Научная статья
УДК 343.98
EDN ULOFWQ
DOI 10.17150/2500-4255.2023.17(3).254-262

ТИПОВАЯ СИТУАЦИОННО-ВЕРСИОННАЯ ХАРАКТЕРИСТИКА ПЕРВОНАЧАЛЬНОГО ЭТАПА РАССЛЕДОВАНИЯ НЕПРАВОМЕРНОГО ВОЗДЕЙСТВИЯ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ: УГОЛОВНО-ПРАВОВЫЕ И КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ

Д.А. Степаненко, Я.В. Гармышев
Байкальский государственный университет, г. Иркутск, Российская Федерация

Информация о статье

Дата поступления
24 мая 2023 г.

Дата принятия в печать
8 июля 2023 г.

Дата онлайн-размещения
18 июля 2023 г.

Ключевые слова

Информационная инфраструктура; следственная ситуация; квалификация; ответственность; первоначальный этап расследования; противодействие преступности

Аннотация. В настоящей статье рассмотрены вопросы обеспечения национальной безопасности с точки зрения современных тенденций цифровизации современного общества при использовании классического подхода в расследовании уголовных дел, связанных с неправомерным воздействием на критическую информационную инфраструктуру. С учетом ситуационного подхода, положений уголовного законодательства и теории квалификации преступлений определены особенности установления обстоятельств, входящих в предмет доказывания уголовных дел при неправомерном воздействии на критическую информационную инфраструктуру, что служит основой для построения общих и частных криминалистических версий, а также основной схемой для формирования планов в процессе предварительного следствия. Сделан вывод о необходимости и неизбежности использования совокупности официальных методик криминалистики и научных подходов к изучению преступной деятельности в сфере информационных систем для составления реальной картины. Делается акцент на непременности изучения и использования различных данных уголовно-правовых наук для современной следственной практики. Определены доминирующие черты первоначального этапа, позволяющие сформулировать его основные задачи. Характеристика задач этапа предопределила его главную функцию — поисково-познавательную деятельность следователей и взаимодействующих с ними субъектов расследования, использование специальных знаний, а также ведущую роль следственных, оперативно-розыскных версий, версий специалистов. Специфичность информации и ее поиск предопределяют доминирование в структуре расследования поисковых коммуникативных и экспериментальных следственных действий. Анализ особенностей производства процессуальных и иных действий на первоначальном этапе расследования позволил сделать заключение о важности использования в расследовании тактических комплексов. Определен комплекс криминалистических рекомендаций технического, тактического, методического характера для внедрения в практику расследования преступлений с целью оптимального решения вопросов противодействия преступлениям в сфере неправомерного воздействия на критическую информационную инфраструктуру.

Original article

TYPICAL SITUATIONAL-VERSION FEATURES OF THE INITIAL STAGE OF INVESTIGATING UNLAWFUL IMPACT ON CRITICAL INFORMATION INFRASTRUCTURE: CRIMINAL LAW AND CRIMINALISTIC ASPECTS

Diana A. Stepanenko, Yaroslav V. Garmyshev
Baikal State University, Irkutsk, the Russian Federation

Article info

Received
2023 May 24

Abstract. The authors examine the questions of ensuring national security on the basis of incorporating modern trends of the digitization of society into the classical approach when investigating criminal cases connected with unlawful impact on critical

ISSN 2500-1442

Accepted
2023 July 8
Available online
2023 July 18

Keywords

Information infrastructure; investigative situation; qualification; responsibility; initial stage of investigation; crime counteraction

information infrastructure. Using the situational approach, clauses of criminal legislation and the theory of crime qualification, the authors determine the circumstances included in the subject of proof for the criminal cases of unlawful influence on critical information infrastructure, which serves as a foundation for building general and specific criminalistic versions, and is also the basic scheme for making plans during the preliminary investigation. The authors conclude that, in order to obtain a realistic picture, it is necessary and unavoidable that an aggregate of official criminalistic techniques and scientific approaches should be used to study criminal activities in the sphere of information systems. They stress the necessity of studying and incorporating various data of criminal law research into modern investigative practice. The dominant features of the initial stage are identified, which make it possible to formulate its key tasks. The description of the tasks at this stage predetermines its key functions — the search and cognitive work of investigators and the subjects of investigation they interact with, the use of expert knowledge, the leading role of investigative, operative search versions and expert versions. The specific character of information and search for it predetermine the dominance of search, communicative and experimental investigative actions in the structure of the investigation. The analysis of the specific features of carrying out procedural and other actions at the initial stage of investigation allowed the authors to make conclusions about the importance of using tactical complexes in the investigation. They specify a complex of criminalistic recommendations of technical, tactical and methodological character to be implemented in the practice of crime investigation with the purpose of optimizing the counteraction to unlawful impact on critical information infrastructure.

Сегодня особенно остро стоит вопрос об обеспечении безопасности критической информационной инфраструктуры нашего государства. Об этом свидетельствует и изданный указ Президента РФ «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» от 30 марта 2022 г. № 166. В соответствии с ним правительству необходимо определить сроки и порядок перехода на использование доверенных программно-аппаратных комплексов, а также «обеспечить создание и организацию деятельности научно-производственного объединения, специализирующегося на разработке, производстве, технической поддержке и сервисном обслуживании доверенных программно-аппаратных комплексов для критической информационной инфраструктуры», создать системы мониторинга и контроля в указанной сфере и организацию подготовки и переподготовки соответствующих кадров.

От развитости и устойчивости критической инфраструктуры общества зависит его благополучие. Национальное благополучие становится одной из основных задач государства и предопределяет системную характеристику элементов объективных обстоятельств (социально-экономических, политических, экологических), обеспечивающих на высоком уровне условия жизни и субъективные показатели удовлетворенности ею [1–3].

Интересно, что в науке «сформировались два подхода, объясняющих становление и поддержание благополучия населения: объективистский, в рамках которого благополучие отождествляется с равновесием, обеспечивающим стабильное функционирование всех элементов и прогрессивное развитие всего общества, и субъективистский, акцентирующий внимание на необходимости изучения соотношения внешних и внутренних факторов и их взаимосвязей, влияющих на субъективное благополучие» [4; 5]. Сегодня мы прекрасно понимаем, что национальное благополучие во многом зависит от безопасности и устойчивости критической инфраструктуры [6].

Цифровая трансформация общества в современных условиях является неотъемлемым компонентом национального благополучия, и информационная безопасность всех сфер жизни и деятельности российского общества и государства имеет огромное значение. Так, например, «многие киберинциденты становятся возможными из-за отсутствия устойчивости и надежности инфраструктуры частных и общественных сетей, плохо защищенных баз данных и других недостатков в критической информационной инфраструктуре» [7–9].

Вице-премьер Д. Чернышенко в ходе рабочей встречи с президентом России В. Путиным заявил, что более 25 тыс. кибератак на государственные ресурсы и 1 200 инцидентов

на критической инфраструктуре было отражено в 2022 г.[1]

С момента вступления в действие статьи Уголовного кодекса РФ, предусматривающей ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации, прошло пять лет. На практике статья применяется нечасто и не во всех субъектах РФ, что обусловлено сложностью выявления и раскрытия данного преступления (так, с целью сокрытия следов преступления виновные лица устанавливают соответствующие компьютерные программы, которые уничтожают или искажают следы в информационных системах) и размытостью в разграничении со смежными составами (ст. 274, 159.6, 205 УК РФ) [10].

В системе характеристик уголовной ответственности необходимо отметить то обстоятельство, что при определении социально-правовой природы рассматриваемого деяния его законодательные элементы располагаются на системном взаимодействии отраслевого правового регулирования, благодаря чему и устанавливается взаимосвязь уголовно-правовых и иных отраслевых норм в сфере обеспечения стандартов правовой охраны информационной безопасности. Следовательно, создание эффективной системы уголовной политики в сфере охраны цифрового пространства «предопределяет включение определенных условий: 1) определение взаимосвязанного правового регулирования уголовного и иного отраслевого права в сфере реализации задачи охраны объекта преступления, определенного в ст. 274[1] УК РФ; 2) обеспечение эффективного взаимодействия уголовного и административного законодательства в области охраны киберпространства; 3) устранение выявленных собственных недостатков УК РФ в части норм, предусматривающих ответственность за преступление в информационной сфере» [11; 12].

Объектом преступления выступает безопасность критической информационной инфраструктуры (КИИ) Российской Федерации, дополнительным объектом — информационная безопасность в любой сфере деятельности государства и общества.

Предметом преступления является охраняемая компьютерная информация, содержащаяся в критической инфраструктуре Российской Федерации. В соответствии со ст. 2 (пп. 6–8) Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ (последняя редакция) под КИИ понимаются информационные системы, информационно-телекоммуникационные сети госорганов, автоматизированные системы управления технологическими процессами в различных областях развития общественных отношений в рамках их комплексного взаимодействия.

Субъектами КИИ являются «государственные органы и учреждения, российские юридические лица, индивидуальные предприниматели, которым принадлежат и или которые обеспечивают взаимодействие информационных систем (ИС), информационно-телекоммуникационных сетей (ИТКС), автоматизированных систем управления (АСУ), функционирующих в одной из следующих областей: здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности» [7, с. 102].

Субъектом же преступления признается вменяемое физическое лицо, которое достигло 16-летнего возраста. В криминалистическом аспекте виновное лицо обладает в сфере информационных технологий достаточными компетенциями, располагает необходимой информацией в данной сфере, имеет соответствующие компьютерные программы, в том числе вредоносные, предназначенные для неправомерного воздействия на КИИ РФ. На этапе правоприменения применительно к отдельным уголовным делам установлено относительно понятий субъекта и объекта КИИ их законодательное смешение, что создает неточности при разрешении дел. Так, к примеру, суд определил: «...Г., действуя умышленно, достоверно зная, что ПАО «Ростелеком» относится к объектам критической информационной инфраструктуры... осуществила неправомерный доступ к охраняемой компьютерной информации... в БД «Авалон» и хранящейся на защищенных сетевых ресурсах ПАО «Ростелеком»[2].

[1] Чернышенко сообщил о ликвидации 25 тыс. кибератак на госресурсы РФ за год. URL: https://iz.ru/1415002/2022-10-24/chernyshenko-soobshchil-o-likvidatcii-25-tys-kiberatak-na-gosresursy-rf-za-god.

[2] Приговор Ленинского районного суда г. Владивостока от 25 сентября 2019 г. по делу № 1-368/2019 // ГАС РФ «Правосудие».

Субъективная сторона основного состава характеризуется прямым умыслом, а в квалифицированных его признаках не исключается неосторожность: преступное бездействие при осуществлении защитных мер по комплексному обеспечению безопасности объекта КИИ, что повлекло причинение вреда объекту посягательства, где в результате преступной неосмотрительности или намеренного деяния могут быть нарушения штатного режима функционирования информационных систем, следовательно, в процессе расследования необходимо детально определить причины правонарушения.

Формируемые компоненты в процессе расследования уголовного дела в аспекте поисково-познавательной характеристики деятельности практического работника и конкретизация различных криминалистических рекомендаций различного характера (технического, методического и пр.) для внедрения в практику уголовного процесса с целью оптимального решения в системе противодействия преступности ее задач становятся насущной проблемой, требующей внимания и разрешения. И главенствующая роль в этом принадлежит криминалистической науке.

Исходя из ситуационного подхода, который в современной криминалистике занимает центральное место, прежде чем разрабатывать поисковой и познавательный инструментарий, создавать типичные программы действий лица, ведущего расследование, нужно сконцентрировать внимание на выявлении и анализе следственной ситуации, что гносеологически является необходимым условием эффективной организации его деятельности, основой для построения общих и частных криминалистических версий, а также основной схемой для формирования планов в процессе предварительного следствия.

Типичным способом является модификация информации в системе с помощью стороннего программного обеспечения, незаконного копирования баз данных клиентов, передача персональных данных третьим лицам, использование «служб микширования» [13]. Почти во всех случаях нарушителями были сотрудники компаний (работники субъектов КИИ). Анализ статистики позволяет сделать вывод о том, что уголовные дела прекращаются или в связи с деятельным раскаянием, добровольным возмещением ущерба, или вынесением приговора с двумя-тремя годами условно.

На стадии возбуждения уголовного дела из информации, содержащейся в материалах предварительной проверки, формируется следственная ситуация, определяющая направление расследования на первоначальном этапе. Следует учесть тот факт, что даже незначительное нарушение предопределяет основания для возбуждения уголовного дела. Анализируя основания для возбуждения уголовного дела по ст. 274.1 УК РФ и в дальнейшем определяя круг обстоятельств, подлежащих установлению, следователь должен иметь в виду, что по конструктивным элементам вышеуказанный состав признается материальным: свойственно определение объекту посягательства общественно опасных последствий, установленных уголовным законом. В процессе расследования уголовного дела, особенно в самом начале данного процесса, необходимо учитывать то, что в уголовном законе не конкретизированы пределы тяжести вреда объекту преступления, анализируемое обстоятельство предопределяется правоприменителем самостоятельно: показатели общественной опасности могут быть представлены в широком диапазоне, исследователь самостоятельно определяет порог размера малозначительности, т.е. размер вреда признак оценочный [7, с. 103]. Юридическое свойство рассматриваемого обстоятельства заключается в том, что его определение не всегда поддается критериям правовой формализации. Малозначительность может образовывать ситуация, когда утраченные данные будут неактуальными, нарушения были кратковременными. Показателями малозначительности деяния могут быть также и иные обстоятельства правонарушения.

В правоприменительной деятельности имеются следующие варианты понимания вреда: во-первых, им признавались сведения, составляющие «коммерческую тайну при копировании компьютерной информации; во-вторых, само по себе нарушение элементов информационной безопасности, закрепленный за соответствующим субъектом КИИ; в-третьих, как видоизменение конфигурации элементов различных цифровых систем, нарушение процесса предоставления услуг связи абонентам» [14, с. 31]. Вместе с тем следует учесть то, что судебная практика корректирует содержание отдельных понятий в уголовном законодательстве, однако не всегда разрешается соответствующая проблема их толкования. Определение критериев для оценки отдельных элементов состава, правовое закрепление ключевых признаков и следование установленным требованиям при квалифи-

кации преступлений с оценочными понятиями предопределяли бы более четкую и эффективную их реализацию, что отвечало бы интересам современного общества и обусловило большее уважение к закону со стороны граждан, а также эффективность правоприменения. Отсутствие рекомендаций по рассмотрению оценочных понятий неизбежно приводит к свободному их толкованию представителями судебной власти в контексте судебного усмотрения. Анализируемое право суда реализуется в границах, установленных законом, в соответствии с правосознанием соответствующего субъекта правоприменения и концепцией законодателя с соблюдением правовых принципов, основ морали, а также с учетом конкретных обстоятельств совершения преступления [15]. Для практических работников подобные оценочные понятия не способствуют прояснению сложной ситуации, а, наоборот, создают дополнительные трудности.

Юридический анализ правоприменительной деятельности по признакам ст. 274.1 УК РФ, где определены материальные характеристики преступных последствий, позволил установить, что единого комплексного понятия «тяжкие последствия» нет на практике в их товарно-денежном выражении. Правоприменителю в каждом уголовном деле, исходя из установленных признаков объективной стороны совершенного преступления, следует самостоятельно конкретизировать показатели преступных деяний, что часто представляется крайне сложной задачей, особенно с учетом динамики социально-экономических показателей товарных ценностей по стране и в отдельно взятом регионе (административном районе). Представляется необходимым обратить внимание на разницу между фактическим и юридическим смыслом законодательной терминологии. Фактически общественная опасность преступлений связывается со всем масштабом отрицательных последствий. Юридически же общественная опасность по общему правилу имеет количественную и качественную характеристики. Следовательно, «для уголовно-правовой оценки общественно опасного деяния имеет значение именно качественная характеристика общественной опасности совершенного преступления, через которую определяется объект преступления, качественная характеристика общественной опасности преступления заключается в создании, к примеру, угрозы причинения какого-либо существенного вреда в условиях опасной ситуации» [16].

Таким образом, определение вышеуказанных обстоятельств очень важно, так как перед следователем стоит задача найти обстоятельства, подлежащие установлению и соответствующие предмету доказывания.

Следственная ситуация — «положение в расследовании преступлений, характеризуемое наличием тех или иных доказательств, информационного материала и возникающими в связи с этим конкретными задачами его собирания и проверки» [17, с. 509]. Среди основных компонентов следственной ситуации в криминалистике традиционно выделяют информационные, психологические, процессуальные, тактические, материальные и организационно-технические [18, с. 94], главным из которых является информационный аспект [19, с. 580].

В случае принятия следователем решения о возбуждении уголовного дела представляется, что наиболее удачным является выделение типичных следственных ситуаций, основанных на обстоятельстве наличия данных о виновном лице:

– лицо, совершившее неправомерное воздействие на КИИ, известно;

– о лице, совершившем преступление, имеются отдельные и неполные сведения;

– информация о виновном лице отсутствует.

Данная классификация ориентирована на основную задачу всего расследования — изобличение преступника, совершившего предполагаемое преступление в виде неправомерного воздействия на КИИ РФ.

Кроме того, если учитывать специфику рассматриваемой категории преступлений, информационный фактор в виде наличия у следствия сведений о виновном субъекте будет играть свою роль при дальнейшем определении лицом, производящим расследование, своего тактического решения, плана действий, выведении следственных версий, выборе тактических операций.

В рамках расследования уголовного дела следователю при установлении причастности конкретного виновного лица и закреплении необходимых доказательств следует определить объективные характеристики преступного деяния (какими противоправными средствами воздействия произошла атака на объект преступления, идентифицировать необходимые компьютерные устройства и специальные программы и их владельцев, которыми осуществлялось воздействие на КИИ РФ), а также выявить иные материальные следы преступления.

Часть 3 ст. 274.1 УК РФ предусматривает специального субъекта преступления, имеющего доступ к объекту КИИ РФ, на которого возложены обязанности по соблюдению правил доступа или эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ, или ИС, ИТКС, АСУ, сетей электросвязи, относящихся к КИИ. Следует учитывать то, что к субъектам КИИ относятся юридические лица, которым принадлежат информационные системы, «в случае передачи ими КИИ на баланс аутсорсинговой компании, сделавшая это, например, какая-либо организация под характеристику субъекта КИИ не подходит, следовательно, ее сотрудников нельзя признать исполнителями преступления, предусмотренного ч. 3 ст. 274.1 УК РФ, однако если такая организация передала КИИ на аутсорсинг, но у нее остались компьютеры, через которые можно удаленно подключаться к КИИ, ее следует считать субъектом КИИ, а ее сотрудников — субъектами рассматриваемых преступлений, несмотря на то что непосредственно соответствующей КИИ она не владеет» [7; 14].

В отношении квалифицированного состава, предусмотренного ч. 3 ст. 274.1 УК РФ, дополнительно, кроме указанных ранее действий, следует определить должностных лиц, имеющих доступ к соответствующему цифровому устройству, сотрудника-пособника, с использованием устройства которого было осуществлено противоправное воздействие, и условия удаленного применения компьютерного устройства.

Обязательным признаком ч. 4 ст. 274.1 УК РФ является совершение преступления или группой лиц по предварительному сговору, или организованной группой, или лицом с использованием своего служебного положения. При расследовании преступлений, предусмотренных ч. 3 и 4 ст. 274.1 УК РФ, особое внимание необходимо уделять установлению и доказыванию служебного статуса субъекта. Для этого необходимы доказательства, указывающие на наличие у виновного лица возможности доступа к объекту посягательства, его должностные права и обязанности, возникающие при эксплуатации элементов цифровой среды различных компьютерных объектов.

На практике также может возникнуть проблема определения соучастия в рассматриваемом составе преступления и конкретизации роли каждого участника преступления. Не исключается возможность наличия только одного «фактического» исполнителя, а если используется несколько цифровых устройств при неправомерном воздействии на КИИ РФ, то необходимо устанавливать фактическую возможность управления устройствами из одного центра [20; 21].

Для первоначального этапа расследования характерны следующие типичные общие версии, основывающиеся на наличии преступления:

– заявление о неправомерном воздействии на КИИ подтверждается, преступление действительно имеет место;

– произошла ошибка пользователей объекта КИИ или сбои программного обеспечения, которые привели к срабатыванию систем информационной безопасности, неправомерного воздействия на КИИ не было.

В криминалистической литературе по методике расследования преступлений в сфере компьютерной информации, как правило, к общим версиям на первоначальном этапе относят версию о наличии ложного заявления о преступлении. В теории она может быть применима при расследовании неправомерного воздействия на КИИ. Но следует учесть специфику исследуемой категории преступлений, где предметом выступают объекты КИИ, принадлежащие специально определенным организациям — субъектам КИИ. Поэтому можно предположить, что ложное заявление о возникновении инцидента и неправомерного воздействия будет связано с наличием у сотрудников субъекта КИИ и (или) его руководителей личных мотивов и интересов, например с желанием скрыть какой-либо факт в деятельности или данные организации под видом уничтожения компьютерной информации в системе КИИ в результате заражения вредоносным программным обеспечением.

Частные же следственные версии выдвигаются в отношении личности виновного лица, мотивов совершения преступления, способов, которые использовались для неправомерного доступа воздействия на КИИ, и др.

Приведенная ранее первая типичная следственная ситуация является наиболее благоприятной для расследования исследуемой категории дел. Для данной ситуации характерно то, что задержание осуществляется следующими лицами: сотрудниками субъекта КИИ, гражданами, ставшими очевидцами правонарушения, сотрудниками правоохранительных органов, либо лицо явилось с повинной. Однако все же следует помнить, что виновность лица и противозаконный характер деяния носят предполо-

жительный характер, и окончательно признать лицо таковым вправе только судебный орган.

При выдвижении следственных версий и их проверке в первую очередь рассматриваются версии о способе внедрения в компьютерную систему и сети КИИ, об обстоятельствах, при которых было совершено преступление, о причиненном ущербе, об умысле и мотивах преступника.

При рассмотрении второй следственной ситуации, в которой имеются только отдельные сведения о виновном лице, первоначально выдвигается версия о его принадлежности к определенному кругу лиц, его личных качествах и профессиональных навыках, о возможных сообщниках преступника. По ходу расследования выдвинутая версия о совершении преступления представителем той или иной группы людей конкретизируется.

Наконец, при третьей ситуации, когда нет никаких сведений о лице, совершившем неправомерное воздействие на КИИ, можно предположить, что выбранный способ проникновения в систему и характер деяния давали возможность получения доступа к ней неопределенному кругу лиц.

Версии о личности виновного лица при этом могут быть следующие:

– деяние было совершено сотрудником субъекта КИИ;

– преступление совершено лицом, входящим в круг знакомых, родственников, друзей, сотрудников субъекта КИИ, обладающих авторизированным доступом к объектам КИИ;

– неправомерное воздействие на КИИ совершено посторонним третьим лицом или группой лиц.

Необходимо отметить, что существенное значение при подтверждении выдвинутых версий имеет факт наличия непротиворечивой совокупности доказательств, собранных процессуальными средствами, и, соответственно, в результате проверки их всех в конце должна остаться только одна версия, которая полностью подтвердилась.

Таким образом, от правильного анализа и оценки сложившейся следственной ситуации во многом зависит эффективное разрешение задач первоначального этапа расследования, а также разработка действенных способов и средств получения необходимой информации путем определения требуемых следственных действий и их последовательности, форм взаимодействия с сотрудниками оперативно-розыскных подразделений других правоохранительных органов.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Шободоева А.В. Стратегия национальной безопасности РФ и ее вклад в развитие понятийного аппарата общей теории национальной безопасности РФ / А.В. Шободоева. — DOI 10.17150/2411-6262.2016.7(1).17. — EDN VLIBNF // Baikal Research Journal. — 2016. — Т. 7, № 1.

2. Вишняков В.Г. О методологических основах правового регулирования проблем безопасности Российской Федерации / В.Г. Вишняков. — EDN OPCUJJ // Журнал российского права. — 2005. — № 9. — С. 27–39.

3. Босхолов С.С. Криминологическая безопасность как идейная основа теории и практики противодействия преступности / С.С. Босхолов. — DOI 10.17150/2411-6262.2021.12(3).30. — EDN WEAOIS // Baikal Research Journal. — 2021. — Т. 12, № 3.

4. Кисилева Л.С. Благополучие российского населения: архитектоника, субъективное восприятие и региональное своеобразие : дис. … д-ра социол. наук : 22.00.04 / Л.С. Кисилева. — Санкт-Петербург, 2020. — 361 с.

5. Киберпространство БРИКС: правовое измерение / И.И. Шувалов, Т.Я. Хабриева, Фэн Цзинжу [и др.] ; ред. Д. Руйпин, Т.Я. Хабриева. — Москва : Ин-т законодательства и сравнит. правоведения при Правительстве РФ, 2017. — 336 с. — EDN RXNGTT.

6. Seele P. Let us not forget: Crypto means secret. Cryptocurrencies as enabler of unethical and illegal business and the question of regulation / P. Seele. — DOI 10.1007/s41463-018-0038-x // Humanistic Management Journal. — 2018. — Vol. 3, № 1. — P. 133–139.

7. Трунцевский Ю.В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов / Ю.В. Трунцевский. — DOI 10.12737/art_2019_5_9. — EDN KRNLWX // Журнал российского права — 2019. — № 5. — С. 99–106.

8. Braaten N.C. Convenience theory of cryptocurrency crime: A content analysis of US federal court decisions / N.C. Braaten, M.S. Vaughn. — DOI 10.1080/01639625.2019.1706706 // Deviant Behavior. — 2021. — Vol. 42, № 8. — P. 958–978.

9. Wronka Ch. Financial crime in the decentralized finance ecosystem: new challenges for compliance / Ch. Wronka. — DOI 10.1108/JFC-09-2021-0218 // Journal of Financial Crime. — 2023. — Vol. 30, № 1. — P. 97–113.

10. Романовский В.Г. Перспективы криминализации кибертерроризма в России и за рубежом / В.Г. Романовский. — DOI 10.17150/1819-0928.2022.23(3).302-311. — EDN MEOJEX // Академический юридический журнал. — 2022. — Т. 23, № 3. — С. 302–311.

11. Савинский А.В. О некоторых неточностях Уголовного кодекса Российской Федерации / А.В. Савинский. — EDN CSSLLF // Сибирские уголовно-процессуальные и криминалистические чтения. — 2020. — № 1. — С. 99–105.

12. Гармышев Я.В. Правовая природа объекта уголовно-правовой охраны преступлений против общественной безопасности в уголовном законодательстве России / Я.В. Гармышев, В.В. Гармышев. — DOI 10.24412/2076-1503-2022-10-334-340. — EDN JNSIVT // Образование и право. — 2022. — № 10. — С. 334–440.

13. Money laundering in the bitcoin network: Perspective of mixing services / Ju. Seo, M. Park, H. Oh, K. Lee. — DOI 10.1109/ICTC.2018.8539548 // International Conference on Information and Communication Technology Convergence. — Jeju, Korea, 2018. — P. 1403–1405.

14. Русскевич Е.А. Квалификация неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации / Е.А. Русскевич, И.Г. Чекунов. — DOI 10.52390/20715870_2022_5_26. — EDN AGHWVK // Уголовное право. — 2022. — № 5 (141). — С. 26–35.

15. Гончаров Д.Ю. Официальные документы: проблемы квалификации по Уголовному кодексу РФ / Д.Ю. Гончаров // Право и экономика. — 2000. — № 12. — С. 43–44.

16. Гармышев Я.В. К вопросу о квалификации некоторых оценочных понятий в уголовном праве России / Я.В. Гармышев, И.М. Егерев, С.В. Пархоменко. — DOI 10.17150/2500-4255.2016.10(4).732-739. — EDN XQTRMR // Всероссийский криминологический журнал. — 2016. — Т. 10, № 4. — С. 732–739.

17. Колесниченко А.Н. Научные и правовые основы расследования отдельных видов преступлений : дис. ... д-ра юрид. наук : 12.00.00 / А.Н. Колесниченко. — Харьков, 1967. — 673 с.

18. Белкин Р.С. Криминалистика: проблемы, тенденции, перспективы. От теории к практике / Р.С. Белкин. — Москва : Юрид. лит., 1988. — 302 с.

19. Гавло В.К. Следственные ситуации как основа организации расследования преступлений / В.К. Гавло // Избранные труды. — Барнаул, 2011. — С. 578–585.

20. Leukfeldt E.R. Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime / E.R. Leukfeldt, A. Lavorgna, E.R. Kleemans. — DOI 10.1007/s10610-016-9332-z // European Journal on Criminal Policy and Research. — 2017. — Vol. 23, № 3. — P. 287–300.

21. Голубев Ф.А. Криминалистическая характеристика расследования неправомерного воздействия на критическую информационную структуру Российской Федерации / Ф.А. Голубев. — DOI 10.7256/2454-0706.2020.10.33985. — EDN JMDHIY // Право и политика. — 2020. — № 10. — С. 50–59.

REFERENCES

1. Shobodoyeva A.V. Strategy of RF National Security and its Contribution to Developing Conceptual Framework of General Theory RF National Security. *Baikal Research Journal*, 2016, vol. 7, no. 1. (In Russian). EDN: VLIBNF. DOI: 10.17150/2411-6262.2016.7(1).17.

2. Vishnyakov V.G. On the Methodological Grounds for the Legislative Regulation of the Questions of Security of the Russian Federation. *Zhurnal rossiiskogo prava = Russian Law Journal*, 2005, no. 9, pp. 27–39. (In Russian). EDN: OPCUJJ.

3. Boskholov S.S. Criminological Security as the Ideological Basis of the Theory and Practice of Counteracting Crime. *Baikal Research Journal,* 2021, vol. 12, no. 3. (In Russian). EDN: WEAOIS. DOI: 10.17150/2411-6262.2021.12(3).30.

4. Kisileva L.S. *Well-being of Russian People: Architectonics, Subjective Perception and Regional Specifics. Doct. Diss.* Saint Petersburg, 2020. 361 p.

5. Shuvalov I.I., Khabrieva T.Ya., Feng Jingru [et al.]; Ruiping D., Khabrieva T.Ya. (eds.). *Cyberspace BRICS: Legal Dimension.* Moscow, Institute of Legislation and Comparative Law under the Government of the Russian Federation Publ., 2017. 336 p. EDN: RXNGTT.

6. Seele P. Let us not Forget: Crypto Means Secret. Cryptocurrencies as Enabler of Unethical and Illegal Business and the Question of Regulation. *Humanistic Management Journal*, 2018, vol. 3, no. 1, pp. 133–139. DOI: 10.1007/s41463-018-0038-

7. Truntsevsky Yu.V. Unlawful Impact on Critical Information Infrastructure: the Criminal Liability of its Owners and Operators. *Zhurnal rossiiskogo prava = Russian Law Journal,* 2019, no. 5, pp. 99–106. (In Russian). EDN: KRNLWX. DOI: 10.12737/art_2019_5_9.

8. Braaten N.C., Vaughn M.S. Convenience Theory of Cryptocurrency Crime: A Content Analysis of US Federal Court Decisions. *Deviant Behavior*, 2021, vol. 42, no. 8, pp. 958–978. DOI: 10.1080/01639625.2019.1706706.

9. Wronka Ch. Financial Crime in the Decentralized Finance Ecosystem: New Challenges for Compliance. *Journal of Financial Crime*, 2023, vol. 30, no. 1, pp. 97–113. DOI: 10.1108/JFC-09-2021-0218.

10. Romanovsky V.G. Prospects for Criminalization of Cyberterrorism in Russia and Abroad. *Akademicheskii yuridicheskii zhurnal = Academic Law Journal,* 2022, vol. 23, no. 3, pp. 302–311. (In Russian). EDN: MEOJEX. DOI: 10.17150/1819-0928.2022.23(3).302-311.

11. Savinsky A.V. On Some Inaccuracies in the Criminal Code of Russia. *Sibirskie ugolovno-protsessual'nye i kriminalisticheskie chteniya = Siberian Criminal Process and Criminalistic Readings,* 2020, no. 1, pp. 99–105. (In Russian). EDN: CSSLLF.

12. Garmyshev Ya.V., Garmyshev V.V. The Legal Nature of the Object of Criminal Protection of Crimes against Public Safety in the Criminal Legislation of Russia. *Obrazovanie i pravo = Education and Law,* 2022, no. 10, pp. 334–440. (In Russian). EDN: JNSIVT. DOI: 10.24412/2076-1503-2022-10-334-340.

13. Seo Ju., Park M., Oh H., Lee K. Money Laundering in the Bitcoin Network: Perspective of Mixing Services. *International Conference on Information and Communication Technology Convergenc*e. Jeju, Korea, 2018, pp. 1403–1405. DOI: 10.1109/ICTC.2018.8539548.

14. Russkevich E.A., Chekunov I.G. Qualification of Wrongful Influence on the Critical Information Infrastructure of the Russian Federation. *Ugolovnoe pravo = Criminal Law,* 2022, no. 5, pp. 26–35. (In Russian). EDN: AGHWVK. DOI: 10.52390/20715870_2022_5_26.

15. Goncharov D.Yu. Official Documentation: Issue of Qualification According to the Criminal Code of the RF. *Pravo i ekonomika = Law and Economics*, 2000, no. 12, pp. 43–44. (In Russian).

16. Garmyshev Ya.V., Egerev I.M., Parhomenko S.V. To the Issue of Classifying Some Evaluative Concepts in Russian Criminal Law. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2016, vol. 10, no. 4, pp. 732–739. (In Russian). EDN: XQTRMR. DOI: 10.17150/2500-4255.2016.10(4).732-739.

17. Kolesnichenko A.N. *Scientific and Legal Basis for the Investigation of Certain Types of Crimes. Doct. Diss*. Kharkov, 1967. 673 p.

18. Belkin R.S. *Criminalistics: Problems, Trends, Prospects. From Theory to Practice*. Moscow, Yuridicheskaya Literatura Publ., 1988. 302 p.

19. Gavlo V.K. Investigative Situations as a Basis for Organizing Crime Investigation. *Selected Works*. Barnaul, 2011, pp. 578–585. (In Russian).

20. Leukfeldt E.R., Lavorgna A., Kleemans E.R. Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research*, 2017, vol. 23, no. 3, pp. 287–300. DOI: 10.1007/s10610-016-9332-z.

21. Golubev F.A. Criminalistic Characteristic of Investigation of Undue Influence Upon Critical Information Structure of the Russian Federation. *Pravo i politika = Law and Politics,* 2020, no. 10, pp. 50–59. (In Russian). EDN: JMDHIY. DOI: 10.7256/2454-0706.2020.10.33985.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Степаненко Диана Аркадьевна — профессор кафедры криминалистики, судебных экспертиз и юридической психологии Института юстиции Байкальского государственного университета, доктор юридических наук, профессор, г. Иркутск, Российская Федерация; e-mail: diana-stepanenko@mail.ru.

Гармышев Ярослав Владимирович — доцент кафедры уголовного права и криминологии Института юстиции Байкальского государственного университета, кандидат юридических наук, доцент, г. Иркутск, Российская Федерация; e-mail: garmyv@mail.ru.

INFORMATION ABOUT THE AUTHORS

Stepanenko, Diana A. — Professor, Chair of Criminalistics, Forensic Expertise and Legal Psychology, Institute of Justice, Baikal State University, Doctor of Law, Professor, Irkutsk, the Russian Federation; e-mail: diana-stepanenko@mail.ru.

Garmyshev, Yaroslav V. — Ass. Professor, Chair of Criminal Law and Criminology, Institute of Justice, Baikal State University, Ph.D. in Law, Ass. Professor, Irkutsk, the Russian Federation; e-mail: garmyv@mail.ru.

ДЛЯ ЦИТИРОВАНИЯ

Степаненко Д.А. Типовая ситуационно-версионная характеристика первоначального этапа расследования неправомерного воздействия на критическую информационную инфраструктуру: уголовно-правовые и криминалистические аспекты / Д.А. Степаненко, Я.В. Гармышев. — DOI 10.17150/2500-4255.2023.17(3).254-262. — EDN ULOFWQ // Всероссийский криминологический журнал. — 2023. — Т. 17, № 3. — С. 254–262.

FOR CITATION

Stepanenko D.A., Garmyshev Ya.V. Typical Situational-version Features of the Initial Stage of Investigating Unlawful Impact on Critical Information Infrastructure: Criminal Law and Criminalistic Aspects. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2023, vol. 17, no. 3, pp. 254–262. (In Russian). EDN: ULOFWQ. DOI: 10.17150/2500-4255.2023.17(3).254-262.