УДК 343.34
ББК 67.410.204(2Рос)

DOI: 10.25683/VOLBI.2020.51.263

Ryvkin Stanislav Yuryevich,
Candidate of Law,
Associate Professor of the Department
of Criminal Procedure and Criminalistics,
Volgograd Institute of management of RANEPA,
Russian Federation, Volgograd,
e-mail: ryvkin_stanislav@mail.ru

Рывкин Станислав Юрьевич,
канд. юрид. наук,
доцент кафедры уголовного процесса
и криминалистики,
Волгоградский институт управления — филиал РАНХиГС,
Российская Федерация, г. Волгоград,
e-mail: ryvkin_stanislav@mail.ru

Huseynov Tofik Azerovich,
3rd year student of the Department of Law,
Law Enforcement,
bachelor's program,
Volgograd Institute of management of RANEPA,
Russian Federation, Volgograd
e-mail: ta_guseynov@mail.ru

Гусейнов Тофик Азерович,
студент 3-го курса юридического факультета
по направлению подготовки
«Правоприменительная деятельность», бакалавриат,
Волгоградский институт управления — филиал РАНХиГС,
Российская Федерация, г. Волгоград
e-mail: ta_guseynov@mail.ru

КИБЕРЦИФРОВОЕ ОРУЖИЕ КАК ЭЛЕМЕНТ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ КИБЕРПРЕСТУПЛЕНИЙ

INFORMATION WEAPONS AS AN ELEMENT OF CRIMINALISTIC CHARACTERISTICS OF CYBERCRIMES

12.00.12 — Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность
12.00.12 — Criminalistics; forensic expertise; operational and investigative activities

Научная статья носит самостоятельный и творческий характер, цели и задачи которой достигнуты. Продолжая исследования по теме «Доктринальные положения процессуальных, поисково-познавательных, тактических действий при расследовании преступлений, повлекших гибель военнослужащих, через призму практических инноваций военно-прикладной криминалистики» (Рывкин С.Ю.), авторы отмечают и анализируют особенности расследования киберпреступлений, в том числе в вооруженных формированиях. Исследуется киберцифровое оружие как элемент криминалистической характеристики кибернетических преступлений. Рассматриваются концепции и сущностные структуры киберцифрового оружия, возможности внесения дополнений в нормативные основы при расследовании кибератак, исследуется зарубежный опыт расследования кибернетических преступлений. В статье отмечается, что Президент РФ Путин В. В. нацеливает на разработку предупреждения и ослабление использования кибернетических средств в целях защиты интересов отечества, на необходимость противодействия информационному оружию. В статье приводится мнение начальника психологической службы Вооруженных сил РФ В. В. Барабанщиковой о том, что новыми вызовами для Вооруженных сил Российской Федерации являются: гибридные войны, кибератаки, международные террористические организации. Авторы разделяют взгляды специалиста по кибербезопасности Сергея Гордейчика о возможности дестабилизировать объекты инфраструктуры, управляемые автоматизированно, посредством кибернетических атак. В исследовании делается вывод о том, что информационное оружие следует рассматривать как в узком — орудия и средства совершения кибернетических преступлений, так и в широком смысле — система криминалистически значимых информационно-технологических комплексов и средств, применяемых в преступлениях, совершаемых с использованием высоких технологий. Авторы выделяют, что информационное оружие обладает следующими признаками: скрытностью, наступательностью, индивидуальной избирательностью к программному обеспечению, существует в кибернетической среде, распространяет свое действие посредством информационно-технологических сетей. Типы информационного оружия: пассивного и активного действия. Комплекс поисково-познавательных действий при расследовании кибернетических преступлений включает осмотр места происшествия, предметов, документов, изъятие электронных носителей информации и копирование с них информации.

The scientific article has an independent and creative character, the goals and objectives of which are achieved. Continuing research on the topic "Doctrinal provisions of procedural, search and cognitive, tactical actions in the investigation of crimes that caused the death of military personnel through the prism of practical innovations in military-applied criminalistics,, (Ryvkin S. Yu.), the features of investigating cybercrimes, including in armed formations, are noted and analyzed. The article examines information weapons as an element of criminalistic characteristics of cybernetic crimes. The concepts and essential structures of cyber digital weapons, the possibility of making additions to the regulatory framework for the investigation of cyber attacks, and foreign experience in the investigation of cybernetic crimes are considered. The article notes that the President of the Russian Federation Putin V. V. aims to develop prevention and reduce the use of cybernetic tools to protect the interests of the Fatherland, and the need to counter information weapons. The article cites the opinion of the head of the psychological service of the Armed Forces of the Russian Federation, V. V. Barabanshchikova that the new challenges for the Armed Forces of the Russian Federation are: hybrid wars, cyber attacks, international terrorist organizations. The authors share the views of cybersecurity specialist Sergey Gordeychik on the possibility of destabilizing infrastructure objects managed

automatically through cyber attacks. The study concludes that information weapons should be considered both in the narrow sense-tools and means of committing cybernetic crimes, and in a broad sense – a system of criminally significant information and technological complexes and tools used in crimes committed using high technologies. The authors emphasize that cyber digital weapons have the following characteristics: stealth; offensive; individual selectivity to software; exist in a cybernetic environment; propagate their action through information technology networks. The types of cyber digital weapons are: passive and active. The complex of search and cognitive actions in the investigation of cybernetic crimes includes inspection of the scene, objects, documents, seizure of electronic media and copying information from them. At the subsequent stages of the investigation, it is proposed to perform interrogations, assign forensic cybernetic examinations, check the evidence on the spot, and, if necessary, conduct an investigative experiment.

Ключевые слова: кибернетические преступления, информационные технологии, киберцифровое оружие, кибернетические атаки, гибридные войны, кибербезопасность, киберсреда, компьютерно-сетевые и судебно-кибернетические экспертизы, осмотр предметов, изъятие электронных носителей информации и копирование с них информации.

Keywords: cyber crimes, information technologies, cyber digital weapons, cyber attacks , hybrid wars, cybersecurity, cyber environments, computer-network and forensic cyber expertise, inspection of items, seizure of electronic data carriers and copying of information from them.

Введение

Актуальность научного исследования состоит в том, что число преступлений в РФ, связанных с информационными технологиями и телекоммуникациями, увеличилось в десятки раз [1], при этом эффективность раскрытия рассматриваемых преступлений растет незначительно.

Вопросы криминалистического обеспечения расследования кибернетических преступлений изучались Россинской Е. Р., Ищенко Е. П., Кучиным О. С., Васюковым В. Ф., Семиколеновой А. С., Шаталовым А. С., Беровой Д. М., Нестеровичем С. А. и др.

Целесообразность исследования рассматриваемой проблематики связана со сравнительно низким процентом раскрываемости преступлений, совершаемых с использованием высоких технологий.

Научная новизна проведенного исследования связана с отражением в статье такого научного понятия, как киберцифровое оружие, являющегося, по нашему мнению, неотъемлемым элементом криминалистической характеристики кибернетически зависимых преступлений.

Авторы научной статьи руководствовались **целью**, связанной с приращением новых знаний в криминалистическом обеспечении расследовании преступлений с использованием информационно-телекоммуникационных систем и технологий. Исследованием решаются задачи по выработке признаков научного понятия киберцифрового оружия.

Теоритическая значимость научной статьи выражается в использовании новой категории криминалистической техники — киберцифрового оружия. Научная статья посвящена аспектам, связанным с расследованием кибернетических преступлений, что, безусловно, выделяет ее практическую значимость.

Основная часть

Формируя процессуальные и криминалистические основы расследования происшествий и преступлений, связанных с гибелью военнослужащих, авторы выделяют инновационные предложения по дополнению криминалистического оружиеведения подотраслью — криминалистическое исследование киберцифрового оружия.

На расширенной коллегии ФСБ 20 февраля 2020 г. Президентом Российской Федерации Путиным В. В. обоснованно сказано о росте угроз в области информационной безопасности, о всеобъемлющем характере кибератак, а также о необходимости противодействия информационному оружию в связи с возрастанием высокотехнологичных разработок [2].

Российская Федерация развивает международное сотрудничество в области противодействия киберпреступлениям, а также информационному оружию. В августе 2019 г. секретарь Совета безопасности РФ доктор юридических наук Н. П. Патрушев провел встречу с руководителем ведомства по кибербезопасности Сингапура Дэвидом Кохом для координации деятельности по борьбе с кибератаками и безопасного использования информационно-коммуникационных технологий [3].

Авторы выражают солидарность с мнением доктора психологических наук начальника психологической службы Вооруженных сил РФ Валентины Владимировны Барабанщиковой о том, что новыми вызовами для Вооруженных сил Российской Федерации являются гибридные войны, кибератаки, международные террористические организации [4].

Разработка сущностных структур, концептуальных положений, методологических основ в области процессуальных, поисково-познавательных, следственных [5], тактических действий при расследовании кибератак, киберпреступлений, использования киберцифрового оружия органами дознания и следствия, военной юстиции являются приоритетными направлениями по предотвращению преступности, в частности гибели в вооруженных формированиях, убийств военнослужащих [6, 7].

Известным российским документалистом Игорем Станиславовичем Прокопенко отмечается уязвимость высокотехнологичного оружия от кибердиверсий. Писателем Прокопенко И. С приводятся примеры сбоев в системе защиты гидроэлектростанции Итайпу в Бразилии, в результате чего в 2009 г. более 60 млн человек остались без света и воды. Игорь Станиславович обоснованно считает, что причиной выхода из строя телекоммуникационного оборудования иранского истребителя в 2010 г. стала кибератака, нацеленная против атомной электростанции «Бушер». Система противовоздушной обороны Ирана своевременно обнаружила и сбила неуправляемый пилотами самолет, пересекающий запрещенное воздушное пространство над АЭС, что позволило избежать катастрофы [8]. В 2012 году АЭС в Иране также подверглась атаке информационного оружия, на особо охраняемом объекте система управления оказалась перехваченной внешним управлением хакерами, и в период атаки издевательски звучала рок-песня «Громом пораженные».

Авторы разделяют взгляды специалиста по кибербезопаности Сергея Гордейчика о возможности дестабилизировать объекты инфраструктуры, управляемые автоматизированно, посредством кибернетических атак. Инфраструктура Минобороны РФ в 2017 г. подверглась атаке кибервирусом WannaCry, успешно ее отразив [9].

Кибердиверсия по взлому военного исходного кода программного обеспечения ВМФ США увенчалась успехом у хакерской группы, получившей доступ к программам управления военными спутниками и ударными ракетами, что могло повлечь их боевое применение и гибель, в том числе военнослужащих. Хакеры в феврале 2016 г. получили доступ к контролю системы управления США боевым беспилотником GLOBAL HAWK и предприняли действия по погружению его в воды Тихого океана, а в августе 2019 г. проникли в программное обеспечение многофункционального истребителя «Фантом-15» США. Критические точки объектов обороны вооруженных сил ЮАР подверглись атаке в 2009 г., в результате чего высокотехнологичное зенитное орудие расстреляло 23 человека, погибло 9 военнослужащих.

Следует признать мощность киберцифрового оружия как элемента криминалистической характеристики киберзависимых преступлений. Хакеры перехватывают управление высокоточными технологичными системами — спутниками, беспилотниками, боевыми надводными кораблями и подводными лодками, бронетанковой техникой, боевыми орудиями, авиационными средствами, ракетами, вносят вредоносные коррективы в программу деятельности и перенацеливают их на нанесение ударов по выбранным ими целям, что, безусловно, ставит перед правоохранительными органами, органами дознания и предварительного расследования, в том числе органами военной юстиции, задачи по предотвращению, своевременному выявлению и расследованию рассматриваемых преступлений с использованием киберцифрового оружия, в целях обеспечения безопасности, предотвращения гибели военнослужащих.

Развитие информационных технологий и формирование доктринальных положений в рамках нашего исследования способствуют разработке новых и совершенствованию известных способов и методов расследования киберпреступлений, способных, в том числе, привести к гибели военнослужащих. В связи с эволюцией цифровых технологий киберпреступники выбирают объекты своих атак не только среди государственных электронных систем, но и операторов связи, банковских структур, добывающих предприятий, граждан.

Преступления, совершаемые посредством кибертехнологий, — это преступления которые свершаются с помощью компьютеров, а также иных информационных средств и вычислительно-программируемых устройств.

Известный ученый-практик Д. М. Берова в своем определении киберпреступности отмечает, что последние совершаются в киберпространстве с использованием компьютерных систем. Нам думается, что следует распространить это определение и на информационно-телекоммуникационные сети, посредством которых информация управления передается по каналам связи [10].

Представляется возможным в качестве определенных особенностей рассматриваемой категории преступлений выделить их латентность, отметить малоизвестность явок с повинной, механизм преступления отличает мгновенность и дерзость преступных мероприятий. Следственная практика не выделяет затруднений по установлению потерпевших от киберпреступлений, которые в большинстве своем относятся к категории неочевидных деяний. Безусловно, нагрузка по выявлению рассматриваемых общественно опасных деяний ложится на оперативные, технически оснащенные органы.

При проведении доследственной проверки сообщений по рассматриваемой категории преступлений устанавливаются в том числе следы, оставленные в ходе преступной деятельности, от использования киберцифрового оружия, с учетом свойства отражения материи. Обнаружение, фиксация и изъятие следов преступления, в том числе электронных [11], является важным условием всестороннего и надлежащего расследования исследуемых преступлений, занимающих небольшой промежуток времени. Так, Т., увидев на веб-сайте объявление с предложением внести денежные средства под процент на счет 890****470*, открытый в Visa Qiwi Wallet, осуществила перевод денежных средств, после чего счет оказался заблокирован [10, с. 2]. Компетентными органами предварительного расследования во время проверки установлены регистрационные данные ве-бсайта с сервера, а также транзакции по указанному счету, что, в свою очередь, способствовало установлению и привлечению к ответственности лицо, совершившее преступление.

Нам видится, что к первоначальным следственным действиям как на стадии возбуждения уголовного дела, так уже и на предварительном расследовании преступлений, совершенных киберцифровым оружием, безусловно, следует отнести осмотр места происшествия, предметов, документов, изъятие электронных носителей информации и копирование с них информации. На последующих этапах расследования представляется возможным выполнять допросы, назначение судебно-кибернетических экспертиз, проверка показаний на месте, при необходимости следственный эксперимент.

Авторы в результате исследования пришли к мнению о дополнении рекомендаций, предложенных доктором юридических наук Кучиным О. С. [12] Олег Стасьевич Кучин считает доказательства кибератак, только отраженные в заключениях эксперта и специалиста. Нам видится, что это может значительно сузить сведения, имеющие значение для уголовного дела, отраженные в протоколах следственных и судебных действий. Безусловно, выявить, зафиксировать и изъять электронные следы кибернетически зависимых преступлений представляет определенную сложность, вместе с тем авторы уверены, что при отражении в протоколах осмотров места преступления, предметов и документов с привлечением специалистов по высоко-технологичному оборудованию искомые сведения, входящие в предмет доказывания, не потеряют своего процессуального статуса.

В целях наглядности поисково-познавательных действий на месте происшествия предлагается тактическая рекомендация по приобщению к протоколу следственного действия, проведенного с участием специалистов, привычных для восприятия блок-схем, отражающих последовательность выполненного киберзависимого преступления.

Посредством интервьюирования выявлено, что для сотрудников органов дознания и следствия вызывает также определенную сложность данная категория дела в связи со спецификой области научных знаний, необходимостью получения дополнительного образования и консультаций специалистов по вопросам высоких технологий.

Проблемам расследования кибернетических преступлений посвятил свои научные работы Нестерович С. А., отмечающий, в частности, что порой сама жертва преступления не понимает, что преступление совершенно [13]. Это происходит ввиду того, что потерпевший может попросту не заметить совершенного преступления (не обратить внимания на исчезновение денежной суммы, особенно если она незначительна; не заметить исчезновения или нарушения работы в какой-либо программе или файле). В последнем

случае все осложняется тем, что зачастую системные неполадки и сбои часто списываются на плохую работу технических средств либо на занесение вредоносных программ по вине самого пользователя. Как следствие — несвоевременное сообщение о преступлении, часто жертва осознает, что против нее совершено противоправное деяние, слишком поздно (более 10 дней) и только тогда сообщает об этом в правоохранительные органы. За столь продолжительный срок многие важные обстоятельства (да и сам преступник) могут бесследно исчезнуть.

Следует отметить сложность и длительность проведения необходимых криминалистических экспертиз. Несмотря на распространенное мнение о применении судебно-компьютерных экспертиз, авторы с вниманием отнеслись к предложению Васюкова В. Ф. о проведении компьютерно-сетевых экспертиз [14]. Авторы уверены в необходимости расширения этимологического наименования и проведения судебно-кибернетических экспертиз, объектами которых, безусловно, являются: информационное оружие в своей совокупности, отдельные носители электронных следов, облачные технологии, информационные глобальные, локальные и беспроводные сети [15].

Именно судебно-кибернетическая экспертиза, на наш взгляд, является основным и наиболее эффективным способом в расследовании преступлений.

Высококвалифицированными специалистами в сфере борьбы с киберпреступностью и проведения соответствующих исследований представляется нужным отметить, в частности, сотрудников Group-IB, LETA IT-company, которые широко сотрудничают с правоохранительными органами как на внутригосударственном, так и на международном уровнях.

В процессе проведения отмеченных экспертиз выполняются кропотливые мероприятия по отысканию вредоносной программы (вируса) путем декомпиляции всех установленных программ и файлов, что требует достаточных временных затрат. Так, например, при заражении телефона с предустановленной операционной системой Android изучаются подозрительные приложения и программы (файлы расширения .apk формата). При исследовании вредоносного вируса специалист способен обнаружить в части кода IP-адрес, на который без ведома владельца вирус отправляет компрометирующую информацию. Посредством дальнейших оперативно-разыскных мероприятий выполняется поиск и обнаружение местонахождения предполагаемого правонарушителя, а впоследствии его задержание и проведение по месту жительства лица таких неотложных следственных действий, как осмотр, обыск, выемка, эффективность которых повышается при использовании специалиста в области высоких технологий.

Выводы, заключение

Киберцифровое оружие следует рассматривать как в узком — орудия и средства совершения кибернетических преступлений, так и в широком смысле — система криминалистически значимых информационно-технологических комплексов и средств, применяемых в преступлениях, совершаемых с использованием высоких технологий.

Киберцифровое оружие обладает следующими признаками: скрытностью, наступательностью, индивидуальной избирательностью к программному обеспечению, существует в кибернетической среде, распространяет свое действие посредством информационно-технологических сетей. К типам киберцифрового оружия следует отнести оружие пассивного и активного действия.

К первоначальным следственным действиям при расследовании преступлений, совершенных посредством киберцифрового оружия, безусловно, следует отнести осмотр места происшествия, предметов, документов, изъятие электронных носителей информации и копирование с них информации. На последующих этапах расследования представляется возможным выполнять допросы, назначение судебно-кибернетических экспертиз, проверку показаний на месте, при необходимости следственный эксперимент.

Авторы отмечают необходимость проведения широкого исследования в данной области, выработки инновационных подходов и современных рекомендаций для следственной и судебной практики. Важным аспектом признается выработка криминалистических основ познания механизма совершения преступления с использованием киберцифрового оружия. Создания специализированных подразделений расследования, укомплектование их специалистами, владеющими навыками и знаниями компьютерных технологий, использование зарубежного опыта, с нашей точки зрения, послужит превосходным опережающим стимулом в борьбе с киберпреступлениями в новых реалиях, в том числе в вооруженных формированиях.

Перефразируя превосходное выражение сэра Уинстона Черчилля перестать генералам готовиться к войне старыми методами, отметим необходимость подготовки и разработки положений по раскрытию новых вызовов преступности — использования киберцифрового оружия в кибернетических атаках.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Петров И. Число киберпреступлений в России увеличилось // Российская газета. 25.03.2019. URL: https://rg.ru/2019/03/25/kolokolcev-chislo-kiberprestuplenij-v-rossii-uvelichilos-v-16-raz.html.

2. Латухина К. Путин предупредил об усилении информационного оружия. // Российская газета. 2020. 20 февраля. URL: https://rg.ru/2020/02/20/reg-szfo/putin-predupredil-ob-usilenii-informacionnogo-oruzhiia.html.

3. Егоров И. Николай Патрушев обсудил в Сингапуре проблемы кибербезопасности // Российская газета. 2019. № 193. URL: https://rg.ru/2019/08/29/patrushev-obsudil-s-interpolom-kiberbezopasnost.html.

4. Свиридова А. На основе комплексного похода // Красная звезда. 11 марта 2019. URL: http://redstar.ru/na-osnove-kompleksnogo-podhoda/?attempt=1.

5. Рывкин С. Ю., Сенькина М. А. Следственные действия: Основы доказывания, процессуальные аспекты : учеб. пособие. М. : Академический научно-издательский, производственно-полиграфический и книгораспространительский центр «Наука», 2015. 72 с.

6. Рывкин С. Ю. Особенности расследования и предупреждения убийств, совершенных военнослужащими : дисс… канд. юрид. наук. Волгоград : Волгоградский государственный университет, 2005. 178 с.

7. Рывкин С. Ю. Особенности расследования и предупреждения убийств, совершенных военнослужащими : автореф. дисс… канд. юрид. наук. Волгоград : ВА МВД России, 2005. 30 с.

8. Прокопенко И. С. Оружие будущего. Каким будут войны нового тысячелетия? М. : Изд-во «Э», 2017. С. 22.

9. Всемирная атака хакеров // Официальный сайт Федерального государственного унитарного предприятия «Информационное телеграфное агентство России (ИТАР-ТАСС)». URL: https://tass.ru/armiya-i-opk/4256146.

10. Берова Д. М. Расследование киберпреступлений // Пробелы в российском законодательстве. 2018. № 2. С. 65—70.

11. Рывкин С. Ю. Малые беспилотные авиационные системы как инновационные элементы технико-криминалистических средств // Право и практика. 2019. № 4. С. 173—176.

12. Кучин О. С. Электронная криминалистика: миф или реальность // Академическая мысль. 2019. № 3. С. 67—70.

13. Нестерович С. А. Проблемы расследования преступлений, которые стоят перед сотрудниками следственных органов // Вестник науки и образования. 2018. № 8. С. 44—50.

14. Васюков В. Ф. Некоторые аспекты назначения судебной компьютерной экспертизы при расследовании хищений в сфере информационных и коммуникационных технологий // Вестник Удмуртского университета. 2016. Т. 26. Вып. 4. С. 109—110.

15. Россинская Е. Р., Рядовский И. А. Современные способы компьютерных преступлений и закономерности их реализации // Lex Russica. № 3. Март 2019 г. С. 87—99.

REFERENCES

1. Petrov I. The number of cybercrimes in Russia has increased. *Rossiyskaya Gazeta*, 25.03.2019. (In Russ.) URL: https://rg.ru/2019/03/25/kolokolcev-chislo-kiberprestuplenij-v-rossii-uvelichilos-v-16-raz.html.

2. Latukhina K. Putin warned about strengthening of information weapons. *Rossiyskaya Gazeta*, 20.02.2020. (In Russ.) URL:https://rg.ru/2020/02/20/reg-szfo/putin-predupredil-ob-usilenii-informacionnogo-oruzhiia.html.

3. Yegorov I. Nikolai Patrushev discussed cybersecurity issues in Singapore. *Rossiyskaya Gazeta*, 2019, no. 193. (In Russ.) URL: https://rg.ru/2019/08/29/patrushev-obsudil-s-interpolom-kiberbezopasnost.html.

4. Sviridova A. On the basis of an integrated approach. *Red star*, 11.03.2019. (In Russ.) URL: http://redstar.ru/na-osnove-kompleksnogo-podhoda/?attempt=1.

5. Ryvkin S. Yu., Senkina M. A. Investigative actions: Bases of proof, procedural aspects. Moscow, Nauka Publ., 2015. 72 p. (In Russ.)

6. Ryvkin S. Yu. *Features of investigation and prevention of murders committed by military personnel*. Diss. of Candidate of Law. Volgograd, Volgograd State University, 2005. 178 p. (In Russ.)

7. Ryvkin S. Yu. *Features of investigation and prevention of murders committed by military personnel*. Abstract Diss. of Cand. of Law. Volgograd, VA of the Ministry of internal Affairs of Russia, 2005. 30 p. (In Russ.)

8. Prokopenko I. S. *Weapons of the future. What will the wars of the new Millennium be like?* Moscow, E Publ., 2017. P. 22. (In Russ.)

9. World hacker attack. Official website of the Federal state unitary enterprise “Information Telegraph Agency of Russia (ITAR-TASS)„ (In Russ.) URL: https://tass.ru/armiya-i-opk/4256146.

10. Berova D. M. Investigation of cybercrime. *Gaps in Russian legislation*, 2018, no. 2, pp. 65—70. (In Russ.)

11. Ryvkin S. Yu. Small unmanned aircraft systems as innovative elements of technical and forensic tools. *Law and practice*, 2019, no. 4, pp. 173—176. (In Russ.)

12. Kuchin O. S. Electronic criminalistics: myth or reality. *Academic thought*, 2019, no. 3, pp. 67—70. (In Russ.)

13. Nesterovich S. A. Problems of investigating crimes that are faced by employees of investigative bodies. *Bulletin of science and education*, 2018, no. 8, pp. 44—50.

14. Vasyukov V. F. Some aspects of the appointment of forensic computer expertise in the investigation of theft in the field of information technology and communication technologies. *Bulletin of the Udmurt University*, 2016, vol. 26, issue 4, pp. 109—110. (In Russ.)

15. Rossinskaya E. R., Ryadovsky I. A. Modern methods of computer crimes and patterns of their implementation. *Lex Russica*, 2019, March, no. 3, pp. 87—99. (In Russ.)

Как цитировать статью: Рывкин С. Ю., Гусейнов Т. А. Киберцифровое оружие как элемент криминалистической характеристики киберпреступлений // Бизнес. Образование. Право. 2020. № 2 (51). С. 264–268. DOI: 10.25683/VOLBI.2020.51.263.

For citation: Ryvkin S. Yu., Huseynov T. A. Information weapons as an element of criminalistic characteristics of cybercrimes. *Business. Education. La*w, 2020, no. 2, pp. 264–268. DOI: 10.25683/VOLBI.2020.51.263.