ВЫЯВЛЕНИЕ И РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

БАСТРЫКИН Александр Иванович

доктор юридических наук, профессор, Заслуженный юрист РФ, Председатель Следственного комитета РФ (г. Москва)

https://doi.org/10.33874/2072-9936-2022-0-4-88-94

В статье рассматриваются вопросы выявления и расследования преступлений, совершенных с использованием информационно-коммуникационных технологий, в качестве важной составляющей комплекса мер по обеспечению прав граждан и восстановлению социальной справедливости. Преступления указанной категории несут в себе глобальные угрозы, именно поэтому разработка и реализация современных подходов по их выявлению, а также формирование оперативной методики расследования являются важными направлениями деятельности Следственного комитета РФ. Автор отмечает необходимость дальнейшего совершенствования как внутригосударственных, так и международных механизмов борьбы с киберпреступностью. Это в свою очередь требует совершенствования механизмов превентивного и прикладного характера, налаживания высокоэффективной системы взаимодействия между правоохранительными органами и органами исполнительной власти, повышения уровня сотрудничества с международными организациями. Ежедневная правоприменительная практика призвана выявлять вопросы, требующие дальнейшей проработки и совершенствования. Необходимость некоторых изменений обусловлена потребностями общества и государства. Таким образом, одними из основных задач в области фиксации и расследования преступлений, совершенных с использованием информационно-коммуникационных технологий, являются формирование международно-правовых механизмов борьбы с киберпреступностью в контексте процессов глобализации, повышение скорости сбора, обработки и обмена оперативными данными, дальнейшее совершенствование внутригосударственных механизмов, выработка единого, комплексного подхода во взаимодействии с институтами гражданского общества, научными и образовательными структурами.

Преступления, совершенные с использованием информационно-коммуникационных технологий (ИКТ); киберпреступность; глобализация; национальная безопасность; технологии; Следственный комитет РФ; расследование преступлений; уголовная ответственность; органы государственной власти

Alexander I. BASTRYKIN

Doctor of Legal Sciences, Professor, Honored Lawyer of the Russian Federation, Chairman of the Investigative Committee of the Russian Federation (Moscow)

IDENTIFICATION AND INVESTIGATION OF CRIMES COMMITTED USING INFORMATION AND COMMUNICATION TECHNOLOGIES

The article discusses the issues of detection and investigation of crimes committed using information and communication technologies as an important component of a set of measures to ensure the rights of citizens and restore social justice. Crimes of this category carry global threats, which is why the development and implementation of modern approaches to their detection, as well as the formation of an operational investigation methodology is an important activity of the Investigative Committee of the Russian Federation. The author notes the need for further improvement of both domestic and international mechanisms for combating cybercrime. This, in turn, requires improving preventive and applied mechanisms, establishing a highly effective system of interaction between law enforcement agencies and executive authorities, and

Crimes committed using information and communication technologies (ICT); cybercrime; globalization; national security; technology;

Investigative Committee of the Russian Federation; investigation of crimes; criminal liability; public authorities

increasing the level of cooperation with international organizations. Daily law enforcement practice is designed to identify issues that require further study and improvement. The need for some changes is due to the needs of society and the state. Thus, one of the main tasks in the field of fixing and investigating crimes committed using information and communication technologies is the formation of international legal mechanisms to combat cybercrime in the context of globalization processes, increasing the speed of collection, processing and exchange of operational data, further improvement of domestic mechanisms, development of a unified, integrated approach in cooperation with institutions civil society, scientific and educational structures.

В системе комплексных мер по обеспечению прав граждан и восстановлению социальной справедливости важное место занимает совершенствование системы выявления и расследования преступлений, совершенных с использованием информационно-коммуникационных технологий. На протяжении последних лет наблюдался рост числа таких преступлений, что в свою очередь несет в себе глобальные угрозы.

Так, согласно данным ведомственной статистики в 2019 г. выявлено 8812 таких преступлений, в 2020 г. – 11 493 (+30,4%), в 2021 г. – 12 112 (+5,4%). При этом качество проводимых Следственным комитетом расследований находится на стабильно высоком уровне, а общий объем раскрытых и расследованных преступлений в сфере ИКТ растет пропорционально повышению числа зарегистрированных правонарушений.

Работа по пресечению и предупреждению таких преступлений в Следственном комитете РФ носит системный, комплексный характер, а ее успех во многом определяется единством подходов в структурном взаимодействии как органов, осуществляющих предварительное расследование, так и государственных органов, обеспечивающих контроль за деятельностью в сфере информационных систем.

Общественная опасность преступлений, совершенных с использованием информационно-коммуникационных технологий, состоит в том, что эти преступления направлены на подрыв информационной безопасности и во многом на дестабилизацию работы институтов финансовой системы страны. Технические средства и программный софт наряду с повышением скорости взаимодействия и обмена данными обеспечивают основу для создания, развития и финансирования незаконной деятельности.

Столь стремительное развитие информационно-коммуникационных технологий требует выработки комплекса мероприятий, реализация которых будет способствовать повышению количественного соотношения совершаемых преступлений к выявленным и доказанным.

В данном контексте немаловажным представляется тот факт, что процессы глобализации, как на межгосударственном уровне, так и в интернет-пространстве, обусловили необходимость формирования международных механизмов борьбы с киберпреступностью. В сложившихся условиях СК России удалось выработать и успешно применить на практике ряд системных подходов при расследовании преступлений, совершенных с использованием информационно-коммуникационных технологий.

Анализируя уголовные дела, преступления по которым совершены с использованием информационно-коммуникационных технологий, а также учитывая тенденцию к увеличению роста числа преступлений данной категории, можно вполне обоснованно предположить, что пик отмеченных показателей еще не достигнут и в среднесрочном периоде тенденция увеличения числа преступлений, совершенных с использованием ИКТ, будет сохраняться.

В структуре преступных деяний, совершенных с использованием информационно-коммуникационных технологий, продолжают преобладать преступления против собственности (кражи, мошенничества и др.), против здоровья населения и общественной нравственности (производство и сбыт наркотических средств, изготовление и оборот порнографических материалов и др.).

С целью сокращения роста преступлений указанных категорий, а также проведения профилактических и превентивных мероприятий, направленных на недопущение условий, при которых совершение таких преступлений становится возможным, следственные подразделения ориентированы на необходимость уделять повышенное внимание правонарушителям, которые ранее были замечены в совершении аналогичных преступлений. Кроме того, при наличии признаков преступления и достаточных оснований для возбуждения уголовного дела с целью эффективного и всестороннего расследования обстоятельств преступного деяния следователям надлежит незамедлительно возбуждать уголовные дела.

Говоря о некоторых особенностях методики организации предварительного расследования по уголовным делам рассматриваемой категории, следует

отметить, что расследование анализируемого вида представляет особую сложность и связано с организационными трудностями, обусловленными их спецификой, неочевидностью, зачастую межрегиональным и международным характером. Для организации системной работы на данном направлении в центральном аппарате Следственного комитета функционирует специализированное подразделение по расследованию киберпреступлений и преступлений в сфере высоких технологий, а также подразделение компьютерно-технических и инженерно-технических исследований, сотрудники которых осуществляют предварительное следствие и производство экспертиз по делам об анализируемых преступлениях.

Тактика и методика расследования преступлений, совершенных с использованием информационно-коммуникационных технологий, позволили выработать методологические подходы к организации предварительного расследования по уголовным делам, где с целью совершения преступлений злоумышленники используют современные технологии коммуникаций. Для повышения эффективности и качества работы на данном направлении в территориальных следственных органах ведомства введена специализация следователей по расследованию указанного вида преступных деяний. С учетом особенностей конкретного уголовного дела, проведение следственных действий, а также формирование исчерпывающей доказательственной базы поручается наиболее опытным следователям, имеющим большой профессиональный стаж и обладающим необходимыми навыками работы.

Представляется, что к основным катализаторам роста преступлений, совершаемых с использованием ИКТ, можно отнести следующие факторы: продолжающийся процесс широкой глобализации; пандемия и постпандемийный период; пересмотр государствами подхода к возможностям, предоставляемым современными ИКТ, более активное их использование в военно-политических и экономических целях; недостаточное законодательное регулирование указанной области с учетом современных реалий и слабый технологический контроль со стороны государств за виртуальным пространством; изменение подходов к оценке уголовно наказуемых деяний, относящихся к совершаемым с использованием ИКТ, расширение составов преступлений, применяемых к данной сфере отношений, и, как следствие, рост соответствующих статистических показателей.

В целях своевременного реагирования на вновь возникающие вызовы и угрозы, которые несут в себе риски совершения преступлений, связанных с использованием информационно-коммуникационных технологий, Следственным комитетом принимаются системные меры, в том числе связанные с внедрением технических комплексов и средств, межведомственных автоматизированных поисковых систем, региональных разработок, направленных на выявление, предупреждение и пресечение преступлений в сфере ИКТ. В первую очередь такие инструменты позволяют эффективно пресекать наиболее опасные посягательства, среди которых: незаконный оборот наркотических средств, оружия, торговля людьми, распространение детской порнографии, преступления террористической направленности.

Важно отметить, что проблеме формирования международных механизмов по борьбе с киберпреступностью и обеспечению стабильности в информационной сфере было посвящено заседание Совета Безопасности РФ. В своем выступлении заместитель Председателя Совета Безопасности РФ Д. А. Медведев справедливо отметил: «Цифровую среду активно используют международные террористы, организованная преступность. Распространена практика создания хакерами межнациональных группировок. Их участники могут находиться на территории разных континентов, что создает серьезные трудности в расследовании компьютерных преступлений» [1]. Также в ходе заседания необходимость рассмотрения основных аспектов развития и совершенствования правового регулирования в данном направлении была отмечена руководителями органов государственной власти, профильных министерств и ведомств.

В современном контексте следует уточнить, что Концепция развития национальной системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, утв. Президентом РФ 30 мая 2018 г. [2], среди прочих целей предусматривает снижение уровня террористической угрозы и экстремистских проявлений в обществе, обеспечение законности и прозрачности деятельности некоммерческих организаций. Не секрет, что финансирование террористической деятельности, распространение террористической идеологии, вербовка последователей различных радикальных течений зачастую происходят с использованием информационно-коммуникационных средств. Таким образом, в современных реалиях цифровизации разработка и внедрение технических комплексов, помогающих выявлять и фиксировать преступления, совершенные с использованием ИКТ, значительно повышают эффективность работы правоохранительной системы в данном направлении.

Важнейшее значение в рассматриваемом вопросе представляет организация взаимодействия на уровне профильных министерств и ведомств. Сотрудники СК России принимают участие в деятельности межведомственных рабочих групп и тематических совещаний, в рамках которых рассматриваются вопросы актуализации нормативной и методической базы по

противодействию преступлениям в сфере ИКТ. Особое внимание в коллективной работе уделяется вопросам расширения использования в практической деятельности автоматизированных поисковых систем, направленных на выявление, предупреждение и пресечение преступлений в сфере ИКТ.

В частности, сотрудниками центрального аппарата ведомства на постоянной основе применяется сервис Росфинмониторинга для отслеживания операций с криптовалютой «Прозрачный блокчейн», возможности которого используются для установления цифровых транзакций по уголовным делам и деанонимизации пользователей.

В то же время существующая активность правоохранительного блока в сегменте повышения оперативности и эффективности извлечения электронно-цифровых следов при работе с открытыми источниками информации в сети Интернет представляется недостаточной и требующей корректировки.

Так, в настоящее время сотрудники, осуществляющие оперативно-розыскную деятельность, осведомлены о постоянно изменяющихся возможностях получения оперативной и следственно значимой информации, позволяющей в сжатые сроки идентифицировать фигурантов уголовных дел и лиц, обладающих ценными сведениями, в том числе находящихся за пределами нашего государства.

В связи с изложенным представляется необходимым проработать вопрос создания криминалистической системы, позволяющей идентифицировать пользователей сети Интернет по электронно-цифровым следам, обеспечив допуск 24/7 к такой системе представителей всех правоохранительных органов.

Одновременно с этим стоит отметить тенденцию к повышению законодательных мер по защите национальных интересов Российской Федерации в вопросах противодействия финансированию терроризма как одной из разновидностей преступлений, совершаемых с использованием информационно-коммуникационных технологий. 10 января 2021 г. вступили в силу поправки к Федеральному закону «О противодействии легализации доходов, полученных преступным путем, и финансированию терроризма» [3], которые усиливают контроль за операциями с денежными средствами. Так, информация о снятии или зачислении наличных на сумму свыше 600 тыс. руб. теперь будет передаваться в Росфинмониторинг [4, с. 9–14].

Важное значение в деятельности Следственного комитета приобрело содействие в пределах компетенции формированию системы международной информационной безопасности (далее – МИБ), направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности. Данная деятельность осуществляется в соответствии с Доктриной информационной безопасности, утв. указом Президента РФ от 5 декабря 2016 г. № 646 [5], и Основами государственной политики Российской Федерации в области международной информационной безопасности, утв. указом Президента РФ от 12 апреля 2021 г. № 213 [6]. Преступления, совершаемые с использованием ИКТ, имеют глобальный характер и элементы транснациональности, что делает международное сотрудничество ключевым фактором принятия эффективных мер противодействия.

В настоящее время наиболее широким по числу участников международным документом в рассматриваемой области является Конвенция о преступности в сфере компьютерной информации от 23 ноября 2001 г. (Будапештская конвенция) [7]. Однако Российская Федерация в этом договоре не участвует.

Таким образом, Россия не имеет специального договора с ведущими в области ИКТ зарубежными странами о борьбе с компьютерными преступлениями. Правовая помощь по уголовным делам о них запрашивается и оказывается Россией в рамках универсальных, региональных общеуголовных международных соглашений, таких как Европейская конвенция о взаимной правовой помощи по уголовным делам от 20 апреля 1959 г. [8] и Дополнительные протоколы к ней, Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам от 22 января 1993 г. [9], двусторонних договоров о правовой помощи и правовых отношениях, имеющих обязательный характер резолюций Совета Безопасности ООН и на основе принципа взаимности. Также ряд договоров о сотрудничестве в указанной области заключен с государствами – членами СНГ, а также в рамках ОДКБ.

Перспективным представляется развитие международного партнерства, в частности, в рамках Соглашения между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г. [10]. В числе основных направлений взаимодействия в документе названы противодействие угрозам использования ИКТ в террористических целях и противодействие информационной преступности. В то же время существующее несовершенство международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий, затрудняет формирование эффективной системы МИБ.

Стоит отметить, что в сфере уголовного судопроизводства в контексте обеспечения МИБ особую значимость имеет не только выработка единого алгоритма информационного взаимодействия правоохранительных и судебных органов, но и гармонизация

уголовного и уголовно-процессуального законодательства государств.

На фоне имеющихся вопросов технического характера (например, при производстве предварительного расследования требуется извлечение данных, находящихся в электронных устройствах и облачных сервисах, получение сведений, скрытых посредством сетевых технологий, обеспечивающих анонимность в сети Интернет, при отсутствии единого стандарта хранения цифровых данных провайдерами и операторами связи, а также единого на международном уровне порядка предоставления услуг связи и доступа в сеть Интернет и связанной с этим необходимости «деанонимизации» (раскрытия личности) владельца или пользователя сервиса цифровых услуг) и вопросов сохранности, оперативного изъятия и передачи цифровых данных ключевой проблемой на этом этапе является отсутствие полноценной международно-правовой базы, регулирующей деятельность государств в сфере использования ИКТ.

Законодательство и правоприменительная практика Российской Федерации не предусматривают возможности непосредственного доступа иностранных правоохранительных и судебных органов с какими-либо запросами (включая просьбы о сохранении (бронировании) данных, добровольном раскрытии информации в чрезвычайных ситуациях, в том числе с согласия пользователя) к российским поставщикам ИКТ-услуг – так называемого асимметричного (диагонального) сотрудничества, относя такие контакты исключительно к компетенции российских органов. При этом требуемая срочность запроса должна обеспечиваться межведомственными коммуникационными сетями 24/7.

В этой связи актуальным видится сосредоточение внимания на имеющемся переговорном механизме ООН, направленном на скорейшее принятие согласованных мер по снижению угроз в сфере информационной безопасности и продолжение работы по МИБ в рамках российской инициативы – Рабочей группы ООН открытого состава. Механизм указанной группы, предполагающий открытый характер обмена мнениями экспертов по данной проблематике, также предоставляет возможность выработки конкретных практических решений вплоть до полномасштабных конвенций и договоров.

Необходимо отметить актуальную проблему, связанную с исполнением запросов о правовой помощи, в том числе по уголовным делам в сфере информационно-коммуникационных технологий, а именно сроки исполнения таких запросов, которые могут составлять от одного до двух лет.

К задачам по совершенствованию международного сотрудничества в сфере борьбы с преступлениями, совершаемыми с использованием ИКТ, можно отнести определение на международном уровне единой классификации компьютерных преступлений и рекомендации государствам по криминализации деяний в данной сфере в национальных законодательствах. Важное значение имеют развитие и совершенствование не только процесса получения, оценки и использования электронных доказательств, но и электронных каналов сношений с зарубежными партнерами, обеспечение юридически значимого международного электронного документооборота.

Например, во время пандемии коронавирусной инфекции из логистических и санитарных соображений центральные органы по вопросам правовой помощи и правовых отношений по уголовным делам многих государств мира уведомили о своем временном переходе на работу с исходящей и входящей корреспонденцией исключительно в безбумажной форме, а также об отложении исполнения многих запросов.

С рядом стран было приостановлено международное почтовое сообщение, например, «Почта России» заблокировала прием отправлений, адресованных в государства, которые временно прекратили обработку входящей и исходящей международной почты.

Также необходимо отметить, что выявление, пресечение, расследование и предотвращение преступлений, совершаемых с использованием ИКТ, требует серьезных специальных познаний от следователей, сотрудников, осуществляющих оперативное сопровождение, и вовлеченных экспертов.

По этой причине огромное значение приобретает непрерывный процесс изучения достижений науки и техники, а также вопросы обеспечения качественного обучения с целью актуализации компетенций специалистов. В связи с этим Следственным комитетом на постоянной основе проводятся научно-практические мероприятия, носящие межведомственный и международный характер, осуществляется подготовка научных и учебных изданий в сфере противодействия анализируемой категории преступлений. Например, Санкт-Петербургская академия ведомства ежегодно выступает инициатором и соорганизатором научно-практических конференций с участием представителей стран – участниц СНГ, Международной полицейской ассоциации и др.

Также проводятся круглые столы для компетентных органов иностранных государств, например, по теме «Противодействие легализации (отмыванию) преступных доходов» с участием представителей Академии правоохранительных органов Республики Казахстан, Института повышения квалификации и переподготовки Следственного комитета Республики Беларусь, Академии Генеральной прокуратуры Республики Узбекистан.

В целях повышения профессионального уровня сотрудников ведомства разработаны специализированные учебные программы, например «Расследование преступлений в сфере информационных, телекоммуникационных и высоких технологий», «Расследование преступлений, совершенных с использованием цифровой валюты и цифровых финансовых активов». К реализации таких программ привлекаются лучшие российские эксперты, имеющие опыт работы в сфере ИКТ и владеющие передовыми практиками, в том числе представители Росфинмониторинга, Банка России и др.

Вместе с тем представляется, что применительно ко всем правоохранительным органам процесс обучения, повышения квалификации и обмена передовыми достижениями, в том числе с компетентными органами зарубежных партнеров, в области борьбы с постоянно обновляющимися способами совершения преступлений с использованием ИКТ носит недостаточно систематизированный характер и требует корректировки.

Кроме того, сотрудники ведомства принимают участие в деятельности ряда многосторонних и двусторонних международных площадок по урегулированию проблемных аспектов в анализируемой сфере.

Так, в 2021 г. представители Следственного комитета вошли в состав делегаций, участвовавших в российско-нидерландских и российско-иранских межведомственных консультациях по информационной безопасности, очередном заседании российско-французской рабочей группы межведомственного стратегического диалога по кибербезопасности и т.д.

С учетом изложенного, в целях выработки мер, направленных на дальнейшее формирование международных механизмов по борьбе с преступлениями, совершаемыми с использованием ИКТ, и обеспечения стабильности в информационной сфере представляется необходимым выполнить следующее:

1) продолжить работу по продвижению и поддержке российского проекта универсальной конвенции о противодействии использованию ИКТ в преступных целях, принятие которого придаст импульс как развитию международных отношений в указанной сфере, так и модернизации законодательства РФ, регулирующего цифровые отношения.

Одновременно необходимо интенсифицировать работу по гармонизации российского законодательства в обозначенной области с учетом положений проекта вышеуказанной конвенции. При этом целесообразно классифицировать виды правонарушений и преступлений с определением критериев их отнесения к совершаемым с использованием ИКТ.

Следует акцентировать внимание на продолжении выработки единой терминологии в указанной области, отграничении термина «киберпреступления» как частного по отношению к используемому в российском проекте конвенции и национальным экспертным сообществом понятию «преступления, совершаемые с использованием информационно-коммуникационных технологий»;

2) проработать вопрос о создании единой криминалистической системы идентификации пользователей сети Интернет по электронно-цифровым следам, которые остаются в результате посещения сайтов и использования онлайн-сервисов. Внедрение такой системы упростит и ускорит процедуру поиска и идентификации лиц, совершающих противоправные деяния с использованием ИКТ;

3) изучить потребность во введении постоянно действующих программ подготовки и непрерывного повышения квалификации сотрудников правоохранительных органов по борьбе с преступлениями, совершаемыми с использованием ИКТ, а также механизмов по обмену передовым опытом в указанной сфере с компетентными органами иностранных государств – партнеров Российской Федерации.

Для реализации указанных предложений могут быть привлечены Следственный комитет РФ, ФСБ России, МВД России, а также Генеральная прокуратура РФ, Минцифры России и другие заинтересованные органы, при этом сроки выполнения следует определить после концептуального одобрения и межведомственного согласования обозначенных инициатив.

Уверен, что реализация озвученных задач наряду с совершенствованием мер по повышению эффективности международного сотрудничества с государствами – членами ОДКБ в борьбе с киберпреступностью, укрепление оперативно-технического сотрудничества с зарубежными государствами при расследовании киберпреступлений, формирование и укрепление института электронных доказательств и выстраивание высокоэффективной системы взаимодействия между правоохранительными органами и органами исполнительной власти позволят своевременно реагировать на вновь возникающие вызовы и угрозы.

Пристатейный библиографический список

1. Заместитель Председателя Совета Безопасности Российской Федерации Д. А. Медведев провел совещание по вопросу «О формировании международных механизмов по борьбе с киберпреступностью и обеспечения стабильности в информационной сфере» // Совет Безопасности Российской Федерации : сайт. URL: http://www.scrf.gov.ru/news/allnews/3191/ (дата обращения: 07.04.2022).

2. Концепция развития национальной системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма от 30 мая 2018 г. // Президент России : сайт. URL: http://www.kremlin.ru/supplement/5310 (дата обращения: 07.04.2022).
3. Федеральный закон от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступных путем, и финансированию терроризма» // СПС «КонсультантПлюс»
4. *Бастрыкин А. И.* О практике выявления и расследования следственными органами СК РФ легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма // Lex Russica. 2021. Т. 74. № 7.
5. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс».
6. Указ Президента РФ от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // СПС «КонсультантПлюс».
7. Конвенция о преступности в сфере компьютерной информации (ETS № 185) (заключена в г. Будапеште 23 ноября 2001 г.) // СПС «КонсультантПлюс».
8. Европейская конвенция о взаимной правовой помощи по уголовным делам (заключена в г. Страсбурге 20 апреля 1959 г.) // СПС «КонсультантПлюс».
9. Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (заключена в г. Минске 22 января 1993 г.) (вступила в силу 19 мая 1994 г., для Российской Федерации 10 декабря 1994 г.) // СПС «КонсультантПлюс».
10. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (вместе с перечнями основных понятий и видов угроз, их источников и признаков) (заключено в г. Екатеринбурге 16 июня 2009 г.) // СПС «КонсультантПлюс».

References

1. Deputy Chairman of the Security Council of the Russian Federation Dmitry Medvedev Held a Meeting on the Issue "On the Formation of International Mechanisms to Combat Cybercrime and Ensure Stability in the Information Sphere". URL: http://www.scrf.gov.ru/news/allnews/3191/ (date of the application: 07.04.2022).
2. Concept of Development of the National System for Countering the Legalization (Laundering) of Proceeds from Crime and the Financing of Terrorism of 30 May 2018. URL: http://www.kremlin.ru/supplement/5310 (date of the application: 07.04.2022).
3. Federal Law of 7 August 2001 No. 115-FZ "On Countering the Legalization (Laundering) of Proceeds from Crime and the Financing of Terrorism" (SPS "ConsultantPlus").
4. *Bastrykin A. I.* On the Practice of Detection and Investigation by the Investigative Bodies of the RF IC of the Legalization (Laundering) of Proceeds from Crime and the Financing of Terrorism. *Lex Russica*. 2021. Vol. 74. No. 7.
5. Decree of the President of the Russian Federation of 5 December 2016 No. 646 "On Approval of the Information Security Doctrine of the Russian Federation" (SPS "ConsultantPlus").
6. Decree of the President of the Russian Federation of 12 April 2021 No. 213 "On Approval of the Fundamentals of the State Policy of the Russian Federation in the Field of International Information Security" (SPS "ConsultantPlus").
7. Convention on Crime in the Field of Computer Information (ETS No. 185) (concluded in Budapest on 23 November 2001) (SPS "ConsultantPlus").
8. European Convention on Mutual Legal Assistance in Criminal Matters (concluded in Strasbourg on 20 April 1959) (SPS "ConsultantPlus").
9. Convention on Legal Assistance and Legal Relations in Civil, Family and Criminal Cases (concluded in Minsk on 22 January 1993) (entered into force on 19 May 1994, for the Russian Federation on 10 December 1994) (SPS "ConsultantPlus").
10. Agreement Between the Governments of the Shanghai Cooperation Organization Member States on Cooperation in the Field of International Information Security (together with Lists of Basic Concepts and Types of Threats, Their Sources and Signs) (concluded in Yekaterinburg on 16 June 2009) (SPS "ConsultantPlus").