К вопросу об уголовно-правовой классификации киберпреступлений

М.В. Арзамасцев,
кандидат юридических наук, доцент кафедры конституционного и административного права юридического факультета Национального исследовательского университета «Высшая школа экономики», г. Санкт-Петербург, Российская Федерация, e-mail: maxim077@mail.ru

УДК 340.115.3: (343.346.8+343.45)

Аннотация. Современная уголовная политика характеризуется расширением круга киберпреступлений. Необходимость единых подходов к их уголовно-правовой оценке требует разработки научно обоснованной классификации таких деяний. В статье показаны недостатки ранее предлагавшихся классификаций, сделан вывод о необходимости построения классификации на основе критерия, относящегося к объективной стороне компьютерных преступлений. В авторской классификации по направленности информационного воздействия выделены подгруппы киберпреступлений: информационно-компьютерные, информационно-технические и информационно-психические.

Ключевые слова: компьютерные преступления, уголовно-правовая классификация, информационная причинность, объективная сторона преступления, признаки преступлений.

В настоящее время необходимость дальнейшего совершенствования мер борьбы с компьютерной преступностью признана как на национальном, так и на международном уровне. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ от 05.12.2016 г. № 646) отмечает возрастание масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличение числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в т.ч. в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. В свою очередь, Организация Объединенных Наций предлагает государствам опробовать конкретные меры, направленные на создание защищенной и устойчивой киберсреды, предупреждать и пресекать преступную деятельность, осуществляемую с помощью Интернета [1, п.п. «с» п. 9].

Активно ведутся споры относительно понятия криминализируемых деяний, которые предлагается обозначать не только как компьютерные [2; 3; 4], информационные [5] или киберпреступления [6; 7], но и как преступления: «в сфере высоких технологий» [8; 9], «в сфере обращения цифровой информации» [10], «с использованием электронной информации» [11], «с использованием компьютерных [12, с. 11-12] или информационных, информационно-коммуникационных [13], информационно-телекоммуникационных [14] технологий», и др. Наверное, эту дискуссию нельзя считать просто спором о терминах, но наличие столь многих вариантов наименования рассматриваемых преступлений связано, главным образом, с новизной самих общественных отношений, возникших и развивающихся в условиях цифровой революции. Последующая эволюция уголовного права определит жизнеспособность тех или иных терминов. Пока что – в целях простоты и удобства – представляется предпочтительным синонимичное использование терминов «компьютерные преступления» или «киберпреступления», помня об их условности. Например, по мнению И.Г. Чекунова, киберпреступность следует рассматривать шире компьютерной преступности, т.к. использование компьютера или компьютерных сетей для составляющих ее преступлений не всегда является необходимостью; кроме того, для совершения киберпреступлений используются не только компьютеры, но и мобильные (сотовые) коммуникационные технические устройства и системы связи [15, с. 53]. Напротив, по оценке М. Герке, «киберпреступность» имеет более узкое значение, чем «преступления, связанные с применением

компьютеров», поскольку подразумевает использование компьютерной сети. Под преступлениями, связанными с применением компьютеров, понимаются даже те правонарушения, которые затрагивают отдельно стоящие устройства и системы [16, с. 12].

В УК РФ помимо главы 28, устанавливающей ответственность за преступления в сфере компьютерной информации, еще ряд норм предусматривают использование информационно-телекоммуникационных сетей (которые в некоторых случаях конкретизированы как сеть «Интернет») в качестве криминообразующего (ч. 3 ст. 137, ст. ст. 159^6, 171^2, 185^3, 282) или квалифицирующего (ч. 2 ст. 205^2, п. «б» ч. 2 ст. 228^1, п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 242^1, п. «г» ч. 2 ст. 242^2, ч. 2 ст. 280, ч. 2 ст. 280^1) признаков. К предмету преступления, предусмотренного ст. 187 УК РФ, законодатель отнес электронные средства, электронные носители информации, технические устройства, компьютерные программы, предназначенные для неправомерного осуществления приема, выдачи, перевода денежных средств. Тем самым законодательная оценка компьютерных преступлений постепенно расширяется, с учетом чего заслуживает внимания так называемая «широкая трактовка киберпреступлений», которую В.Н. Черкасов, хотя и считает ошибочной, связывает с отнесением к преступлениям в киберпространстве любых преступных посягательств с использованием компьютерной техники и информационных технологий [17]. Тенденция развития законодательства именно в рамках данного подхода признается и другими специалистами [18, с. 247], а ее экстраполяция позволяет считать правильным вывод А.И. Халлиулина, что перечень таких преступлений будет постоянно пополняться [7, с. 38], причем не только в связи с отмечаемым им научно-техническим прогрессом, но и в связи с изменением социальной значимости информационных и телекоммуникационных отношений, а также криминогенными процессами в этой сфере.

Специалисты признают, что степень общественной опасности преступления повышает как способ его совершения, связанный с использованием технических средств и позволяющий конспирировать преступную деятельность [19, с. 63], так и сами средства [15, с. 53]. Хотя, по мнению В.Н. Черкасова, использование современных компьютерных технологий явно повышает опасность только конкретных видов преступления, что требует введения соответствующих квалифицирующих признаков [17], следует – учитывая идею А. П. Козлова о необходимости унификации квалифицирующих и отягчающих обстоятельств [20, с. 124.] – признать и допустимость внесения аналогичного признака в ст. 63 УК РФ, который в литературе, например, формулируется как «использование технических средств обработки электронной информации» [19, с. 67].

Кроме того, обсуждается вопрос о возможности уголовной ответственности за подделку электронного документа по ст. 327 УК РФ [21, с. 57-62], за незаконную эмиссию или подделку электронных денег [6, с. 21], за сбыт цифровой и документированной информации, добытой заведомо преступным путем [10, с. 18-20]. Внимание законодателя обращается на составы преступлений, при совершении которых использование высокотехнологичных средств и способов передачи ложной информации становится все более типичным (например, ст. ст. 128^1, 207 УК РФ) [19, с. 64].

Поскольку круг компьютерных преступлений в уголовном законе стал достаточно широким, они приобрели разнородный характер, их дальнейший анализ требует выделения подгрупп, к которым применимы – с учетом общности их признаков – как единые принципы законодательной оценки, так и единые правила квалификации. Эта исследовательская задача может быть решена при помощи метода классификации преступных деяний, которая не только является необходимым условием правильного толкования норм об этих преступлениях, но и полезна в научно-методическом отношении [22, с. 120].

Традиционно уголовно-правовая классификация выражается «в систематизации преступлений по определенным признакам, предусмотренным в УК РФ» [23, с. 61]. Такие признаки (критерии классификации преступлений) последовательно различаются: на уровне единичного – дифференциации составов преступлений – ими служат отдельные признаки составов преступлений (главным образом объективной стороны), на уровне особенного (Особенной части УК) – родовой объект, на уровне всеобщего (Общей части УК) – общественная опасность в целом, ее характер и степень [24, с. 520]. С учетом множества закрепленных законодателем объективных и субъективных признаков преступлений (по которым они могут быть разделены на группы) расширяются как возможности классификации преступлений, так и варианты классификаций [20, с. 120]. Это, в свою очередь, требует оценки пригодности тех или иных классификаций для уголовно-правового анализа.

В литературе сформулирован ряд требований, которым должна отвечать уголовно-правовая классификация преступлений. Так, отмечается, что при выборе классификационного критерия необходимо руководствоваться следующими положениями: во-первых, роль основания для деления преступлений на группы или классы может выполнять лишь основной существенный признак; во-вторых, этот признак должен быть объективным, вытекающим из внутренней природы преступления как социального явления; в-третьих, такой признак должен отражать не только общее, но и особенное, т.е. не только сходство, но и различие в отдельных преступлениях; в-четвертых, содержание признака должно быть четким и ясным [20, с. 135]. Считается также, что любая классификация может быть правильной, если за ее основу берется стабильный признак, выражающий качественное свойство и своеобразие классифицируемых явлений [25, с. 66]. Кроме того, нельзя искусственно разбивать единую в функциональном отношении группу, основываясь на малозначительных деталях. В противном случае будет утрачено целостное видение предмета [22, с. 116].

Весь массив преступлений обычно классифицируется по следующим критериям: по степени тяжести; по видам вины; по характеру отражения преступления в законе; по характеру вреда объекту преступления [20, с. 118]. Чаще всего специалисты считают наиболее предпочтительной для науки уголовного права классификацию преступлений по объекту посягательства. Такая классификация, по оценке В. Н. Кудрявцева, полезна, по крайней мере, в двух отношениях: во-первых, она распределяет все преступления по направленности этого посягательства – против личности, имущества, государственных, общественных интересов и т.д. и тем самым группирует их по определенным признакам, а во-вторых, она дает представление о смежных составах преступлений [23, с. 61].

Учитывая, что в нашей стране компьютерные преступления законодатель выделил в разных главах Особенной части УК РФ, их можно классифицировать по соответствующим видовым объектам, однако такая классификация вряд ли будет отражать сущностные признаки этих деяний, поскольку их специфика определяется не объектом посягательства. Например, одна из таких классификаций включает в систему компьютерных преступлений преступления против личности; преступления в сфере экономики; преступления против общественной безопасности, общественного порядка и общественной нравственности; преступления против безопасности государства [26, с. 19]. Очевидно, что эта классификация не изменится и при ее применении к традиционно выделяемым преступлениям.

При этом одним из обязательных признаков любого киберпреступления специалисты считают одновременное наличие двух объектов посягательства: как общественных отношений в сфере безопасности обращения компьютерной информации, так и связанных с ней общественных отношений, имеющих взаимосвязь с реальным миром (отношений собственности, жизни, здоровья и т.д.) [7, с. 38]. В зависимости от того, являются ли отношения, возникающие в сфере компьютерной информации или обеспечивающие безопасность компьютерной информации, основным или дополнительным объектом, выделяют собственно преступления в сфере компьютерной информации (гл. 28 УК РФ) и большой круг преступных деяний, предусмотренных статьями других глав УК РФ [15, с. 54]. Вместе с тем, размещение законодателем запрещаемых форм поведения по главам носит условный характер, с учетом чего меняется и оценка объекта как основного или дополнительного. Соответственно, такая классификация носит формальный, а не сущностный характер.

Предложенная А.Г. Волеводзом классификация по своей сути также строится на признаке объекта преступлений. Так, он выделяет преступления в сфере компьютерной информации, посягающие на информационные компьютерные отношения; преступления в информационном компьютерном пространстве, посягающие на отношения, возникающие по поводу реализации прав на информационные ресурсы, информационную инфраструктуру и составляющие ее части; иные преступления, для которых характерно использование компьютерной информации или составляющих ее элементов информационного пространства, посягающие на иные охраняемые уголовным законом правоотношения [27, с. 49-50]. Вместе с тем, проводя такую классификацию, он отмечает, что вторая группа не требует самостоятельной регламентации в уголовном законодательстве [27, с. 51]. С учетом этого, теряется уголовно-правовое значение такой классификации, поскольку она не отражает качественный признак криминализируемых деяний.

Конвенция о преступности в сфере компьютерной информации (ETS № 185) (Конвенция о киберпреступности)

от 23 ноября 2001 г. предлагает государствам-участникам включить в уголовное право четыре группы преступлений: преступления против конфиденциальности, целостности и доступности компьютерных данных и систем; правонарушения, связанные с использованием компьютерных средств; правонарушения, связанные с содержанием данных; правонарушения, связанные с нарушением авторского права и смежных прав (разделы 1-4 части 1 главы II). Конечно, в таком разделении не соблюдается ни последовательность деления, ни наличие единого критерия для этого. Аналогичные недостатки можно выделить и в подготовленном группой экспертов ООН обзоре, который делит киберпреступления на три группы: преступления против конфиденциальности, целостности и доступности компьютерных данных или систем; преступления, связанные с использованием компьютеров (*computer-related acts*) с целью получения корыстной или личной выгоды либо причинения вреда; преступления, связанные с содержанием информации (*computer content-related acts*) [28, p. 16].

Главной особенностью киберпреступления (компьютерного преступления, преступления в сфере высоких технологий) специалисты признают использование сетей компьютера для совершения противоправного поступка или преступления в виртуальном пространстве [18, с. 244], что предполагает наличие прямого умысла. С умышленным характером кибепреступлений согласны и другие авторы [15, с. 56]. Хотя представляется возможным выделение состава нарушения правил кибербезопасности, повлекшего по неосторожности тяжкие последствия (который был бы смежным иным уголовно наказуемым случаем нарушения специальных правил безопасности в главе 24 УК РФ), уголовно-правовая классификация анализируемых преступлений по признакам субъективной стороны также малоперспективна.

Если раньше специфика преступлений в сфере компьютерной информации была обусловлена использованием при их совершении высоких технологий и новейших достижений науки и техники, необходимостью обладания определенным уровнем специальных познаний, то в настоящее время в глобальной сети Интернет в практически свободном доступе находятся как программы, предназначенные для совершения несанкционированных действий с компьютерной информацией, так и инструкции по их применению [29]. Соответственно, значимая для уголовного права классификация этих преступлений по признакам субъекта построена быть не может.

В литературе распространены классификации, построенные на изменении места информации (информационных технологий) в механизме совершения преступления. Например, в первой категории преступлений информационные технологии признаются в качестве объекта нападения, т.е. преступлением является хищение информации или нанесение какого-либо урона информационной системе. Во второй категории информационные технологии используются в качестве орудий совершения традиционных преступлений и электронных атак. Третью категорию составляют преступления, в которых информационные технологии и системы содержат запоминающие устройства, на которые совершается несанкционированный доступ [30]. Похожую классификацию приводит И.О. Морар, который считает, что она может базироваться на своеобразии способов совершения деяний: а) способы, применимые для получения доступа к информации, находящейся на машинных носителях (аппаратные устройства компьютерного типа, телефоны, пейджеры, аналоговые записывающие устройства и т.д.); б) способы, где компьютерная техника и средства коммуникации используются в качестве орудий и средств совершения преступления и/или их сокрытия; в) способы, где применяются высокотехнологичные устройства с целью незаконного доступа к компьютерной информации, ее модификации или блокирование [31, с. 39]. По оценке А.И. Халиуллина, наиболее простым (но не оправдывающим себя) способом является классификация киберпреступлений по принципу определения роли компьютера (компьютерной информации) как средства либо предмета преступления [7, с. 37]. Еще больше запутывают ситуацию утверждения, что информацию следует рассматривать как предмет уголовно-правовой охраны, а не предмет состава преступления [15, с. 53]. Все подобные классификации строятся не на одном признаке состава преступления, а на отнесении информации (информационных технологий) к разным элементам состава преступлений, с учетом чего они носят непоследовательный характер.

Неслучайно ряд исследователей приходят к выводу, что преступления в сфере компьютерной информации являются разнородными, вследствие чего нельзя создать классификацию способов совершения преступлений [32, с. 2]. Наиболее пессимистичная оценка сводится к тому, что наличие настолько разнородных преступлений,

совершаемых в информационно-телекоммуникационных сетях, не позволяет говорить о существовании киберпреступлений в уголовно-правовом смысле как отдельной группы преступлений [7, с. 38]. Действительно, в подготовленном для обсуждения на Тринадцатом конгрессе ООН по предупреждению преступности и уголовному правосудию справочном документе отмечается, что в целом граница между киберпреступностью и обычной преступностью становится все более размытой [33, п. 16], однако вряд ли это исключает возможность уголовно-правовой классификации киберпреступлений.

Перспективным для построения естественной классификации широко понимаемых компьютерных преступлений по единому критерию представляется обращение к признакам объективной стороны и развитие идей А.А. Тер-Акопова, который считал, что деяние может иметь различную причиняющую природу: физическую, информационную и нормативно-программную. По его оценке, при информационном воздействии деяние характеризуется передачей информации, которая имеет уголовно-правовое значение, причиняющую силу. Такое воздействие А.А. Тер-Акопов делил на четыре вида: информационно-психологическое (обманы, угрозы, подделки документов, заведомо ложные сообщения и т.п.); манипулирование информацией (выдача, передача, разглашение информации; непредоставление или сокрытие информации; искажение информации); несанкционированный доступ к защищаемой информации; информационно-компьютерные способы причинения имущественного вреда [34, с. 248-249]. Хотя сама идея информационного воздействия заслуживает поддержки, выделенные при этом виды не могут считаться последовательной классификацией, поскольку, в частности, искажение информации тесно сближается с обманом и заведомо ложными сообщениями. Кроме того, неясен критерий выделения этих видов.

Признавая информационное воздействие отличительной чертой компьютерных преступлений, можно построить уголовно-правовую классификацию по характеру (направленности) данного способа совершения преступления. Использование данного критерия позволяет выделить следующие виды анализируемых преступлений: информационно-компьютерные (для которых характерно изменение технически, компьютерной обрабатываемой информации без воздействия на психику человека или состояние технических устройств); информационно-психические (когда при помощи коммуникационных технологий информация адресуется конкретному лицу или неопределенному кругу лиц с интеллектуальным или эмоциональным воздействием); информационно-технические (когда информация передается, блокируется, изменяется с целью управляющего или разрушающего воздействия на технические устройства).

Теоретически можно было бы говорить о возможности информационного воздействия не только на психику, но и на организм человека. В частности, И.Г. Чекунов утверждает, что судебной практике известны случаи, когда путем распространения информации совершались убийства или причинялся вред здоровью, способами чего служили массовый гипноз людей или зомбирование конкретного человека. Распространение информации может явиться одним из способов доведения до самоубийства. Соответственно, путем использования информационно-коммуникационных технологий возможно не только информационное, но и физическое воздействие на человека с целью причинения вреда его здоровью или убийства [15, с. 55]. Встречаются упоминания о психонаркогенах, которые оказывают эффект, сходный с наркотическим в результате применения комбинации определенных электромагнитных излучений цвета и звука [35, с. 221]. Как отмечает Л.И. Романова, в Интернете был отмечен всплеск поисковых запросов, связанных с «аудионаркотиками» [36, с. 144]. В изученной при подготовке настоящей статьи практике судов примеров доказанного воздействия такого рода найти не удалось. Конечно, возможно убийство путем информационного вмешательства в работу, например, компьютерных устройств, входящих в состав реанимационного оборудования. В данном случае способ самого киберпреступления тогда будет носить информационно-технический характер, способ же причинения смерти будет основываться на физической, а не информационной причинности. С развитием науки, если будет показана возможность зомбирования и тому подобного воздействия (меняющего не психические, а физиологические процессы в организме), оно может быть отнесено к четвертому его виду – информационно-физическому (при этом может быть более корректным будет даже термин «информационно-физиологическое»), которое должно квалифицироваться как физическое насилие.

Предложенная в настоящей статье классификация построена по одному критерию, отражающему

сущность этих преступлений и характеризующему их объективную сторону, может позволить сформировать единые подходы к уголовно-правовой оценке компьютерных преступлений, единые правила квалификации предложенных групп преступлений и, в конечном счете, единые принципы применяемой к ним уголовной политики.

Библиографический список

1. Дохинская декларация о включении вопросов предупреждения преступности и уголовного правосудия в более широкую повестку для Организации Объединенных Наций в целях решения социальных и экономических проблем и содействия обеспечению верховенства права на национальном и международном уровнях, а также участию общественности // Библиотека криминалиста. – 2015. – № 6. – С. 366–379.

2. Ляпунов, Ю., Максимов, В. Ответственность за компьютерные преступления [Текст] / Ю. Ляпунов, В. Максимов // Законность. – 1997. – № 1. – С. 8–15.

3. Степанов-Егиянц, В. Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями [Текст] / В. Г. Степанов-Егиянц // Российский следователь. – 2012. – № 24. – С. 43–46.

4. Комаров, А. А. О целесообразности использования «кибертерминологии» в исследовании проблем преступности [Текст] / А. А. Комаров // Информационное право. – 2016. – № 1. – С. 4–7.

5. Крылов, В. Информационные преступления – новый криминалистический объект [Текст] / В. Крылов // Российская юстиция. – 1997. – № 4. – С. 22–23.

6. Чекунов, И. Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений [Текст] / И. Г. Чекунов // Право и кибербезопасность. – 2012. – № 1. – С. 9–22.

7. Халиуллин, А. И. Подходы к определению киберпреступления [Текст] / А. И. Халиуллин // Российский следователь. – 2015. – № 1. – С. 34–39.

8. Мороз, Н. О. Актуальные вопросы международного сотрудничества в борьбе с преступностью в сфере высоких технологий в рамках СНГ [Текст] / Н. О. Мороз // Международное уголовное право и международная юстиция. – 2016. – № 3. – С. 12–14.

9. Третьяк, М. И. Проблема законодательной регламентации преступлений против собственности в сфере высоких технологий [Текст] / М. И. Третьяк // Законность. – 2016. – № 7. – С. 41–46.

10. Бегишев, И. Р. Преступления в сфере обращения цифровой информации [Текст] / И. Р. Бегишев // Информационное право. – 2010. – № 2. – С. 18–21.

11. Ефремова, М. А. Мошенничество с использованием электронной информации [Текст] / М. А. Ефремова // Информационное право. – 2013. – № 4. – С. 19–21.

12. Сафонов, О. М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. ... канд. юрид. наук: 12.00.08 / Сафонов Олег Михайлович. – М., 2015. – 222 с.

13. Хисамова, З. И. Зарубежный опыт уголовно-правовой охраны отношений в сфере использования информационно-коммуникационных технологий [Текст] / З. И. Хисамова // Юридический мир. – 2016. – № 2. – С. 58–62.

14. Ефремова, М. А. Уголовно-правовое обеспечение кибербезопасности: некоторые проблемы и пути их решения [Текст] / М. А. Ефремова // Право и кибербезопасность. – 2014. – № 2. – С. 33–38.

15. Чекунов, И. Г. Понятие и отличительные особенности киберпреступности [Текст] / И. Г. Чекунов // Российский следователь. – 2014. – № 18. – С. 53–56.

16. Герке, М. Понимание киберпреступности: явление, задачи и законодательный ответ [Электронный ресурс] / М. Герке // Международный союз электросвязи: [сайт]. [2014]. URL: http://www.itu.int/en/ITU- / Cybersecurity/Documents/Cybercrime2014_R.pdf (дата обращения 25.01.2017)

17. Черкасов, В. Н. Информационные технологии и организованная преступность [Электронный ресурс] / В. Н. Черкасов // Саратовский Центр по исследованию проблем организованной преступности и коррупции: [сайт]. [2014]. URL: http://sartraccc.ru/Pub/cherkasov%2824-03%29.htm (дата обращения 25.01.2017).

18. Рассолов, И. М. Право и Интернет. Теоретические проблемы [Текст] / И. М. Рассолов. – 2-е изд., доп. – М.: Норма, 2009. – 384 с.

19. Смолин, С. Уголовно-правовая борьба с высокотехнологичными способами и средствами совершения преступлений [Текст] / С. Смолин // Уголовное право. – 2014. – № 4. – С. 62–68.

20. Энциклопедия уголовного права: понятие преступления. Т. 3 / И. Я. Гонтарь, И. А. Зинченко, А. П. Козлов, Н. Ф. Кузнецова и др.; отв. ред. В. Б. Малинин. – СПб.: Изд. профессора Малинина, 2005. – 522 с.

21. Лукьянова, А. А. Электронный официальный документ как предмет преступления, предусмотренного ст. 327 УК РФ [Текст] / А. А. Лукьянова // Уголовное право. – 2016. – № 3. – С. 57–62.

22. Клепицкий, И. А. Система хозяйственных преступлений: монография [Текст] / И. А. Клепицкий. – М.: Статут, 2005. – 572 с.

23. Кудрявцев, В. Н. Борьба мотивов в преступном поведении: монография / В. Н. Кудрявцев. – М.: Норма, 2007. – 128 с.

24. Кузнецова, Н. Ф. Избранные труды: монография [Текст] / Н. Ф. Кузнецова; предисл. В. Н. Кудрявцева. – СПб.: Изд-во «Юридический центр Пресс», 2003. – 834 с.

25. Егиазарян, Н. А. Преступления против порядка управления в уголовном праве Армении и России (сравнительно-правовое исследование): дис. … канд. юрид. наук: 12.00.08 / Егиазарян Наира Ашотовна. – М., 2013. – 225 с.

26. Широков, В. А., Беспалова, Е. В. Компьютерные преступления: основные тенденции развития [Текст] / В. А. Широков, Е. В. Беспалова // Юрист. – 2006. – № 10. – С. 18–21.

27. Волеводз, А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества: монография [Текст] / А. Г. Волеводз. – М.: Юрлитинформ, 2001. – 496 с.

28. Comprehensive Study on Cybercrimes [Электронный ресурс] / United Nations Office on Drugs and Crime: [сайт]. [2013]. URL: http://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf (дата обращения 25.01.2017)

29. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) [Электронный ресурс]. Документ опубликован не был. Доступ из справ. -правовой системы «Консультант Плюс».

30. Демьянец, М. В. Предпринимательская деятельность в сети Интернет: монография [Текст] / М. В. Демьянец, В. М. Елин, А. К. Жарова. – М.: Юркомпани, 2014. – 440 с.

31. Морар, И. О. Могут ли в рамках науки криминологии рассматриваться способы совершения компьютерных преступлений и их последствия? [Текст] / И. О. Морар // Российский следователь. – 2012. – № 12. – С. 37–41.

32. Будаковский, Д. С. Способы совершения преступлений в сфере компьютерной информации [Текст] / С. С. Будаковский // Российский следователь. -– 2011. – № 4. – С. 2–4.

33. Укрепление мер реагирования систем предупреждения преступности и уголовного правосудия на появляющиеся формы преступности, такие как киберпреступность и незаконные оборот культурных ценностей, в том числе извлеченные уроки и международное сотрудничество. Справочный документ семинара-практикума. Электронный ресурс] / United Nations Office on Drugs and Crime: [сайт]. [2015]. URL: A/CONF.222/12 [Электронный ресурс] // http://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_r_V1500665.pdf (дата обращения 25.01.2017)

34. Тер-Акопов, А. А. Преступление и проблемы нефизической причинности в уголовном праве: монография [Текст] / А. А. Тер-Акопов. – М.: «Юркнига», 2003. – 480 с.

35. Основные направления противодействия транснациональному организованному криминальному наркобизнесу: монография / Л. Драпкин, Р. Вафин, Я. Злоченко и др.; под общ. ред. И. И. Ищенко. – М.: ЛексЭст, 2003. – 424 с.

36. Романова, Л. И. Наркопреступность: криминологическая и уголовно-правовая характеристика: учеб. -метод. пособие / Л. И. Романова. – 2-е изд. – Владивосток: Изд-во Дальневосточного ун-та, 2009. – 314 с.