-первых, уверенно ориентируется во всех аспектах функционирования современного транснационального киберпространства, во-вторых, имеет соответствующие ресурсы для выявления следов криминальной деятельности в киберпространстве, в-третьих, способен применять вариативные методы выявления транснациональных кибермошенничеств с учетом положений иностранного уголовно-процессуального

законодательства и особенностей криминалистических методик, применяемых за рубежом при расследовании данной разновидности криминального обмана.

Иными словами, качество профессиональной подготовки сотрудников правоохранительных органов имеет самое непосредственное отношение к обеспечению приемлемого качества доказывания по уголовным делам о кибермошенничестве. То, что уровень профессиональной подготовки может не всегда в полной мере соответствовать уровню поставленных задач, отмечается в работах авторов, исследовавших проблемы расследования преступлений данного вида [10, с. 6]. По оценкам специалистов, в некоторых случаях заметной проблемой может быть даже плохое знание английского языка сотрудниками правоохранительных органов [18, с. 35].

В качестве одной из важнейших составляющих в технологию доказывания транснационального кибермошенничества необходимо включить правовой компонент реализации международной единой стратегии противодействия киберпреступности, которая предполагает определенную унификацию национальных уголовных законодательств государств, осуществляющих такое противодействие.

Транснациональный характер кибермошенничества предопределяет большое значение взаимодействия субъектов доказывания по данной категории уголовных дел на международном уровне.

Правовую основу такого взаимодействия должны образовывать международные нормативные акты, предусматривающие разумную по содержанию и срокам процедуру, отвечающую интересам каждого субъекта взаимодействия.

В литературе справедливо отмечалось, что необходимость международного сотрудничества при расследовании транснациональных киберпреступлений определяется потребностями практической деятельности национальных правоохранительных органов в получении доказательств на территории других государств, в обеспечении реализации предусмотренных законом уголовно-процессуальных функций и осуществления правосудия [5, с. 5]. Трудно не согласиться с выводами специалистов в сфере информационной безопасности о том, что без международного сотрудничества эффективная борьба с киберпреступностью невозможна, так как она не имеет национальности и не знает границ, и в рамках одной страны бороться с ней не имеет смысла [12].

На международном уровне одной из не урегулированных проблем остается проникновение при проведении расследования в информационные сети другого государства, без соответствующего уведомления и разрешения на такие действия с его стороны (так называемая проблема установления границ национального «цифрового» суверенитета при глобальной дигитализации всего мира).

В литературе описан случай, когда ФБР США, занимаясь расследованием ряда преступлений (в том числе и мошенничества), совершенных двумя гражданами РФ, нарушило, по мнению ФСБ России, законодательство Российской Федерации, в связи с чем российскими правоохранительными органами было инициировано уголовное преследование (ст. 272 ч. 2 УК РФ), а сотрудник ФБР США был обвинен в несанкционированном проникновении в российские компьютерные сети [9, с. 300–301].

Нельзя не учитывать, что в настоящее время международное сотрудничество РФ в области обеспечения информационной безопасности осуществляется в условиях обострения международной конкуренции за обладание технологическими и информационными ресурсами, за доминирование на рынках сбыта, в условиях продолжения попыток создания структуры международных отношений, основанной на односторонних решениях ключевых проблем мировой политики, противодействия укреплению роли Российской Федерации как одного

из влиятельных центров формирующегося многополярного мира, усиления технологического отрыва ведущих держав мира [8, с. 133].

Наличие проблем в выстраивании эффективного взаимодействия в связи с несовершенством нормативной базы признается в правоохранительных органах. В МВД России считают, что совершенствование национального и международного законодательства является важной задачей, а также признают, что это долгий и нелегкий процесс [3].

В целом в последние годы на международном уровне отмечается как увеличение количества случаев взаимовыгодных контактов, так и повышение качественных характеристик взаимодействия специализированных подразделений правоохранительных органов в уголовном преследовании при расследовании выявленных случаев кибермошенничества. В частности, в свое время эффективными были признаны результаты сотрудничества по отдельным уголовным делам с правоохранительными органами Великобритании, Италии, Франции и Германии [7].

Деятельность по формированию необходимой нормативной базы предполагает разработку новых и совершенствование существующих законов, положений, постановлений и инструкций. Совершенствование нормативной базы должно осуществляться непрерывно, так как сетевые технологии в наше время развиваются семимильными шагами, и многие из них практически мгновенно становятся востребованными пользователями Сети. Такое быстрое развитие предопределяет появление новых правоотношений, требующих соответствующей правовой регламентации.

Законодательная база в сфере противодействия транснациональному кибермошенничеству включает в себя международные договоры Российской Федерации, федеральные законы, указы Президента РФ, постановления Правительства РФ, межведомственные и ведомственные руководящие нормативные акты.

В этой связи можно отметить, что ряд действующих международных соглашений РФ содержит положения, в которых в той или иной степени регламентируется доказывание по уголовным делам о киберпреступности[1].

В такого рода международных соглашениях фиксируются самые различные формы сотрудничества. Как правило, устанавливаются параметры информационного обмена между сторонами, пределы совместного планирования и координации совместных мероприятий при выявлении и расследовании киберпреступлений.

Качество доказывания по уголовным делам о кибермошенничестве во многом будет предопределяться тем, насколько успешными окажутся усилия по выработке единых международных подходов в сфере борьбы с киберпреступностью, и кибермошенничеством в том числе. Потребность в принятии универсального международного правового акта, обеспечивающего приемлемый уровень взаимодействия международных правоохранительных организаций, правоохранительных органов разных стран, но при этом в достаточной степени уважающий суверенитет государств, принимающих участие в таком взаимодействии, оценивается и теоретиками, и практиками борьбы с киберпреступностью как весьма высокая.

В настоящее время признается, что механизм построения конструктивных взаимоотношений субъектов доказывания транснационального кибермошенничества недостаточно разработан. Существование многочисленных договоров России о правовой помощи с другими государствами, федеральных законов, которые их ратифицируют, иных конвенций и

[1] См., например: Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (заключено в г. Минске 01.06.2001) // URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=INT;n=9210

ратифицирующих их федеральных законов, национальных систем законодательства порой не могут обеспечить субъекту доказывания правильное понимание и применение конкретных норм международного или национального права.

Свою специфику в технологию доказывания по уголовным делам о транснациональном кибермошенничестве вносит и то, что эти преступления нередко совершаются организованными преступными формированиями. Характерным примером, показывающим, насколько сложна и специфична может быть технология доказывания по делам о кибермошенничестве, служит операция «Карточный магазин» по одновременному задержанию по подозрению в совершении преступления 24 человек в нескольких странах мира (США, Великобритания, Босния, Болгария, Норвегия, Германия, Италия, Япония). Задержанные обвинялись в использовании Интернета для совершения мошеннических действий с банковскими счетами и личной информацией сотен тысяч человек. Помимо названных государств следственные действия по данному делу проводились в Австралии, Канаде, Дании и Македонии [13].

Технология доказывания по уголовным делам о кибермошенничестве включает в себя широкое использование результатов оперативно-розыскной деятельности, которая, безусловно, в этой сфере имеет ярко выраженную специфику.

Состав кибермошенничества предполагает наличие у субъектов оперативно-розыскной деятельности и предварительного следствия разносторонних знаний и навыков прежде всего в области современных компьютерных технологий, функционирования информационных систем и информационно-телекоммуникационных сетей.

Решение задач оперативно-розыскной деятельности при выявлении и расследовании кибермошенничества невозможно без использования самых современных аппаратно-программных средств. Учитывая, что киберпреступники традиционно стремятся использовать в своей криминальной деятельности последние достижения научной и технологической мысли, те, кто им противостоит, не должны позволять себе отставания в этом аспекте. От уровня оснащенности самыми совершенными аппаратно-программными средствами отечественных правоохранительных органов зависит во многом и эффективность принимаемых ими мер в противостоянии кибермошенничеству.

Для выявления и расследования кибермошенничества правоохранительными органами задействуются как универсальное программное обеспечение, так и специализированное – предназначенное изначально для решения более узкого круга задач. Известно, что специализированные программы способны осуществлять поиск и сбор оперативно значимой информации как в отношении параметров компьютерной системы, информационно-телекоммуникационной сети, так и в отношении лиц, которые причастны к кибермошенничеству (например, идентификационные характеристики разработанных программистом компьютерных программ).

Специфика технологии доказывания по делам о кибермошенничествах предполагает также процедуру легализации результатов применения такого рода программного обеспечения правоохранительными органами. Следственными действиями, в рамках которых такая легализация возможна, традиционно считаются следственный осмотр и выемка.

С одной стороны, киберпреступления в связи с тем, что для их совершения используются возможности, предоставляемые Интернетом, имеют особую (нетрадиционную для обычных, не киберпреступлений) следовую картину, но, с другой стороны, задействование мошенниками для реализации своих криминальных намерений ресурсов Сети позволяет правоохранительным органам до определенной степени автоматизировать сбор оперативно значимой информации. Речь идет о воз-

можностях, предоставляемых в этой связи компьютерными программами, которые относятся к классу так называемых интеллектуальных агентов (так называемые «пауки»). Эти программы способны вести целевой мониторинг Интернета, результаты которого, например, могут способствовать выявлению лиц, причастных к совершенному, совершаемому либо подготавливаемому кибермошенничеству.

К такого рода программному обеспечению можно отнести систему ФБР Carnivore. Она устанавливалась непосредственно на серверах провайдера и была способна пропускать и сканировать на предмет оперативно значимой информации миллионы электронных сообщений одновременно [21]. В июне 2013 г. после громкого скандала общественности стало известно об использовании правоохранительными органами США программы PRISM, которая позволяет отслеживать перемещения людей и их контакты. Как было заявлено, в функционировании PRISM принимают участие компании *Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube и Apple* [17]. Использование подобного рода программного обеспечения всегда будет вызывать у общественности вопросы о правомерности ограничения правоохранительными органами конституционных прав и свобод граждан, а также о надлежащем соблюдении процедур судебного санкционирования применения подобного рода программ. Отсюда возникает и проблема правомерности формирования доказательств на основе информации, полученной таким образом.

Более того, как выяснилось, использование подобного рода программ несет в себе еще и другие неприемлемые риски. Троянская программа, применяемая немецкой полицией для сбора значимой информации, была протестирована специалистами, которые пришли к выводу о том, что сама программа недостаточно защищена от хакерских атак и, соответственно, злоупотреблений злоумышленниками с полученными при ее помощи сведениями. Несовершенной оказалась программа и при решении задач по сбору данных в Сети. Опытному хакеру вполне по силам подбросить ей дезинформацию. Такие негативные выводы специалистов привели к отказу от использования данной программы в деятельности полиции Германии [24, с. 22–23].

Еще одной особенностью доказывания по делам о кибермошенничестве является необходимость осуществлять тесное взаимодействие не только с государственными структурами, но и с негосударственными организациями, как специализирующимися на оказании услуг в сфере информационной безопасности, так и являющимися пользователями продукции и услуг вышеназванных негосударственных организаций.

Показательным в этом отношении является пример взаимодействия Интерпола и «Лаборатории Касперского» по выявлению и изобличению международных киберпреступников в настоящее время и на обозримую перспективу после 2014 г., когда в полном объеме начнет функционировать международный центр для инноваций Интерпола (IGCI) в Сингапуре, которому «Лаборатория Касперского» будет предоставлять техническую поддержку и оперативные данные по киберпреступникам.

Таким образом, Интерпол реализует стратегию защиты от преступных посягательств киберпространства, в основе которой лежит совместная скоординированная деятельность на региональном и международном уровнях правоохранительных органов и частных структур, в том числе и компаний, которые являются общепризнанными лидерами в сфере информационной безопасности (подобные соглашения Интерпол имеет не только с «Лабораторией Касперского», но и с другими компаниями, занимающимися обеспечением информационной безопасности – японским институтом кибероборонны, компанией LAC и иссле-

довательским институтом по вопросам кибербезопасности Fourteenforty) [12].

Эффективная технология доказывания по делам о кибермошенничестве невозможна без проведения научно-исследовательской работы в сфере обеспечения информационной безопасности. Особое значение научно-исследовательская работа имела и будет иметь для совершенствования методики проведения экспертных исследований в сфере борьбы с киберпреступностью. Изобличение и привлечение к уголовной ответственности кибермошенников становится невозможным без своевременно и профессионально проведенных судебных экспертиз.

Подытоживая вышеизложенное, можно отметить, что совершенствование технологии доказывания при расследовании кибермошенничеств в целом, а также отдельных ее (технологии) компонентов способно существенно повысить эффективность деятельности правоохранительных органов в противодействии угрозам со стороны транснациональных кибермошенников в информационно-телекоммуникационных сетях.

Эффективность технологии доказывания транснационального кибермошенничества прежде всего зависит: 1) от наличия и качества унифицированных международных нормативных актов, регламентирующих процедуру доказывания по транснациональным киберпреступлениям в целом и по делам о кибермошенничестве в частности; 2) от степени профессионализма лиц, осуществляющих расследование по уголовным делам данной категории; 3) от качества взаимодействия международных правоохранительных органов, государственных и негосударственных структур, специализирующихся на противодействии киберпреступности; 4) от результативности способов обнаружения следов криминальной деятельности в Интернете и методики проведения судебных экспертиз с обнаруженными следами киберпреступлений.

Пристатейный библиографический список

1. Абдуллаев Т. Троян атакует // Российская газета. 2012. 18 сентября. URL: http://www.rg.ru/2012/09/18/hakery.html
2. Атаманов Р.С. Криминалистическая характеристика мошенничества в онлайн-играх // Российский следователь. 2011. № 21. С. 2–4.
3. В Гонконге открылся форум стран АТР «Доверие и безопасность в информационном обществе». 2012. 26 сентября // Официальный сайт МВД. URL: http://mvd.ru/news/item/146944
4. Взаимодействие в борьбе с мошенничествами в сфере высоких технологий. Официальный сайт МВД России. 2011. 30 ноября // URL: http://mvd.ru/news/item/160298
5. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: Юрлитинформ, 2001.
6. Воронина Ю. Данные в опасности // Российская газета. 2013. 12 февраля // URL: http://www.rg.ru/2013/02/12/kiberprestuplenia.html
7. Выступление начальника Бюро специальных технических мероприятий МВД России генерал-полковника милиции Бориса Мирошникова на конференции в рамках Проекта международного сотрудничества по уголовным делам на тему «Перспективы международного сотрудничества в Конвенции о киберпреступности 2001 г.» // Официальный сайт МВД. URL: http://mvd.ru/news/item/185083/
8. Гафнер В.В. Информационная безопасность: учеб. пособие. Ростов-на-Дону: Феникс, 2010.
9. Грень И.В. Компьютерная преступность. Минск: Новое знание, 2007.
10. Илюшин Д.А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет: автореф. дис. ... канд. юрид. наук. Волгоград, 2008.
11. Информационное право: учебник для бакалавров / отв. ред. И.М. Рассолов. Москва: Проспект, 2013.
12. Касперский проконсультирует Интерпол // Ведомости. 2013. № 49 (3311). 22 марта. URL: www.vedomosti.ru/newsline/news/10325821/kasperskij_pomozhet_interpolu

13. Крупную операцию против киберпреступности провели спецслужбы США // Российская газета. 2012. 27 июня. URL: http://www.rg.ru/2012/06/27/hakeri-anons.html
14. Мишина И.М. Расследование мошенничества, совершенного с использованием банковских карт: криминалистические и уголовно-процессуальные аспекты: автореф. дис. ... канд. юрид. наук. М., 2009.
15. Минкомсвязь: Россия стала мировой интернет-державой // Взгляд. 2013. 25 апреля. URL: http://www.vz.ru/news/2013/4/25/630283.html
16. Панькина И.Ю. Некоторые аспекты эволюции теории доказывания в уголовном судопроизводстве России // Школы и направления уголовно-процессуальной науки. Доклады и сообщения на учредительной конференции Международной ассоциации содействия правосудию (г. Санкт-Петербург, 5–6 октября 2005 г.) / под ред. А.В. Смирнова. СПб., 2005. 192 с. URL: http://www.iuaj.net/lib/konf-MASP/pankina.htm
17. Путин прокомментировал скандал со спецслужбами в США // Взгляд. 2013. 11 июня. URL: http://www.vz.ru/news/2013/6/11/636781.html
18. Стрельцов А. Cyber criminalis vulgaris // Компьютербилд. 2011. № 20. С. 30–35.
19. Сумма ущерба от кибермошенников в США $240 млн. 2008. 4 апреля. URL: http://www.cnews.ru/news/line/index.shtml?2008/04/04/
20. Фалалеев М. Считайте ваши деньги. Четверть мирового ущерба наносят российские хакеры // Российская газета. 2012. 4 апреля. URL: http://www.rg.ru/2012/04/04/kiberprestupleniasite.html
21. ФБР объявило об использовании системы слежения за электронной почтой Carnivore. URL: http://www.cnews.ru/news/line/index.shtml?2000/07/12/103879
22. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире. СПб.: Питер, 2003.
23. XI Конгресс ООН по предупреждению преступности и уголовному правосудию (Бангкок, 18–25 апреля 2005 г.): сб. документов / сост. А.Н.Сухаренко. М.: Юрлитинформ, 2008.
24. Chaos Computer Club. От хакерской банды до влиятельной организации // Компьютербилд. 2013. №11 (90). С. 20–23.