УДК 343.23:004
ББК 67.408.135

Современные подходы к определению компьютерной преступности и особенности компьютерных преступлений

Т.А. Ханов А.Ж. Нуркеев

Карагандинский экономический университет Казпотребсоюза (Караганда, Казахстан)

Modern Approaches to the Computer Criminality Definition and Features of Computer Crimes

T.A. Khanov, A.J. Nurkeev

Karaganda Economic University of Kazpotrebsouz (Karaganda, Kazakhstan)

Рассмотрены имеющиеся подходы к определению компьютерных преступлений и на основе их анализа сформулировано понятие компьютерного преступления (киберпреступность), под которым следует признавать общественно-опасное деяние, совершенное вменяемыми физическими лицами, посягающее на охраняемые законом права и интересы пользователей информационно-телекоммуникационных сетей путем нарушения систем безопасности функционирования компьютерных устройств посредством создания, внедрения, использования либо распространения запрещенной или охраняемой законом информации. Раскрыта взаимосвязь данного вида правонарушений с другими противоправными деяниями и обозначена их высокая общественная опасность. Подчеркнута латентность рассматриваемых преступлений, что вызывает сложности с выявлением лиц, совершивших правонарушение, и привлечением их к уголовной ответственности. Рассмотрены особенности данных видов преступных деяний, связанные с тем, что правонарушитель находится на значительном удалении от места, в условиях анонимности и, как правило, не контактирует с жертвой.

Приведены конкретные примеры, подтверждающие полученные выводы. Внесены отдельные предложения, направленные на противодействие рассматриваемым преступлениям.

Ключевые слова: Интернет, информационные системы, компьютерные преступления, компьютерные вирусы, кибертерроризм.

The authors consider the available approaches to the definition of computer crimes and, based on the analysis of existing approaches, formulate the authors' concept of computer crime (cybercrime), under which it is necessary to recognize a socially dangerous act committed by sane individuals, encroaching on the rights and interests of information and telecommunication network users protected by law, information and telecommunications networks, by violation of security systems, the functioning of computer devices, through the creation, implementation, use or dissemination of prohibited or legally protected information. Deep interrelation of this type of offenses with other illegal acts is revealed and their high social danger is indicated.

The emphasis is made on the latency of the crimes which makes it difficult to identify the perpetrators and bring them to criminal responsibility. Consideration is given to the features of these types of criminal acts with the offender being at a considerable distance from the place, in conditions of anonymity and, as a rule, not contacting with the victim. Specific examples that confirm the conclusions are given. Separate proposals have been made to counteract the crimes in question.

Key words: internet, information systems, computer crimes, computer viruses, cyberterrorism.

DOI 10.14258/izvasu(2017)6-19

Отличительной чертой современного общества является развитие информационных технологий, сегодня общество уже нельзя представить без различных электронно-вычислительных машин (ЭВМ). В связи данным обстоятельством информативные технологические процессы не только предоставили стимул для прогресса сообщества, но и спровоцировали появление и формирование незнакомых прежде неблагоприятных действий.

Одним из негативных последствий, связанных с информатизацией, следует признать «компьютерные правонарушения». По мнению отдельных ученых, наступившие вредные последствия от их совершения не соизмеримы с ущербом от других преступлений [1, с. 28].

Целью настоящей статьи является анализ компьютерной преступности, определение понятия, содержания и общественной опасности.

Из истории компьютерных правонарушений известно, что впервые о них заговорили в период с 1969 по 1973 г., первоначально у правонарушителей были меркантильные интересы. Так, в одной из заметок Д. Фролов приводит следующие примеры: Альфонсе Конфессоре осуществил налоговое преступное деяние в необходимую ему сумму 620 тыс. долларов и в 1969 г. предстал перед североамериканским трибуналом. В 1973 г. казначей нью-йоркского Ситибанка, применив служебный компьютер, перебросил на собственный счет два миллиона долларов [2, с. 34]. Можно считать, что с данных правонарушений началась хроника компьютерных преступлений.

Информатизация нынешнего общества способствовала развитию особых типов правонарушений, для совершения которых приспосабливаются новые виды телекоммуникаций и услуг связи, позволяющие использовать интернет-ресурсы для получения доступа к конфиденциальным данным и тайного извлечения различных сведений. Помимо этого, расширилось вредоносное вмешательство через компьютерные сети в работу различных систем, при этом с каждым годом существенным способом изменяется вид атак: они крайне усложняются. Современные атаки стали наиболее развилистыми: нападающая область стремится приспособиться к инфраструктуре фирмы и совершить атаку предельно малозаметно. Нередко факт системного взлома выявляется слишком поздно либо не выявляется вообще.

Актуальность рассматриваемой темы определяется высокой значимостью борьбы с компьютерной преступностью и расширением использования информационных технологий для совершения экономических и иных имущественных преступлений.

Переворот в сфере электроники создал определенный потенциал правонарушителям, их организованным группировкам и сообществам, для допуска к новейшим технологическим орудиям, которые дали им возможность противозаконно приписывать миллиардные прибыли, приобретенные незаконным путем, обходить налогообложение и осуществлять групповые деяния, связанные с длительной подготовкой и совершением замаскированных преступлений.

В XXI в. по всему миру повышается угроза взломов информационных систем, которые могут привести к негативным последствиям как регионального, так и глобального масштаба. Такие атаки, осуществляемые посредством несанкционированного проникновения или внедрения компьютерного вируса, могут вывести из строя важнейшие стратегические объекты, транспортные узлы и сети, ядерные реакторы, системы водо- и энергоснабжения. К примеру, можно выделить случай, который произошел в США в штате Даллас. Неизвестный хакер получил удаленный доступ ко всем 156 городским сиренам безопасности Далласа и включал их на полную громкость в течение полутора часов ночью с пятницы на субботу. Как отмечает мэр города, хакер преследовал цель вывести из строя систему чрезвычайных оповещений [3].

В Казахстане уровень цифровой грамотности населения не так уж высок. Мы существенно отстаем от ведущих и большинства развивающихся стран. О совершенных компьютерных правонарушениях, как правило, наши граждане узнают из мировых новостей. Поэтому само сообщество пока не осознало всей серьезности и остроты анализируемой проблемы. В этой связи видится актуальным рассмотрение отдельных уголовно-правовых аспектов компьютерных преступлений.

В научных работах многих авторов, наряду с понятием «компьютерные преступления», широко используется дефиниция «киберпреступность», которое, по их мнению, более полно отражает суть преступных деяний, совершаемых с помощью компьютерных устройств, информационно-телекоммуникационных сетей и информационных технологий [4, с. 13; 5, с. 23].

Данное определение первоначально вошло в обиход и употреблялось в научном обороте зарубежных юристов и криминологов [6; 7].

Между тем многие российские исследователи отождествляют понятия «преступность в Интернете», «киберпреступность», «компьютерная преступность» [8, с. 251–253; 9, с. 11–13]. Данный подход представляется нам вполне обоснованным.

Согласно данным, подготовленным исследователями Threat Intelligence Software Technologies, которые были представлены в ежемесячном отчете компанией Check Point, специализирующейся на сетевой кибербезопасности, за январь 2017 г. количество атак на казахстанские компании снизилось. В то же время аналитики отмечают: Казахстан находится на 19-й позиции в списке самых подверженных кибератакам стран, отечественные компании по-прежнему

находятся в зоне риска. Анализ рейтинга позволяет сделать вывод, что хакеры продолжают использовать весь арсенал инструментов для таргетированных атак на казахстанский бизнес. При этом угроза заражения возникает на каждом этапе, включая рассылаемые ботами спам-письма, содержащие загрузочные файлы, внедряющие вредоносную программу на устройство жертвы [10].

Уголовный кодекс Республики Казахстан, вступивший в действие с 1 января 2015 г., ввел новую главу — «Уголовные правонарушения в сфере информатизации и связи», определив родовым объектом компьютерных преступлений состояние защищенности информации, обрабатываемой и передаваемой электронно-вычислительными машинами, системами и киберсетями.

Анализ статистических данных показывает, что количество преступлений данной категории в Казахстане падает; так, если в 2015 г. было зарегистрировано 176 правонарушений, то в 2016-м — 132, а за шесть месяцев 2017 г. всего 58 (против 107 за аналогичный период 2016-го) [11]. Однако это не говорит о снижении активности хакерских атак, а показывает лишь выявленные факты и подтверждает повышенную латентность данного вида преступлений. К тому же в гл. 6 УК РК «Преступления и проступки против собственности» содержится ряд статей (ст. 188, 190, 195), предусматривающих в качестве квалифицирующего признака преступного деяния: «путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций», которые отдельно не выделяются в общей статистике зарегистрированных правонарушений.

В настоящий период бешеного формирования электронных денег чаще всего мишенями преступников становятся банки, и количество кибератак с каждым годом увеличивается. Так, в 2016 г. в Казахстане было зарегистрировано 36 фактов хищения денег хакерами. Однако возникают определенные сложности с установлением лиц, их совершивших. Только за три месяца 2017 г. полицейские вынуждены были прервать досудебное расследование 75% уголовных дел по киберпреступлениям по данному основанию [12].

Между тем имеются и примеры успешной борьбы с хакерами: например приговор, который в январе 2017 г. вынес суд №2 Жетысуского суда города Алматы. Согласно материалам уголовного дела, два жителя южной столицы, проявив недюжинные способности в хакерстве, смогли похитить из финансовой системы «Нурбанка» и перевести на счет в другом банке 155 миллионов тенге [13].

Следует отметить, что хакерским атакам подвергаются не только банки и компании, нередко жертвами становятся граждане и отдельные организации. Взломав серверы и браузеры Интернета, хакер находит слабое звено в защитных системах, тем самым получая удаленный доступ в компьютерную систему, внедряет вирусы-роботы, способные в заданный момент искажать и даже уничтожать важную информацию. В отличие от других видов преступных деяний, правонарушитель, как правило, находится на значительном удалении от места, в условиях анонимности и не контактирует с жертвой. Нередко преступления в данной сфере совершаются организованными группами [14, с. 222] и носят транснациональный характер [15, с. 328].

В качестве примера можно выделить организованную преступную группу, которая работала под видом Генпрокуратуры в Алматы, в эту ОПГ входило 20 человек. Преступная схема заключалась в рассылке письма с вирусом от имени Генпрокуратуры и других государственных служб на электронные почты предприятий. Получателям высылался текст, побуждающий перейти по ссылке, по которой скачивалась вредоносная программа. В дальнейшем они получали удаленный доступ к компьютерам этих пользователей. Предварительно сумма ущерба составила 53 млн тенге [16].

К сожалению, рассматриваемый вид угрозы национальной безопасности пока не воспринимается казахстанским сообществом адекватно. Даже несмотря на то, что глава государства в своем ежегодном Послании народу Казахстана выступил с инициативой по созданию системы «Киберщит», до недавнего времени данный вопрос не получил широкой огласки. Между тем система «Киберщит Казахстана» представляет собой целый комплекс организационно-правовых и технических мер, набор аппаратно-программных комплексов и проектов, реализуемых государственными органами в сфере информационной и кибербезопасности [17].

Поэтому видится своевременным шагом подписание меморандума о партнерстве и взаимодействии в сфере кибербезопасности между «Казахтелекомом» и российской компанией «Solar Security». Партнерство двух компаний предусматривает создание центра мониторинга и реагирования на кибератаки. Внедрение в Казахстане системы кибербезопасности обусловлено задачами по обеспечению информационной безопасности на всех уровнях, а также защиты неприкосновенности частной жизни граждан при использовании информационно-коммуникационных технологий [18].

Однако на сегодня имеется существенный недостаток, связанный с точным и единообразным определением компьютерной преступности и общим осмыслением сути данного действа. Это значительно усложняет ликвидацию проблем правоприменительных органов в выработке тотальной стратегии противодействия данному виду противоправных деяний.

Особую актуальность имеют вопросы защищенности информации от несанкционированного доступа и возможности эффективной оценки риска информационной безопасности, на что неоднократно указывалось отечественными [19, с. 41; 20, с. 164] и зарубежными [21, с. 90–92; 22, с. 168] специалистами путем внесения соответствующих предложений.

Имеется немало научных работ, посвященных как общим вопросам информационной безопасности [23–25], так и проблемам противодействия компьютерной преступности [26; 27]. Между тем в научном сообществе пока нет общепризнанной точки зрения, в связи с чем продолжаются многочисленные дискуссии. В юридической науке имеется несколько подходов к данной проблематике, суть их сводится к пониманию компьютерной преступности в широком либо узком смысле.

В широком смысле к компьютерным правонарушениям относятся все деяния, совершенные вменяемыми физическими лицами, посягающие на законные права и интересы государства, общества, физических и юридических лиц в сфере безопасного оборота (создания, хранения, обработки, передачи, получения, защиты и т.д.) компьютерной информации и функционирования компьютерных устройств, информационно-телекоммуникационных сетей и иных средств создания, использования, распространения компьютерной информации [28, с. 88; 29, с. 11].

В узком смысле — совокупность преступлений, в которых предметом преступного деяния выступают компьютерные устройства, информационные телекоммуникационные сети, любая компьютерная информация, а также средства создания, хранения, обработки, передачи и защиты. При этом они используются в качестве средства и орудия совершения преступления [8, с. 16; 30, с. 21].

Вместе с тем уголовное право многих государств еще больше сужает суть данных правонарушений, признавая предметом преступного посягательства сведения, содержащие компьютерную информацию, а также ее использование в противоправных целях, при этом персональный компьютер (ПК) представляется лишь инструментом совершения противоправного деяния [31, с. 9].

Следует отметить, что 23 ноября 2001 г. в Будапеште была подписана «Конвенция Совета Европы о преступности в сфере компьютерной информации». Конвенция ратифицирована почти 50 государствами, в т.ч. она подписана США и Японией, но до сих пор не признана Российской Федерацией и Казахстаном. Данный международный акт призван стандартизировать правовое закрепление киберпреступлений в национальных законодательствах стран-участниц, сближение уголовно-процессуальных норм, упорядочение международного сотрудничества по предотвращению и расследованию компьютерных преступлений.

В данной Конвенции закреплено пять групп компьютерных правонарушений, которые, по сути, образуют компьютерную преступность: преступления против конфиденциальности, целостности и доступности компьютерных данных и систем; правонарушения, связанные с использованием компьютерных средств; правонарушения, связанные с содержанием компьютерных данных; правонарушения, связанные с нарушением авторского права и смежных прав; акты расизма и ксенофобии, совершенные посредством компьютерных сетей [32].

Большинство авторов, занимающихся проблемами компьютерных правонарушений, считают такую группировку обоснованной и утверждают, что уголовное законодательство придерживается аналогичной классификации [33, с. 92]. Хотя анализ главы 7 УК РК показывает, что не все деяния подпадают под данную классификацию.

Однако не все согласны с таким систематизированием компьютерных преступлений. Интересную точку зрения высказал Е.В. Томчак. Он считает, что правонарушения, сопряженные с применением ПК, необходимо расценивать равно как:

а) правонарушения, нацеленные в компьютерную область и коммуникационные технологические процессы;

б) правонарушения с применением числовых технологий в ходе совершения преступления;

в) правонарушения с применением ПК равно как прибора в ходе совершения других правонарушений [9, с. 12].

Между тем сфера компьютерных правонарушений может быть намного шире. Сегодня киберпреступность содержит в себе обширный диапазон противоправных действий — от неразрешенного вторжения в компьютерные сети, краж индивидуальной данных до финансового шпионажа и отмывания наличных средств. Как отмечают отдельные авторы, в последние годы интернет-ресурсы используются во всех циклах торговли людьми и запрещенными предметами, а также в последующей легализации преступных доходов [34, с. 12; 35, с. 150]. Следует также учесть, что нередко полученные преступным путем средства используются для финансирования международного экстремизма и терроризма [36].

Поскольку финансовая и информативная защищенность непосредственно переплетены и взаимосвязаны, объективным и актуальным остается вопрос межгосударственного взаимодействия по различным направлениям сотрудничества в борьбе с преступностью [37, с. 310; 38; 39, с. 79], а также унификация национального права и сближение правовых систем государств, направленных на уменьшение имеющихся в законодательстве различий и повышение эффективности правоохранительной деятельности [37, с. 312; 40].

В последние годы одним из наиболее опасных видов компьютерной преступности признается кибертерроризм [41, с. 26], раскрытие и расследование которого, в отличие от традиционного, осложнено рядом факторов. В частности возникают сложности с выявлением лиц, совершивших преступление, и привлечением их к уголовной ответственности, поскольку правонарушители используют псевдонимы или получают доступ к сайтам через гостевой вход, что затрудняет их идентификацию. Кроме того, действия террористов координируются через интернет-мессенджеры — системы мгновенного обмена сообщениями в реальном времени через Интернет. Их использование еще больше усложняет деятельность спецслужб по предотвращению терактов. Наиболее активно используется мессенджер Telegram, предоставляющий террористам возможность создавать секретные чаты с высоким уровнем шифрования передаваемой информации.

Как отмечает глава Роскомнадзора Александр Жаров, его создатель Павел Дуров нейтрален по отношению к террористам и преступникам, которые пользуются его мессенджером, и абсолютно игнорирует безопасность простых пользователей Telegram, отказываясь оказывать содействие спецслужбам и исполнять российское законодательство [42].

В этой связи актуальным является высказанное А.К. Нурпеисовой мнение о том, что законодатель обязан системно решить имеющееся противоречие: обеспечить охрану компьютерных данных и гарантировать присутствие в Уголовном кодексе норм, предусматривающих ответственность за пособничество в совершении компьютерных правонарушений [43, с. 9].

Таким образом, в связи с расширением возможностей использования киберпространства повышается и усиливается вопрос общественной опасности от компьютерной преступности в разных ее проявлениях. Наряду с организационно-техническими мерами должно совершенствоваться и национальное законодательство.

1. Следует выделить основные признаки, характеризующие данное правонарушение, сформулировать определение компьютерных преступлений.

Компьютерным преступлением (киберпреступностью) следует признавать общественно-опасные деяния, совершенные вменяемыми физическими лицами, посягающие на охраняемые законом права и интересы пользователей информационно-телекоммуникационными сетями путем нарушения систем безопасности функционирования компьютерных устройств, посредством создания, внедрения, использования либо распространения запрещенной или охраняемой законом информации.

2. Для повышения эффективности сотрудничества, а также усиления взаимодействия между правоохранительными структурами государств, заинтересованных в борьбе с международной киберпреступностью, необходимо провести систематизацию компьютерных правонарушений и привести ее в соответствие международным стандартам, а также наладить оперативный обмен информацией между специальными органами.

3. Следует расширить диспозицию норм уголовного закона путем введения квалифицирующего признака «совершенные путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций» по экономическим и другим видам правонарушений, включив данный признак в раздел правовой статистики для учета и контроля за киберпреступностью.

4. Усилить уголовную ответственность за кибертерроризм и экстремизм, в том числе за предоставление услуг по размещению информации на интернет-ресурсах.

Библиографический список:

1. Золотухин С.Н. Уголовно-правовая и криминологическая характеристика компьютерной преступности и ее предупреждение : учеб. пособие. — Челябинск, 2005.

2. Фролов Д. История информационной преступности // Закон. — 2002. — №12.

3. Hacker Sets off All 156 Emergency Sirens in Dallas [Электронный ресурс]. — URL: https://www.usatoday.com/story/news/2017/04/08/hacker-triggers-all-156-emergency-sirens-dallas/100212412/

4. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дисс. … канд. юрид. наук. — Владивосток, 2005.

5. Чекунов И.Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: дисс. … канд. юрид. наук. — М., 2013.

6. Wallace J., Mangan M. Sex, Laws and Cyberspace. — New York, 1996.

7. Kirwan G., Power A. Cybercrime: the Psychology of Online Offenders // Cybercrime: The Psychology of Online Offenders, 2011.

8. Рассолов И.М. Право и Интернет. Теоретические проблемы. — М., 2003.

9. Томчак Е.В. Из истории компьютерного терроризма // Новая и новейшая история. — 2007. — №1.

10. Казахстан находится в двадцатке самых уязвимых для кибератак стран [Электронный ресурс]. — URL: https://informburo.kz/novosti/kazahstan-nahoditsya-v-dvadcatke-samyh-uyazvimyh-dlya-kiberatak.

11. Комитет по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан [Электронный ресурс]. — URL: http://qamqor.gov.kz/portal/page/portal/POPageGroup/Services/Pravstat?_piref36_223083_36_223082_223082.

12. Казахстанские банки решили совместно бороться с хакерами [Электронный ресурс]. — URL: https://informburo.kz/novosti/kazahstanskie-banki-reshili-sovmestno-borotsya-s-kiberatakami.html.

13. На щите или со щитом: Что Казахстан противопоставит хакерам всего мира [Электронный ресурс]. — URL: https://informburo.kz/stati/na-shchite-ili-so-shchitom-chto-kazahstan-protivopostavit-hakeram-vsego-mira.html.

14. Чирков Д.К., Саркисян А.Ж. Преступность в сфере телекоммуникаций и компьютерной информации как угроза национальной безопасности страны // Актуальные проблемы экономики и права. — 2013. — № 3 (27).

15. Скляров С.В., Евдокимов К.Н. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации // Всероссийский криминологический журнал. — 2016. — Т. 10. — № 2.

16. В Алматы судят предполагаемых киберпреступников, работавших под видом Генпрокуратуры [Электронный ресурс]. — URL: https://informburo.kz/novosti/v-almaty-sudyat-predpolagaemyh-kiberprestupnikov-rabotavshih-pod-vidom-finansovyh-i-silovyh-gosstruktur.html.

17. В Казахстане создается комплекс защитной системы «Киберщит» [Электронный ресурс]. — URL: http://profit.kz/news/36966/V-Kazahstane-sozdaetsya-kompleks-zaschitnoj-sistemi-Kiberschit.

18. Центр мониторинга и реагирования на кибератаки создадут Казахстан и Россия [Электронный ресурс]. — URL: https://informburo.kz/novosti/centr-monitoringa-i-reagirovaniya-na-kiberataki-sozdadut-kazahstan-i-rossiya.html.

19. Буркитбаев А.М., Абеуов Р.Р., Баширов А.В. Проблемы защиты информации с учетом человеческого фактора // Проблемы современной науки и образования. — 2017. — № 19 (101).

20. Баширов А.В., Ханов Т.А., Сыздык Б.К., Оразметов Н.С. Оценка риска информационной безопасности подразделения // Современные научные исследования и разработки. — 2016. — № 6 (6).

21. Юдина Н.Ю., Лапшина М.Л. Защита информации в информационных системах // Моделирование систем и процессов. — 2016. — Т. 9. — № 4.

22. Джоган В.К., Курило А.П. Защищенность информационных ресурсов компьютерных систем как система показателей эффективности защиты информации // Безопасность информационных технологий. — 2011. — № 4.

23. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. — М., 1991.

24. Баширов А.В. Вопросы информационной безопасности в РК // Актуальные проблемы современности. — 2015. — № 4 (10).

25. Ханов Т.А., Жиенбеков Ж.Е. Система обеспечения информационной безопасности // Актуальные проблемы современности. — 2016. — № 2 (12).

26. Степанов И.В. Компьютерная преступность: уголовно-правовой анализ и предупреждение : дисс. … канд. юрид. наук. — СПб.,, 2006.

27. Лопатина Т.М. Компьютерная преступность и противодействие ей. — Смоленск, 2006.

28. Евдокимов К.Н. Структура и состояние компьютерной преступности в Российской Федерации // Юридическая наука и правоохранительная практика. — 2016. — № 1 (35).

29. Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью : дис. … канд. юрид. наук. — М., 2005.

30. Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение : дисс. … канд. юрид. наук. — М., 2003.

31. Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан) : автореф. дисс. ... канд. юрид. наук. — Махачкала, 2004.

32. Конвенция о компьютерных преступлениях (Будапешт, 23 ноября 2001 года; ETS n 185) [Электронный ресурс]. — URL: http://online.zakon.kz/Document/?doc_id=30170556#pos=3;-173.

33. Евдокимов К.Н. Структура и состояние компьютерной преступности в Российской Федерации // Юридическая наука и правоохранительная практика. — 2016. — № 1 (35).

34. Халиуллина Л.Г. Торговля людьми в пространстве сети Интернет // Юридическая наука и практика: альманах научных трудов Самарского юридического института ФСИН России. гл. ред. Р. А. Ромашов. — Самара, 2014.

35. Дикарев В.Г., Олимпиев А.Ю. К вопросу о противодействии бесконтактному способу сбыта наркотиков через сеть Интернет // Вестник Московского университета МВД России. — 2016. — № 8.

36. Баринов Д.А., Понукарина Е.С. Незаконный оборот наркотических средств как источник финансирования экстремизма и терроризма // Современные проблемы противодействия наркопреступности и распространению наркомании в азиатско-тихоокеанском регионе : сб. материалов Междунар. науч.-практ. конф.: в 2 ч. — Хабаровск, 2010. — Ч. 1.

37. Попов А.Б. Международное сотрудничество государств в борьбе с компьютерной преступностью // Вестник Тамбовского университета. Сер. : Гуманитарные науки. — 2010. — № 4 (84).

38. Буйтекулы К.Б. К вопросу о международном сотрудничестве Республики Казахстан в сфере борьбы с незаконным оборотом наркотиков // Вестник института: преступление, наказание, исправление. — 2008. — № 3.

39. Ханов Т.А., Борецкий А.В. Взаимодействие Российской Федерации и Республики Казахстан в противодействии преступности, связанной с торговлей людьми // Криминологический журнал Байкальского государственного университета экономики и права. — 2012. — № 4.

40. Ханов Т.А., Феткулов А.Х., Нурпеисова А.К. Гармонизация и унификация национального законодательства по формированию договорно-правовой базы таможенного союза и единого экономического пространства // Евразийский юридический журнал. — 2014. — № 11 (78).

41. Лопатина Т.М. О новых составах компьютерных преступлений // Современное право. — 2006. — № 4.

42. ФСБ: террористы использовали Telegram при организации взрыва в метро Петербурга [Электронный ресурс]. — URL: https://zona.media/news/2017/06/26/teleg.

43. Нурпеисова А.К. Практические аспекты доказывания правонарушения, совершенного с использованием сети Интернет // Закон. — 2006. — № 11.