УДК 343.9.01
DOI: https://doi.org/10.17816/RJLS60982

Особенности формирования алгоритмов выявления, раскрытия и расследования «высокотехнологичных» преступлений экстремистского характера, совершенных с использованием сети Интернет

© В.В. Бычков, В.А. Прорвич

Московская академия Следственного комитета Российской Федерации

Аннотация. В статье рассматриваются важнейшие проблемы, возникающие при выявлении, раскрытии и расследовании «высокотехнологичных» экстремистских преступлений, совершенных с использованием сети Интернет. Выявлены основные источники юридических ошибок, возникающих уже на стадии идентификации обязательных и факультативных признаков преступлений данного вида по их развернутой уголовно-правовой характеристике. Описаны содержательные особенности семи групп алгоритмов, на основе которых может быть создано надлежащее информационное обеспечение всех видов следственных действий. Рассмотрены особенности реализации данной системы алгоритмов в рамках интерактивной экспертной системы, позволяющей следователю в режиме реального времени получить необходимую информационную поддержку.

Ключевые слова: экстремизм; преступления экстремистского характера; высокотехнологичные экстремистские преступления; уголовно-правовая характеристика; квалификация преступлений; юридические ошибки; информационное обеспечение; алгоритм; искусственный интеллект; интерактивная экспертная система.

Как цитировать:
Бычков В.В., Прорвич В.А. Особенности формирования алгоритмов выявления, раскрытия и расследования «высокотехнологичных» преступлений экстремистского характера, совершенных с использованием сети Интернет // Российский журнал правовых исследований. 2021. Т. 8. № 1. С. 89–96. DOI: https://doi.org/10.17816/RJLS60982

Рукопись получена: 15.02.2021 **Рукопись одобрена:** 03.03.2021 **Опубликована:** 22.03.2021

DOI: https://doi.org/10.17816/RJLS60982

Development of Algorithms to Identify, Disclose, and Investigate High Tech Crimes of an Extremist Nature Committed Via the Internet

© V.V. Bychkov, V.A. Prorvich

Moscow Academy of the Investigative Committee of the Russian Federation

***ABSTRACT*:** This article examines the most important problems arising in the detection, disclosure, and investigation of high tech extremist crimes committed through use of the Internet. The main source of legal errors is found through the identification of mandatory and optional signs of crimes of this type according to their deployed criminal legal characteristics, have been revealed. The specific features of seven groups of algorithms are described, on the basis of which proper information support of all kinds of investigative actions can be created. The specifics of this system of algorithms, within an interactive expert framework, allow investigators to receive necessary information support in real time.

Keywords: extremism; extremist crimes; high tech extremist crimes; criminal characterization; crime qualification; legal errors; information support; algorithm; artificial intelligence; interactive expert system.

To cite this article:
Bychkov VV, Prorvich VA. Development of algorithms to identify, disclose, and investigate high tech crimes of an extremist nature committed via the internet. *Russian journal of legal studies.* 2021;8(1):89–96. DOI: https://doi.org/10.17816/RJLS60982

Received: 15.02.2021 **Accepted:** 03.03.2021 **Published:** 22.03.2021

В Российской Федерации с начала 90-х годов прошлого века фиксируется рост проявлений экстремизма [1, с. 60–71]. В последние годы отмечается качественное изменение характера, способов совершения и субъектов таких преступлений со значительным увеличением экстремистских преступлений, осуществляемых с использованием информационно-телекоммуникационных сетей, в том числе Интернета [2, с. 43–46]. Выявление, раскрытие и расследование преступлений данного вида осложняется применением при их совершении специфических технических средств — электронно-вычислительного оборудования и современных информационных технологий, адаптированных к сети Интернет. Выявление таких преступлений, их раскрытие и расследование нередко вызывает определенные затруднения у правоприменителей.

Решению данной проблемы однозначно будет способствовать использование правоохранительными органами современных информационных технологий, включая элементы искусственного интеллекта [3, с. 45–50]. Хотя при этом нельзя не учитывать появление новых задач. Прежде всего, необходимо подчеркнуть, что искусственный интеллект определяется в рамках науки информатики как сложная компьютерная программа, созданная для решения определенных задач без участия человека [4, с. 47–50; 5. с. 34–49].

Но правоприменение по уголовным делам не может осуществляться в автоматизированном режиме, без участия оперативных сотрудников, следователей и дознавателей, а затем прокуроров и судей. Поэтому возникает ряд принципиально новых задач организации взаимодействия юристов-правоприменителей с искусственным интеллектом, а точнее такого построения алгоритмов компьютерных программ данного вида, которое полностью укладывается в рамки уголовного и уголовно-процессуального права.

Анализ публикаций об особенностях применения современных информационных технологий, включая использование различных видов искусственного интеллекта, правоохранительными органами показывает, что чаще всего речь идет о применении уже готовых, «фирменных» программ, разработанных крупными компьютерными фирмами. При этом во многих случаях речь идет о целевых установках, связанных с обработкой больших данных, содержащихся в специализированных базах данных правоохранительных органов.

Вместе с тем для выявления, раскрытия и расследования «высокотехнологичных» экстремистских преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, в том числе Интернета, с широким применением электронных документов различного вида — графических, текстовых, причем на разных языках, табличных и иных, необходимо более широкое применение самых разнообразных информационных технологий. При этом проявляется активность как экспертов-компьютерщиков, объявивших несколько лет назад о создании своей «науки» — форензики [6], так и крупных компьютерных фирм, претендующих не только на создание компьютерной криминалистики, но и на ее практическое применение [7].

Отдавая должное усилиям ученых и специалистов, разрабатывающих проблемы информационной и компьютерной безопасности, а также активной позиции опытных экспертов-компьютерщиков, необходимо подчеркнуть возникновение высокого уровня рисков совершения юридических ошибок различного вида, способных оказать негативное влияние на всю систему уголовного судопроизводства. Прежде всего, речь идет о том, что в рамках информационных технологий, предлагаемых следователям, используются компьютерные программы, созданные крупными западными фирмами. Более того, эти программы настолько сложны, что их пишут и отлаживают крупные коллективы, которыми руководят суперпрограммисты, а не юристы. Даже если к участию в таких коллективах привлекаются юристы, то полное взаимопонимание с программистами у них возникает крайне редко.

Но и в тех случаях, когда сложные компьютерные программы ведущие компьютерные фирмы создают с учетом мнения юристов, то речь идет о тех юристах, которые мыслят в парадигме англосаксонского права. Особенно ярко это проявляется в программах, предлагаемых для внедрения компьютерных роботов на основе нейросетевых алгоритмов в российское электронное судопроизводство и даже в электронное правосудие [8; 9, с. 181–184]. Это создает неприемлемо высокий уровень рисков совершения юридических ошибок в уголовном судопроизводстве. Особенно опасны такие ошибки при выявлении, раскрытии и расследовании экстремистских преступлений, совершаемых с использованием Интернета.

Вполне естественным выходом является формирование при активном участии юристов-правоприменителей таких алгоритмов, которые могут быть положены в основу информационных технологий, необходимых следователям и оперативным сотрудникам для существенного повышения эффективности борьбы с преступлениями рассматриваемого вида.

Результаты проведенных исследований показали, что во многих случаях при подготовке и совершении экстремистских преступлений с использованием сети Интернет выявлялись признаки второго преступления, отнесенного законодателем к сфере уголовно наказуемых деяний с компьютерной информацией. Более того, активная деятельность специалистов по информационной безопасности и форензике, о которой упоминалось выше, нацелена на выявление и борьбу именно с «компьютерными» преступлениями. Из-за этого применение соответствующих информационных технологий может приводить к быстрому выявлению соответствующих

DOI: https://doi.org/10.17816/RJLS60982

преступлений. Однако при этом может происходить «маскировка» признаков экстремистских преступлений, совершенных с использованием сети Интернет. То есть подобные информационные технологии универсального характера могут не облегчать, а, наоборот, затруднять работу следователей и оперативных сотрудников по выявлению, раскрытию и расследованию преступлений рассматриваемого вида.

Поэтому при разработке проблемно-ориентированных алгоритмов для создания информационных технологий, нацеленных на повышение качества всего комплекса средств, используемых для борьбы с современными экстремистскими преступлениями, необходимо применение всего арсенала наук уголовно-правового блока. Соответственно, при этом возможно создание нескольких групп таких алгоритмов следующего вида.

Первая группа алгоритмов нацелена на создание прочного, научно обоснованного фундамента для всей совокупности следственных действий, направленных на выявление, раскрытие и расследование преступлений рассматриваемого вида, включая взаимодействие с оперативными сотрудниками, экспертами и специалистами. С ее использованием создается возможность формирования развернутой уголовно-правовой характеристики конкретного преступления, установления и систематизации всех его обязательных и факультативных признаков. При этом приходится учитывать, что диспозиции уголовно-правовых норм о преступлениях экстремистского характера носят бланкетный характер, а при раскрытии их содержательных особенностей с применением положений гражданского и специального законодательства возникают риски выхода за рамки уголовного права. Поэтому необходимо включить в состав алгоритмов этой группы ряд процедур по контролю за данной деятельностью следователя, которые практически не отличаются от разработанных для других уголовно-правовых норм [8].

Следует отметить, что при раскрытии содержательных особенностей диспозиций указанных преступлений приходится учитывать и наличие ряда противоречий некоторых положений действующего законодательства об информации и информационной деятельности[1], электронном документообороте[2] и электронной подписи[3], а также о техническом регулировании в данной сфере. Необходимо учитывать и проблемы, связанные с тем, что содержание соответствующих правовых норм в некоторых случаях приходится раскрывать с использованием положений подзаконных актов и иных инструктивно-методических документов.

Проведенные исследования показали, что по этим и ряду других причин следователи нередко совершают юридические ошибки при идентификации важнейших признаков экстремистских преступлений, совершенных с использованием сети Интернет. Поэтому возникает объективная необходимость в выполнении целенаправленных исследований и разработок, позволяющих сформировать «эталонные» варианты научно обоснованных и выверенных по важнейшим критериям уголовного права развернутых уголовно-правовых характеристик преступлений рассматриваемого вида.

На этой основе могут быть сформированы проблемно-ориентированные базы данных, содержащие информационно полные перечни обязательных признаков «основных» и «дополнительных» вариантов составов «высокотехнологичных» преступлений экстремистской направленности. С помощью них создаются соответствующие алгоритмы обработки всего комплекса информации, имеющей значение для надлежащего выявления, раскрытия и расследования преступлений данного вида.

Важно обратить внимание на то, что речь идет не только о «фильтрации» той весьма обширной информации, которая прямо или косвенно может быть связана с конкретным преступлением. С помощью алгоритмов этой группы на основе отобранных из баз данных развернутых вариантов составов данного преступления возможно также сформировать план соответствующих следственных действий как на стадии выполнения доследственной проверки сведений о данном преступлении, так и на первоначальном, последующем и завершающем этапах расследования соответствующего уголовного дела. При этом для надлежащей организации взаимодействия следователя с оперативными сотрудниками, судебными экспертами и специалистами могут использоваться другие группы алгоритмов, рассматриваемые ниже.

Одной из важнейших особенностей первой группы алгоритмов является необходимость дифференцирования признаков тех составов преступлений, которые связаны с высокотехнологичным экстремизмом. Проведенный анализ показывает, что нередко из-за неверной идентификации состава конкретного преступления рассматриваемого вида возникают юридические ошибки. Чаще всего это связано с тем, что совершение экстремистских преступлений с использованием сети Интернет сопряжено с незаконным проникновением в определенные информационные системы, взломом их систем защиты, в том числе с применением компьютерных вирусов и иных высокотехнологичных приемов. То есть фактически в таких случаях речь идет, прежде всего, о совершении определенного преступления в сфере компьютерной информации, предусмотренного главой 26 УК РФ.

---

[1] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006 № 31 (часть I). Ст. 3448.

[2] Федеральный закон от 24.04.2020 № 122-ФЗ «О проведении эксперимента по использованию электронных документов, связанных с работой» // Собрание законодательства РФ. 2020. № 17. Ст. 2700.

[3] Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // Собрание законодательства РФ. 2011. № 15. Ст. 2036.

DOI: https://doi.org/10.17816/RJLS60982

В результате на практике могут возникать следующие ситуации. Во-первых, кроме экстремистского преступления может быть совершено и компьютерное преступление тем же лицом или лицами с определенными формами соучастия. Понятно, что речь идет о выявлении совокупности преступлений, для надлежащей идентификации признаков, раскрытия и расследования которых необходимо использовать соответствующее информационно-методическое обеспечение на основе определенной группы алгоритмов, особенности которых рассматриваются ниже.

Во-вторых, может быть совершено «высокотехнологичное» экстремистское преступление, причем состав одного из компьютерных преступлений отсутствует. Соответственно, речь идет о формировании весьма сложного состава преступления, а для идентификации всех его обязательных и факультативных признаков необходимо применение специальных алгоритмов и созданного на их основе информационного обеспечения.

В-третьих, речь может идти о совершении одного или нескольких компьютерных преступлений, с определенными признаками экстремистского преступления, но их недостаточно для надлежащего формирования состава данного преступления по его развернутой уголовно-правовой характеристике.

В-четвертых, детальный анализ признаков состава предполагаемого преступления может показать на отсутствие такого преступления.

В-пятых, может быть выявлено наличие признаков нескольких преступлений рассматриваемого вида, а также определенных «смежных» преступлений, которые могут образовывать идеальную или реальную совокупность преступлений. В таких случаях важно обратить внимание на соответствующие положения Общей части Уголовного кодекса РФ, раскрывающие критерии для их идентификации. При этом группа алгоритмов для информационного обеспечения необходимого и достаточного комплекса следственных действий отличается наибольшей сложностью как в их разработке, так и в практическом применении.

Понятно, что при раскрытии особенностей развернутой уголовно-правовой характеристики столь сложных «высокотехнологичных» экстремистских преступлений и идентификации всей совокупности обязательных и факультативных признаков следователь сталкивается с рядом проблем, решить которые даже с привлечением опытнейших экспертов и специалистов оказывается далеко не просто. Поэтому приходится еще раз подчеркнуть необходимость проведения подобных комплексных исследований силами ведущих ученых и специалистов в различных сферах наук уголовно-правового блока, информатики и кибернетики. И созданные на их основе алгоритмы проблемно-ориентированной обработки правовой информации позволят «контрастировать» всю совокупность различных вариантов формирования состава конкретного преступления рассматриваемого вида, минимизируя риски совершения юридических ошибок.

Для информационного обеспечения практической работы следователя на данной стадии обработки имеющейся информации о конкретном преступлении первая группа алгоритмов может быть использована при создании соответствующей интерактивной экспертной системы. При этом для того, чтобы обеспечить не только быстрый анализ особенностей многочисленных вариантов, подобных упоминавшимся выше, но и обоснование наиболее подходящих к конкретной ситуации со ссылками на положения конкретных нормативных правовых актов, возможно использование элементов искусственного интеллекта.

Здесь следует подчеркнуть, что соответствующие компьютерные программы в рамках интерактивной экспертной системы позволяют организовать диалог следователя со своим компьютером. Но эта экспертная система по своим функциям уже играет роль не столько справочной системы, подобной широко используемым Консультатнт Плюс, Гарант и т.п., а становится проблемно-ориентированным помощником следователя, выполняющим его конкретные задания, связанные с выявлением, раскрытием и расследованием конкретных высокотехнологичных экстремистских преступлений.

Вторая группа алгоритмов нацелена на информационную поддержку важнейшей стадии практической работы следователя по надлежащей квалификации конкретного высокотехнологичного экстремистского преступления. Ее структура имеет ряд особенностей, обусловленных целевой функцией, связанной с установлением взаимного соответствия полученных первоначальных сведений о совершенном деянии, а затем полученных доказательств тем признакам конкретного состава преступления, которые были формализованы по его развернутой уголовно-правовой характеристике. Для этого в параллельно-последовательном режиме формируется система юридических тождеств.

Левая часть каждого из тождеств данной системы последовательно заполняется описанием обязательных и факультативных признаков объекта, объективной стороны, субъекта и субъективной стороны данного преступления. В правую часть каждого из тождеств на стадии доследственной проверки помещаются сведения о квалифицируемом деянии, причем производится их сортировка по соответствию содержания тому признаку, который расположен в левой части каждого из тождеств. На стадии расследования уголовного дела в правую часть данных тождеств помещается описание полученных доказательств, прошедших надлежащую проверку и оценку.

То есть вторая группа алгоритмов тесно связана с первой группой, поскольку при формировании системы юридических тождеств необходимо использовать результаты применения алгоритмов формирования

развернутой уголовно-правовой характеристики данного преступления и формализации его обязательных и факультативных признаков. При этом может быть использовано несколько вариантов тех результатов обработки информации, которые были получены с использованием алгоритмов первой группы.

Применение алгоритмов первой и второй группы в рамках рассмотренной выше интерактивной экспертной системы позволяет создать прочный научно обоснованный фундамент для современного информационного обеспечения работы следователя по конкретному преступлению. Важно подчеркнуть, что речь идет не только о получении следователем обширных и юридически выверенных сведений о преступлении, которые он может использовать для надлежащей квалификации определенного деяния. Следователь также получает принципиально новые возможности и для научно обоснованного планирования своих действий на различных стадиях выявления, раскрытия и расследования высокотехнологичных экстремистских преступлений.

В частности, на стадии доследственной проверки сведений об определенном деянии, в котором предполагается наличие признаков преступления рассматриваемого вида, анализ содержательных особенностей сформированной системы юридических тождеств в большинстве случаев показывает наличие определенных информационных пробелов в их правой части. Для заполнения этих пробелов следователь в соответствии с положениями ст. 144 УПК РФ может привлечь специалистов и судебных экспертов, а также выполнить ряд других процессуально регламентированных действий до принятия решения о возбуждении уголовного дела. Вместе с тем они не могут заменить полноценное расследование уголовного дела, поэтому принимать обоснованное решение о возбуждении уголовного дела и его обоснование следователю приходится в условиях информационной неопределенности.

В такой ситуации по результатам анализа сформированной системы юридических тождеств следователь может не только констатировать наличие определенных информационных пробелов, но и проанализировать возможности их заполнения на стадии предварительного следствия. Это позволяет существенно снизить уровень рисков при принятии решения о возбуждении уголовного дела по результатам доследственной проверки с надлежащим информационным обеспечением на основе описанной выше интерактивной экспертной системы с использованием алгоритмов первой и второй группы.

На стадии предварительного следствия правая часть каждого из юридических тождеств формируется на основе полученных следователем доказательств, прошедших надлежащую проверку и оценку в соответствии с требованиями ст. 87 и 88 УПК РФ. Как правило, после завершения первоначального этапа расследования уголовного дела в системе юридических тождеств также может быть выявлен ряд информационных пробелов уже в собранной совокупности доказательств. После анализа их содержательных особенностей создаются новые возможности для корректировки первоначального плана расследования с его ориентацией на получение недостающих доказательств в рамках последующего этапа расследования уголовного дела. При этом могут использоваться различные следственные действия на основе положений криминалистической тактики, техники и методики, включая формирование следственных версий и их проверку, взаимодействие с оперативными сотрудниками, специалистами и судебными экспертами.

Для надлежащего информационного обеспечения перечисленных выше следственных и иных процессуально регламентированных действий могут использоваться алгоритмы третьей, четвертой и пятой групп. При этом третья группа может быть нацелена на информационное обеспечение важнейших положений криминалистической науки, четвертая — для информационного обеспечения взаимодействия с оперативными сотрудниками, а пятая — со специалистами и судебными экспертами.

Шестая группа алгоритмов нацелена на надлежащее информационное обеспечение проверки и оценки каждого из собранных доказательств по расследуемому уголовному делу. Их содержание обусловлено необходимостью обязательного выполнения требований ст. 87 и 88 УПК РФ. При этом используется специальный инструментарий, позволяющий привести доказательства различного вида к единому информационному формату, обеспечивая вместе с тем контроль за сохранением их правового статуса. Кроме этого, при взаимном сопоставлении доказательств при выполнении их проверки, а также при сопоставлении каждого из доказательств с критериями относимости, допустимости и достоверности, установленными ст. 88 УПК РФ для их оценки, используется интерактивный режим, позволяющий следователю принимать соответствующие решения самостоятельно.

Седьмая группа алгоритмов предназначена для надлежащего информационного обеспечения завершающего этапа расследования уголовного дела. Прежде всего, речь идет об установлении достаточности собранной совокупности доказательств, на что прямо указывается в требованиях ст. 88 УПК РФ. Правда, при этом содержательные особенности названного критерия в данной статье не раскрываются. Поэтому первая часть этой группы алгоритмов нацелена на формирование итогового варианта системы юридических тождеств с использованием уже рассмотренных выше алгоритмов второй группы. После этого выполняется анализ информационной полноты полученной системы — как на количественном, так и на качественном уровне.

Если выявляются информационные пробелы, а также возникают сомнения в том, что какое-либо из доказательств при дальнейшем рассмотрении уголовного дела

DOI: https://doi.org/10.17816/RJLS60982

прокурором и судом может быть исключено, что не позволит доказать наличие в расследуемом деянии состава преступления, то приходится возвращаться к предыдущему этапу расследования и принимать меры для получения недостающих доказательств. Но в том случае, когда информационные пробелы в итоговом варианте системы юридических тождеств отсутствуют, следователь может сделать вывод о наличии в расследуемом деянии состава преступления и принять обоснованное решение о достаточности собранной им совокупности доказательств. При этом он также принимает обоснованное решение о завершении предварительного следствия и переходе к завершающей стадии следственных действий — подготовке и оформлению обвинительного заключения по данному уголовному делу.

Используемое для этого информационное обеспечение основано на применении не только соответствующей части алгоритмов седьмой группы. Эта часть алгоритмов сопряжена и с другими группами алгоритмов, описанными выше, чтобы обеспечить возможность использования в тексте обвинительного заключения той информации, которая была получена на различных этапах расследования уголовного дела. При этом речь идет отнюдь не об «автоматической генерации» текста обвинительного заключения с помощью искусственного интеллекта.

С использованием описанной системы алгоритмов в рамках интерактивной экспертной системы у следователя возникает возможность в режиме реального времени получать необходимое ему в определенный момент информационное обеспечение на всем протяжении своей работы, начиная с доследственной проверки, всех этапов предварительного следствия и заканчивая подготовкой обвинительного заключения. Следует подчеркнуть, что при возникновении необходимости сформировать и провести сопоставление нескольких вариантов плана расследования, следственных версий, а также ряда других видов нового информационного обеспечения, возникающего в ходе выполнения процессуально регламентированных действий, следователь может получить его также в режиме реального времени.

Но речь идет не только о новых возможностях существенного сокращения трудоемкости и сроков выполнения большей части следственных действий. Не менее важно обратить внимание на ряд новых возможностей для значительного повышения качества следственных действий, что достигается в результате обработки больших объемов информации, имеющей отношение к расследуемому высокотехнологичному экстремистскому преступлению, в том числе с использованием элементов искусственного интеллекта. Такие объемы информации в настоящее время в ходе выявления преступлений данного вида и расследования соответствующих уголовных дел ни один следователь обработать не в состоянии. Из-за этого фактически используется лишь малая часть сведений о фактах и обстоятельствах, имеющих отношение к таким преступлениям. А возникающие пробелы и противоречия в собранной совокупности доказательств нередко приводят к развалу уголовного дела в суде, в результате чего преступники избегают заслуженного наказания.

Таким образом, для создания научных основ надлежащего информационного обеспечения всех стадий работы следователя по высокотехнологичным преступлениям экстремистского характера, совершенных с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, необходима консолидация усилий ученых и специалистов для разработки системы алгоритмов, рассмотренных в настоящей статье. На их основе могут быть созданы интерактивные экспертные системы, позволяющие в режиме реального времени обеспечить следователя всей необходимой информацией по его запросам.

СПИСОК ЛИТЕРАТУРЫ

1. Бычков В.В. Динамика российского терроризма и экстремизма в XXI веке // Расследование преступлений: проблемы и пути их решения. 2018. № 3(21). С. 60–71.

2. Бычков В.В. Информационно-телекоммуникационные сети как средство совершения преступлений экстремистской направленности // Вестник Московской академии Следственного комитета Российской Федерации. 2020. № 3. С. 43–46.

3. Бычков В.В. Искусственный интеллект: государственная политика и векторы применения // Расследование преступлений: проблемы и пути их решения. 2020. № 4. С. 45–50.

4. Бычков В.В., Прорвич В.А. Искусственный интеллект как средство противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет» // Вестник Московской академии Следственного комитета Российской Федерации. 2020. № 4. С. 47–52.

5. Бычков В.В., Прорвич В.А. Искусственный интеллект в борьбе с преступлениями, совершаемыми по экстремистским мотивам, с использованием Интернета // Современное уголовно-процессуальное право — уроки истории и проблемы дальнейшего реформирования. 2020. Т. 1. С. 34–49.

6. Федотов Н.Н. Форензика — компьютерная криминалистика. М.: Юридический Мир, 2007. 432 с.

7. Волынский А.Ф., Прорвич В.А. Компьютерная криминалистика в системе уголовно-правовой защиты «традиционной» и цифровой экономики: монография. М.: Экономика, 2020. 476 с.

8. Волынский А.Ф., Прорвич В.А. Электронное судопроизводство по преступлениям в сфере экономики (научно-практические аспекты): монография. М.: Экономика, 2019. 364 с.

9. Эриашвили Н.Д. Новый уровень разработки проблем электронного судопроизводства по преступлениям в сфере экономики // Государственная служба и кадры. 2020. № 1. С. 181–184.

DOI: https://doi.org/10.17816/RJLS60982

REFERENCES

1. Bychkov VV. Dynamics of russian terrorism and extremism in the 21st century. *Investigation of crimes: problems and ways to solve them*. 2018;3(21):60–71. (In Russ.)
2. Bychkov VV. Information and telecommunication networks as a means of committing crimes of extremist orientation. *Herald of the Moscow academy of the Investigative committee of the Russian Federation*. 2020;(3):43–46. (In Russ.)
3. Bychkov VV. Artificial intelligence: public policy and vectors of application. *Crime investigation: problems and ways to solve them*. 2020;(4):45–50. (In Russ.)
4. Bychkov VV, Prorvich VA. Artificial intelligence as a means of countering crimes of extremist orientation committed using information and telecommunications networks, including the Internet. *Herald of the Moscow academy of the Investigative committee of the Russian Federation*. 2020;(4):47–52. (In Russ.)
5. Bychkov VV, Prorvich VA. Artificial intelligence in the fight against crimes committed for extremist reasons, using the Internet. *Modern criminal procedure law — lessons of history and the problems of further reform*. 2020;(1):34–49. (In Russ.)
6. Fedotov NN. Forenzica is a computer forensics. Moscow: Legal World, 2007. 432 p.
7. Volynskij AF, Prorvich VA. Komp'yuternaya kriminalistika v sisteme ugolovno-pravovoj zashchity «tradicionnoj» i cifrovoj ekonomiki. Moscow: Ekonomika, 2020. 476 p. (In Russ.)
8. Volynskij AF, Prorvich VA. Elektronnoe sudoproizvodstvo po prestupleniyam v sfere ekonomiki (nauchno-prakticheskie aspekty). Moscow: Ekonomika, 2019. 364 p. (In Russ.)
9. Eriashvili ND. New level of development of problems of electronic justice on crimes in the economy. *Public service and personnel*. 2020;(1):181–184. (In Russ.)

ОБ АВТОРАХ

***Василий Васильевич Бычков,** кандидат юридических наук, доцент; e-mail: bychkov_vasilij@bk.ru

Владимир Антонович Прорвич, доктор юридических наук, доктор технических наук, профессор; e-mail: kse60@mail.ru

AUTHOR INFORMATION

***Vasily V. Bychkov,** candidate of law science, associate professor; e-mail: bychkov_vasilij@bk.ru

Vladimir A. Prorvich, doctor of law science, doctor of technical science, professor; e-mail: kse60@mail.ru