Научная статья
УДК 343.37
DOI: 10.37973/KUI.2022.10.11.011

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА НЕПРАВОМЕРНОЕ ВОЗДЕЙСТВИЕ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ РОССИЙСКОЙ ФЕДЕРАЦИИ

Марина Александровна Ефремова,
Казанский филиал Российского государственного университета правосудия,
Казань, Россия, crimlaw16@gmail.com

Аннотация

Введение: статья посвящена проблемам уголовно-правовой охраны критической информационной инфраструктуры Российской Федерации. С 1 января 2018 г. вступила в силу ст. 274[1] Уголовного кодекса Российской Федерации (УК РФ), которая устанавливает уголовную ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. В это же время вступил в силу Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Проблема реализации положений данных законодательных актов является недостаточно исследованной и все еще нуждается в теоретическом осмыслении.

Материалы и методы: методологическую основу исследования составила совокупность философских, общенаучных и частнонаучных методов научного познания: анализ и синтез, индукция и дедукция, формально-логический и структурно-функциональный методы. В качестве материалов исследования выступили нормы уголовного законодательства, нормы иных отраслей права, материалы судебно-следственной практики, а также труды отечественных ученых, посвященные проблемам уголовной ответственности за неправомерное воздействие на объекты критической информационной инфраструктуры.

Результаты исследования: в статье рассматриваются объективные и субъективные признаки неправомерного воздействия на критическую информационную инфраструктуру. Автор приходит к выводу, что ст. 274[1] УК РФ не лишена ряда серьезных недостатков, которые порождают ряд проблем при ее правоприменении. Обозначенные в статье дефекты законодательной техники нуждаются в исправлении.

Обсуждение и заключение: обосновывается, что неопределенность нормативных предписаний, закрепленных в ст. 274[1] УК РФ, снижает эффективность ее применения.

Ключевые слова: информация; безопасность; информационная безопасность; уголовное право; информационное право; критически важная информационная инфраструктура; объекты критически важной информационной инфраструктуры; борьба с преступностью; отрасль права; уголовный кодекс; информационное общество; преступления против общественной безопасности; криминализация; киберпреступность; кибертерроризм

Для цитирования: Ефремова М.А. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Вестник Казанского юридического института МВД России. 2022. Т. 13. № 4 (50). С. 86 – 92. DOI: 10.37973/KUI.2022.10.11.011

Scientific article
UDC 343.37
DOI: 10.37973/KUI.2022.10.11.011

CRIMINAL LIABILITY FOR UNLAWFUL IMPACT ON THE CRITICAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION

Marina Aleksandrovna Efremova,
Kazan Branch of the Russian State University of Justice, Kazan, Russia,
crimlaw16@gmail.com

Abstract

Introduction: the article is devoted to criminal protection of the critical information infrastructure of the Russian Federation. On January 1, 2018, Article 274[1] of the Criminal Code of the Russian Federation entered into force. This establishes criminal liability for unlawful influence on the critical information infrastructure of the Russian Federation. At the same time, Federal Law No. 187-FZ dated 26.07.2017 "On the Security of the Critical Information Infrastructure of the Russian Federation" began its operation. The challenge of implementation the provisions of these legislative acts is insufficiently researched and still needs theoretical understanding.

Materials and Methods: the author used philosophical, general scientific and specific scientific methods of scientific cognition: analysis and synthesis, induction and deduction, logical and structural-functional methods. The research materials were the norms of criminal legislation, norms of other branches of law, materials of judicial and investigative practice, as well as the works of domestic scientists devoted to the issues of criminal liability for unlawful impact on critical information infrastructure objects.

Results: the article examined objective and subjective signs of undue influence on the critical information infrastructure. The author came to the conclusion that Article 274[1] of the Criminal Code of the Russian Federation has serious flaws that are rise to a number of enforcement challenges. The defects of legislative technique outlined in the article need to be corrected.

Discussion and Conclusions: it is substantiated that the uncertainty of the regulatory requirements enshrined in Article 274[1] of the Criminal Code of the Russian Federation reduces the effectiveness of its application.

Keywords: information; security; information security; criminal law; information law; critical information infrastructure; objects of critical information infrastructure; fight against crime; branch of law; criminal code; information society; crimes against public security; criminalization; cybercrime; cyberterrorism

For citation: Efremova M.A. Criminal Liability for Unlawful Impact on the Critical Information Infrastructure of the Russian Federation // Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2022. Vol. 13. № 4 (50). P. 86 – 92. DOI: 10.37973/KUI.2022.10.11.011

Введение

В условиях перехода к цифровой экономике существенное влияние на развитие различных отраслей отказывают информационные технологии. Их внедрение позволяет минимизировать затраты при производстве, одновременно увеличив его объем. Вместе с тем большинство таких технологий, внедренных в отрасли российской экономики, основано на зарубежных разработках, что позволяет говорить об их уязвимости. Особую обеспокоенность вызывает их использование на объектах критической информационной инфраструктуры (далее по тексту – КИИ). В целях обеспечения устойчивого функционирования КИИ законодателем был предпринят целый ряд мер.

Для обеспечения устойчивого функционирования КИИ и противодействия компьютерным атакам в отношении нее 26.07.2017 был принят Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[1]. Закон раскрывает понятие КИИ и определяет ее как «объекты КИИ, а также сетей электросвязи, используемые для организации взаимодействия таких объектов». Таким образом, законодательно КИИ определяется через объекты: «информационные систе-

1 О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 № 187-ФЗ // Российская газета. 2017. 31 июля.

мы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ». Подобные объекты активно используются в различных сферах: здравоохранении, науке, транспорте, связи, кредитно-финансовой сфере, области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности. Особая значимость объектов КИИ заключается в том, что в случае нарушения их устойчивого и бесперебойного функционирования могут наступить тяжкие последствия. Как отмечается в пояснительной записке к законопроекту «О безопасности критической информационной инфраструктуры Российской Федерации»[1], компьютерная атака способна полностью парализовать КИИ государства и вызвать социальную, финансовую и (или) экологическую катастрофу.

Для противодействия таким противоправным деяниям Федеральным законом от 26.07.2017 № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»[2] Уголовный кодекс Российской Федерации был дополнен ст. 274[1] «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации». Анализируемая статья была включена в главу 28 «Преступления в сфере компьютерной информации» раздела IX «Преступления против общественной безопасности и общественного порядка».

Несмотря на то, что с момента включения в УК РФ ст. 274[1] прошло уже несколько лет и начала формироваться судебная практика, ее применение вызывает некоторые сложности, а соответствующие разъяснения Верховного Суда Российской Федерации пока отсутствуют. Указанные обстоятельства и обусловили выбор тематики исследования.

Обзор литературы

Исследованием проблем уголовной ответственности за неправомерное воздействие на КИИ занимались И.Р. Бегишев, И.И. Бикеев, С.Д. Бражник, Р.И. Дремлюга, К.Н. Евдокимов, Е.А. Русскевич, Ю.В. Трунцевский, И.Г. Чекунов. Ученые солидарны во мнении, что законодательная конструкция ст. 274[1] имеет ряд существенных недостатков.

Материалы и методы

Методологическую основу исследования составила совокупность философских, общенаучных и частнонаучных методов научного познания: анализ и синтез, индукция и дедукция, формально-логический и структурно-функциональный методы. Выбор приведенной методологической базы позволил всесторонне изучить вопросы, относящиеся к предмету исследования и сформулировать авторские выводы и предложения. В качестве материалов исследования выступили нормы уголовного законодательства, нормы иных отраслей права, материалы судебно-следственной практики, а также труды отечественных ученых, посвященные проблемам уголовной ответственности за неправомерное воздействие на КИИ.

Результаты исследования

Конструкция ст. 274[1] УК РФ имеет сложную структуру, так как объединяет «несколько составов преступлений, уже известных уголовному закону», зачастую такой прием законодательной техники присущ «способу описания квалифицирующих признаков, но не самостоятельной норме» [1, с. 157]. В статье предусмотрена уголовная ответственность за три противоправные формы посягательства на объекты КИИ: неправомерный доступ; создание и распространение вредоносного программного обеспечения; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации. Как отмечает Е.А. Русскевич, такой подход к конструированию ст. 274[1] УК РФ «противоречит отечественным традициям криминализации и использования юридической техники при описании уголовно-правовых норм» [2, с. 139].

Если непосредственным объектом преступлений, предусмотренных ст. 272-274 УК РФ, являются общественные отношения по поводу обеспечения целостности и сохранности компьютерной информации, а также безопасного функционирования и использования информационных технологий, то непосредственный объект анализируемого преступления будет иным. В связи с тем, что объекты КИИ функционируют в различных сферах, в научной литературе высказываются различные подходы к определению непосредственного объекта данного посягательства. В частности, К.Н. Евдокимов под таковым понимает «охраняемые законом права и интересы собственников (владельцев) компьютерной

[1] Пояснительная записка к законопроекту «О безопасности критической информационной инфраструктуры Российской Федерации». URL: http://sozd.parlament.gov.ru/bill/47571-7 (дата обращения 21.10.2022).

[2] О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 № 194-ФЗ // Российская газета. 2017. 31 июля.

информации» в сфере ее безопасного обращения, а также безопасного функционирования соответствующих технических устройств, относящихся к КИИ РФ [3, с. 306-307]. По мнению Р.И. Дремлюги, объектом преступления, предусмотренного ст. 274[1] УК РФ, являются «общественные отношения в сфере цифровой экономики и информационного общества по поводу безопасности объектов информационной инфраструктуры, имеющих критическое значение» [4, с. 136]. Представляется, что объектом анализируемого преступления выступают отношения, обеспечивающие безопасность КИИ как совокупности объектов, имеющих особую значимость. Такое понимание объекта данного преступления вытекает из положений Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», где предусмотрено категорирование объектов КИИ в зависимости от их значимости и определен порядок их учета. Хотя и значимость того или иного объекта КИИ не указана в ст. 274[1] УК РФ в качестве квалифицирующего признака, она может быть учтена при оценке последствий, причиненных преступлением.

Предметом рассматриваемого преступления могут выступать как компьютерная информация, содержащаяся в КИИ, так и средства хранения, обработки или передачи такой информации, информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, сети электросвязи, если они отнесены к КИИ РФ.

Ч. 1 ст. 274[1] УК РФ предусматривает ответственность за создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на КИИ РФ. Указание законодателя на заведомое предназначение таких программ порождает вопрос о квалификации использования уже существующей вредоносной программы, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации при воздействии на КИИ. Законодатель не уточняет, в чем заключается принципиальное отличие таких программ. Однако, как свидетельствует анализ немногочисленной судебной практики, виновные используют вредоносное программное обеспечение, которое создано для иных неправомерных целей, но используют его для воздействия на объекты КИИ. Так как состав по конструкции формальный, то преступление следует считать оконченным с момента создания, распространения и (или) использования таких программ, независимо от наступивших последствий.

Ч. 2. ст. 274[1] УК РФ предусматривает ответственность за неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ РФ, если это деяние повлекло наступление последствий в виде причинения вреда. Таким образом, состав сконструирован как материальный. Ю.В. Трунцевский справедливо замечает, что отсутствие указание на размер тяжести причиненного вреда позволяет судам трактовать его довольно широко [5, с. 103]. Как указал Верховный Суд Российской Федерации в официальном отзыве на проект Федерального закона «О внесении изменений в законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 15.05.2015 № 3-ВС-2996/15[1], вызывает некоторые опасения, что в диспозиции для определения общественно опасных последствий используются признаки только субъектно-оценочного характера. Результаты изучения материалов судебной практики дают основание утверждать, что такие опасения не напрасны. Иногда суды и вовсе игнорируют упоминание характера причиненного вреда, ограничиваясь в приговоре лишь общими формулировками. Такая широкая трактовка вреда позволяет любой акт неправомерного доступа к информации, содержащийся в КИИ, рассматривать как противоправный. Представляется, что применительно к анализируемой норме необходимо вести речь о вреде материальном, так как причинение критической информационной инфраструктуре вреда физического должно квалифицироваться по нормам главы 21 УК РФ «Преступления против собственности».

С субъективной стороны преступление, предусмотренное ч. 1 ст. 274[1] УК РФ, характеризуется только прямым умыслом, а субъективную сторону преступления, предусмотренного ч. 2 ст. 274[1] УК РФ, может составлять не только прямой, но и косвенный умысел.

Субъект данных преступлений – общий, то есть вменяемое физическое лицо, достигшее возраста 16 лет.

[1] Официальный отзыв Верховного Суда Российской Федерации на проект Федерального закона «О внесении изменений в законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 15.05.2015 № 3-ВС-2996/15. Доступ из СПС «КонсультантПлюс» (дата обращения 21.10.2022).

В ч. 3 ст. 274[1] УК РФ предусмотрена ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в ней, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к КИИ РФ, если таковое повлекло причинение вреда КИИ РФ. В Федеральном законе от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» данные правила не содержатся. Вместо этого законодатель использует термин «требования по обеспечению безопасности значимых объектов КИИ», полномочия по установлению которых возложены на Федеральную службу по техническому и экспортному контролю (ФСТЭК). Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»[1] определяет требования и к организационно-распорядительным документам по безопасности значимых объектов. Эти документы должны содержать: цели и задачи обеспечения безопасности значимых объектов КИИ, перечень основных организационно-технических мероприятий, сведения о системе безопасности, а также правила работы работников субъекта КИИ на значимых объектах КИИ, действия работников субъекта КИИ при возникновении компьютерных инцидентов и иных нештатных ситуаций. Организационно-распорядительные документы по безопасности значимых объектов утверждаются руководителем субъекта КИИ и доводятся до сведения соответствующих работников.

Таким образом, в Федеральном законе говорится об «обязанности соблюдать требования», а уголовная ответственность устанавливается за «нарушение правил», которые устанавливаются субъектом КИИ с учетом особенностей его деятельности. Следовательно, каждый субъект КИИ разработает такой документ, который может существенно отличатся от аналогичного документа другого субъекта КИИ по целому ряду оснований, например, из-за того, что в одном случае субъектом КИИ выступает государственный орган, а в другом – индивидуальный предприниматель. Правоприменителю каждый раз необходимо обращаться к такому документу, чтобы установить правовые основания по соблюдению этих правил у конкретного лица.

Дискуссионным в настоящее время является вопрос относительно субъективных признаков преступления, предусмотренного ч. 3 ст. 274[1] УК РФ. Так, характеризуя субъективную сторону данного преступления, Ю.В. Трунцевский отмечает, что она может быть выражена как форме умысла, так и неосторожности [5, с. 105]. Схожую позицию занимает и Р.И. Дремлюга [4, с. 143]. По мнению Р.Р. Гайфутдинова, использование признака «нарушение правил» присуще для законодательного описания деяний с неосторожной формой вины [6, с. 124], следовательно, субъективная сторона деяния, ответственность за которое предусмотрена ч. 3. ст. 274[1] УК РФ, может характеризоваться исключительно неосторожной формой вины. Действительно, конструкция состава анализируемого преступления предполагает неосторожную форму вины, поэтому законодателю следовало бы указать форму вины непосредственно в диспозиции. Дискуссия относительно формы вины во многом обусловила споры об определении субъекта данного преступления. Есть мнение, что он может быть как общим, так и специальным [2, с. 143]. Р.Р. Гайфутдинов полагает, что субъект преступления, предусмотренного ч. 3 ст. 274[1] УК РФ, только специальный – «лицо, обладающее знаниями определенных правил эксплуатации и правил доступа» [6, с. 129]. Соглашаясь с приведенной позицией, отметим, что лицо не просто должно обладать соответствующими знаниями, на него должна быть возложена обязанность по соблюдению таких правил.

К числу квалифицирующих признаков неправомерного воздействия на КИИ законодатель относит совершение преступления группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения (ч. 4 ст. 274[1] УК РФ), наступление тяжких последствий (ч. 5 ст. 274[1] УК РФ).

Как мы уже отмечали ранее, эти последствия могут наступить в любой сфере, так как и сами объекты КИИ делятся на категории, исходя из их значимости для той или иной сферы. В пояснительной записке к законопроекту «О безопасности критической информационной инфраструктуры Российской Федерации» отмечается, что эти последствия могут быть «катастрофическими». С учетом того что КИИ

[1] Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования: приказ ФСТЭК России от 21.12.2017 № 235. Доступ из СПС «КонсультантПлюс» (дата обращения 21.10.2022).

является связующим звеном между другими секторами национальной инфраструктуры, причинение вреда ей нанесет ущерб и этим секторам. Таким образом, тяжкие последствия могут выражаться в выходе из строя объектов жизнеобеспечения, объектов оборонного комплекса, что, в свою очередь, может вызвать причинение существенного имущественного ущерба, массовую гибель людей.

До включения в УК РФ ст. 274[1] в специальной литературе отмечалось, что при совершении преступления в сфере компьютерной информации, посягающего на безопасность КИИ страны, действия злоумышленника должны квалифицироваться по совокупности с террористическим актом [7, с. 82]. По мнению И.Р. Бегишева, атаки на критически важные объекты информационной инфраструктуры Российской Федерации являются проявлением кибертерроризма [8, с. 9]. Следует поддержать Е.А. Русскевича и И.Г. Чекунова в том, что неправомерное воздействие на информационные ресурсы объектов транспорта, оборонной, атомной, ракетно-космической, химической промышленности и др. в зависимости от обстоятельств дела должно быть дополнительно квалифицировано по ст. 205, 281, 275 и другим статьям УК РФ [9, с. 34].

Обсуждение и заключение

Подводя итоги исследованию, следует отметить, что ст. 274[1] УК РФ является специальной по отношению к ст. 272-274 УК РФ. Представляется, что дифференцировать ответственность за посягательства в отношении объектов КИИ можно было бы и в рамках этих статей путем включения в них соответствующих квалифицирующих признаков. Однако законодатель пошел по иному пути. Проведенный анализ позволил нам выявить ряд упущений законодателя при конструировании ст. 274[1] УК РФ, которые могут привести к ошибкам в правоприменительной деятельности. Полагаем, что законодателю следовало бы провести «работу над ошибками» для их устранения.

СПИСОК ИСТОЧНИКОВ

1. Комаров А.А. Отдельное мнение относительно законопроекта «О внесении изменений в Уголовный кодекс Российской Федерации и в Уголовно-процессуальный кодекс Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» // Вестник Северо-Кавказского гуманитарного института. 2017. № 3. С. 155-156.

2. Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения. Москва: ИНФРА-М, 2019. 300 с.

3. Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: дис. … д-ра юрид. наук: 12.00.08. Москва, 2021. 557 с.

4. Дремлюга Р.И. Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: доктрина, закон, правоприменение. Москва: Юрилитинформ, 2022. 328 с.

5. Трунцевский Ю.В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. 2019. № 5. С. 99-106.

6. Гайфутдинов Р.Р. Квалификация преступлений против безопасности компьютерной информации. Москва: Юрлитинформ, 2019. 200 с.

7. Противодействие киберпреступности в аспекте обеспечения национальной безопасности: монография / [П.В. Агапов и др.]; Акад. Ген. прокуратуры Рос. Федерации. Москва, 2014. 136 с.

8. Бегишев И.Р. Проблемы противодействия преступным посягательствам на информационные системы критически важных и потенциально опасных объектов // Информационная безопасность регионов. 2010. № 1. С. 9-13.

9. Русскевич Е.А., Чекунов И.Г. Квалификация неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации // Уголовное право. 2022. № 5. С. 26-35.

REFERENCES

1. Komarov A.A. Otdel'noe mnenie otnositel'no zakonoproekta «O vnesenii izmenenij v Ugolovnyj kodeks Rossijskoj Federacii i v Ugolovno-processual'nyj kodeks Rossijskoj Federacii v svyazi s prinyatiem Federal'nogo zakona «O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii» // Vestnik Severo-Kavkazskogo gumanitarnogo instituta. 2017. № 3. S. 155-156.

2. Russkevich E.A. Ugolovnoe pravo i «cifrovaya prestupnost'»: problemy i resheniya. Moskva: INFRA-M, 2019. 300 s.

3. Evdokimov K.N. Protivodejstvie komp'yuternoj prestupnosti: teoriya, zakonodatel'stvo, praktika: dis. … d-ra yurid. nauk: 12.00.08. Moskva, 2021. 557 s.
4. Dremlyuga R.I. Ugolovno-pravovaya ohrana cifrovoj ekonomiki i informacionnogo obshchestva ot kiberprestupnyh posyagatel'stv: doktrina, zakon, pravoprimenenie. Moskva: YUrilitinform, 2022. 328 s.
5. Truncevskij YU.V. Nepravomernoe vozdejstvie na kriticheskuyu informacionnuyu infrastrukturu: ugolovnaya otvetstvennost' ee vladel'cev i ekspluatantov // ZHurnal rossijskogo prava. 2019. № 5. C. 99-106.
6. Gajfutdinov R.R. Kvalifikaciya prestuplenij protiv bezopasnosti komp'yuternoj informacii. Moskva: YUrlitinform, 2019. 200 s.
7. Protivodejstvie kiberprestupnosti v aspekte obespecheniya nacional'noj bezopasnosti: monografiya / [P.V. Agapov i dr.]; Akad. Gen. prokuratury Ros. Federacii. Moskva, 2014. 136 s.
8. Begishev I.R. Problemy protivodejstviya prestupnym posyagatel'stvam na informacionnye sistemy kriticheski vazhnyh i potencial'no opasnyh ob"ektov // Informacionnaya bezopasnost' regionov. 2010. № 1. S. 9-13.
9. Russkevich E.A., CHekunov I.G. Kvalifikaciya nepravomernogo vozdejstviya na kriticheskuyu informacionnuyu infrastrukturu Rossijskoj Federacii // Ugolovnoe pravo. 2022. № 5. S. 26-35.

Информация об авторе:
Ефремова Марина Александровна, доктор юридических наук, доцент, профессор кафедры уголовно-правовых дисциплин Казанского филиала Российского государственного университета правосудия, crimlaw16@gmail.com

Автор прочитал и одобрил окончательный вариант рукописи.

Information about the author:
Efremova Marina A., Doctor of Law, Associate Professor, Professor of the Department of Criminal Law Disciplines Kazan Branch of the Russian State University of Justice, crimlaw16@gmail.com

The author has read and approved the final version of the manuscript.

Статья получена: 15.09.2022.
Статья принята к публикации: 21.12.2022.
Статья опубликована онлайн: 26.12.2022.

Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаю.