ТРИБУНА МОЛОДОГО УЧЕНОГО
TRIBUNE OF YOUNG SCIENTIST

DOI: 10.18287/2542-047X-2025-11-2-96-102

НАУЧНАЯ СТАТЬЯ

УДК 343.3/.7

Дата поступления: 16.03.2025
рецензирования: 19.04.2025
принятия: 12.05.2025

Средства совершения преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана

А. Г. Корпеев
Самарский национальный исследовательский университет
имени академика С. П. Королева, г. Самара, Российская Федерация
E-mail: atakor@mail.ru

Аннотация: В статье в сравнительном ключе рассматривается правовая природа средств совершения преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана. Дается общая характеристика средств совершения преступлений в сфере компьютерной информации, описываются их видообразование и классификация. С учетом комплекса оснований (информационно-технологического, международно-правового, национально-правового и доктринального характера) предложено авторское деление средств совершения преступлений в сфере компьютерной информации. Это компьютерные программы (в том числе вредоносные) либо иная компьютерная информация (ст. 272, 272[1], 273, 274, 274[1] УК РФ, 373, 374, 375, 379 УК Туркменистана); компьютерные устройства и иные виды электронно-вычислительных устройств (ст. 274, 274[1] УК РФ, 373, 374, 375, 377 УК Туркменистана); информационно-телекоммуникационные сети, включая сеть «Интернет», и иные коммуникационные сети (ч. 6 ст. 272[1], 274, 274[1], 274-2 УК РФ, 373, 374, 375, 376, 377, 379 УК Туркменистана). Делается вывод, что теоретико-прикладное исследование правовой природы средств совершения преступлений в сфере компьютерной информации является важной составляющей противодействия криминальным посягательствам в названной области, эффективности предупреждения преступлений данной категории.

Ключевые слова: компьютерная информация; программы для электронных вычислительных машин, в том числе вредоносные компьютерные программы; информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления; средства хранения, обработки или передачи компьютерной информации; средства совершения преступлений в сфере компьютерной информации, компьютерные устройства.
Цитирование. Корпеев А. Г. Средства совершения преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана // Юридический вестник Самарского университета Juridical Journal of Samara University. 2025. Т. 11, № 2. С. 96–102. DOI: https://doi.org/10.18287/2542-047X-2025-11-2-96-102.
Информация о конфликте интересов: автор заявляет об отсутствии конфликта интересов.

Ата Гельдыевич Корпеев – ассистент кафедры теории и истории государства и права и международного права, Самарский национальный исследовательский университет имени академика С. П. Королева, 443086, Российская Федерация, г. Самара, Московское шоссе, 34.

SCIENTIFIC ARTICLE

Submitted: 16.03.2025
Revised: 19.04.2025
Accepted: 12.05.2025

Means of committing crimes in the field of computer information under the criminal legislation of the Russian Federation and Turkmenistan

A. G. Korpeev
Samara National Research University, Samara, Russian Federation
E-mail: atakor@mail.ru.

Abstract: The legal nature of the means of committing crimes in the field of computer information under the criminal legislation of the Russian Federation and Turkmenistan is examined in a comparative manner. A general description

of the means of committing crimes in the field of computer information is given, their modification and classification are described. Taking into account the complex of grounds (information technology, international law, national law and doctrinal nature), the author's division of the means of committing crimes in the field of computer information is proposed into: computer programs (including malicious ones) or other computer information (Articles 272, 272[1], 273, 274, 274[1] of the Criminal Code of the Russian Federation, 373, 374, 375, 379 of the Criminal Code of Turkmenistan); computer devices and other means of storing, processing or transmitting computer information (Articles 274, 274-1 of the Criminal Code of the Russian Federation, 373, 374, 375, 377 of the Criminal Code of Turkmenistan); information and telecommunication networks, including the Internet and public communications networks (Part 6 of Articles 272[1], 274, 274[1], 274[2] of the Criminal Code of the Russian Federation, 373, 374, 375, 376, 377, 379 The Criminal Code of Turkmenistan). It is concluded that theoretical and applied study of legal nature of the means of committing crimes in the field of computer information is an important component of countering criminal encroachments in this area, increases the effectiveness of preventing crimes of this category.
Key words: computer information; programs for electronic computers, including malicious computer programs; information systems; information and telecommunication networks and terminal equipment; automated control systems; telecommunication networks; means of storing, processing or transmitting computer information; means of committing crimes in the field of computer information.
Citation. Korpeev A. G. *Sredstva sovershеniya prestuplenii v sfere komp'yuternoi informatsii po ugolovnomu zakonodatel'stvu Rossiiskoi Federatsii i Turkmenistana* [Means of committing crimes in the field of computer information under the criminal legislation of the Russian Federation and Turkmenistan]. Iuridicheskii vestnik Samarskogo universiteta Juridical Journal of Samara University, 2025, vol. 11, no. 2, pp. 96–102. DOI: https://doi.org/10.18287/2542-047X-2025-11-2-96-102 [in Russian].
Information on the conflict of interests: author declared no conflicts of interests.

Ata Geldyevich Korpeev – assistant lecturer at the Department of Theory and History of State and Law and International Law, Samara National Research University, 34, Moskovskoye shosse, Samara, 443086, Russian Federation.

Преступления в сфере компьютерной информации занимают особое место среди современных видов преступлений. Продолжающийся рост таких криминальных посягательств связан с научно-технологическим развитием электронных и информационно-телекоммуникационных технологий [1–7]. Революция в сфере компьютерной техники предоставляет широкие возможности социального доступа к использованию новейших технических средств, в том числе и криминального толка[1]. Перечень электронных и информационно-телекоммуникационных технологий является открытым, ввиду того что перед многими предприятиями и иными организациями, специализирующимися на производстве компьютерных технологий, программного обеспечения, стоит задача цифровой трансформации экономических, социальных, политических сегментов общественной жизни, а также обеспечения цифрового суверенитета страны. Президент Российской Федерации В. В. Путин предложил провести цифровую трансформацию всей страны, а также обеспечить внедрение повсеместно искусственного интеллекта[2]. Равным образом Президент Туркменистана С. Г. Бердымухамедов заявил о необходимости цифровизации сегментов общественной жизни, которая позволит совершить экономический рывок[3]. Непрерывное развитие высоких технологий – общемировой тренд. Во многих государствах, в том числе в Российской Федерации и Туркменистане, курс технологической трансформации определен как приоритетный. Обратной стороной распространения электронных и информационно-телекоммуникационных технологий как раз и является использование компонентов цифровизации в криминальных и иных противоправных целях. С учетом вышеизложенного возникает вопрос: что следует признавать средством совершения преступлений в сфере компьютерной информации? Современная уголовно-правовая наука ставит данный вопрос во главу угла в связи с тем, что он является одним из основных вопросов предмета доказывания таких видов преступлений. Понятно, что все преступления в сфере компьютерной информации совершаются с использованием электронных и информационно-телекоммуникационных технологий, но для уголовно-правовой доктрины, а также правоприменительной практики релевантным положением являются унифицированное определение понятия и категоризация различных способов и средств совершения преступлений в сфере компьютерной информации [8–16].

Следует подчеркнуть, что объективные признаки составов преступлений в сфере компьютерной информации являются по своей правовой природе бланкетными. Как правильно указывается в п. 1 Постановления Пленума Верховного Суда РФ от 15 декабря 2022 года «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет"», при рассмотрении уголовных дел о преступлениях в сфере компьютерной информации следует руководствоваться положениями федеральных зако-

[1] См.: Конявский В.А., Лопаткин, С.В. Компьютерная преступность: в 2 т. Т. 1 [4].
[2] См.: Путин заявил о необходимости цифровой трансформации России [6]..
[3] См.: Цифровизация – ключевой фактор экономического развития [7].

нов, которые регламентируют вопросы создания, распространения, передачи, защиты информации и применения информационных технологий. Это, в частности, федеральные законы от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»,от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и другие федеральные законы, подзаконные акты, технические регламенты. Также речь идет о ратифицированных Российской Федерацией международных договорах и соглашениях, посвященных указанным вопросам и борьбе с преступлениями в сфере компьютерной информации, в частности Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (заключено в городе Душанбе 28 сентября 2018 года)[4]. В этом смысле при определении легальных понятий факультативных признаков объективной стороны, в частности, средств совершения преступлений, деяний, предусмотренных главой 28 УК России «Преступления в сфере компьютерной информации», главой 33 УК Туркменистана «Преступления в сфере компьютерной информации», следует обращаться к действующим нормативным правовым актам Российской Федерации и Туркменистана, регулирующим общественные отношения в сфере безопасности информации и информационных технологий, в том числе указанных в приведенном выше постановлении.

Для ряда преступлений, в том числе преступлений в сфере компьютерной информации, имеет место наличие средств совершения преступлений как вспомогательных предметов для реализации преступного умысла. По своей правовой природе средства совершения преступлений являются частью объективной стороны преступления, однако не входят в число обязательных признаков объективной стороны. Зачастую средства совершения преступлений в доктрине уголовного права характеризуют как факультативный признак объективной стороны преступления, однако в ряде преступлений уголовного законодательства Российской Федерации и Туркменистана, к которым в том числе относятся преступления в сфере компьютерной информации, средства совершения преступлений являются одной из «обязательных составляющих объективной стороны, ввиду того, что наличие средств совершения преступлений может указывать на характер и степень общественной опасности, общественные отношения, ставшие целью преступного посягательства»[5]. Вместе с тем использование средства совершения преступлений является «индикатором» отягчающих обстоятельств. Преступления в сфере компьютерной информации относятся в когорте преступлений, объективная сторона которых не может не включать средства совершения преступлений. Например, ст. 272 УК РФ, 373 УК РФ: незаконный доступ, а впоследствии копирование, уничтожение и модификация компьютерной информации обязательно будут сопровождаться использованием соответствующего средства совершения преступлений, что по своей сути выступает существенным условием при установлении общественной опасности деяния. В этом смысле в доктрине также указывают на аналогию понятий «средства совершения компьютерных преступлений» и «орудия совершения преступлений». Средства совершения преступлений и орудие преступлений определяют, как равнозначные или единые категориальные понятия. Применительно к преступлениям в сфере компьютерной информации компьютерные устройства выполняют разную роль при совершении преступлений. В связи с этим по данному признаку преступления в сфере компьютерной информации следует распределить по следующим группам: многосредственные, технологические, аппаратные, сетевые, дистанционные, автоматизированные, многоспектральные, простые компьютеризованные, сложные многоуровневые[6]. «С другой стороны, средства совершения преступлений и орудия совершения преступлений унифицируют как род и вид»[7], однако орудия преступлений относят к числу материальных предметов, в отличие от средств совершения преступлений, которые могут быть как материальными, так и нематериальными компонентами. Например, в рамках рассматриваемых преступлений в сфере компьютерной информации материальными средствами могут быть электронно-вычислительные машины (компьютеры, смартфоны), а нематериальными – информационно-телекоммуникационные сети, включая сеть «Интернет».

«Под средством совершения преступлений обычно понимаются предметы материального мира, с помощью которых преступник совершает преступление и (или) применяет их (при совершении действий, образующих объективную сторону состава преступления) для достижения намеченных преступных целей. Средства совершения преступлений являются возможным инструментом в рамках сокрытия преступного намерения»[8].

---

[4] См.: Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» [11].

[5] Григорян Г. Р. Мошенничество в сфере компьютерной информации: проблемы криминализации, законодательной регламентации и квалификации: дис. ... канд. юрид. наук [3].

[6] Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия [2].

[7] Гальчун Е. А. Средства и орудия совершения преступления. С. 717–721 [16].

[8] Григорян Г. Р. Мошенничество в сфере компьютерной информации... С. 128 [3].

Многие авторы характеризуют средства совершения преступлений с позиции материального компонента. Однако при совершении преступлений в сфере компьютерной информации, как было указанно выше, используются не только материальные (физические) средства, но и нематериальные. К группе нематериальных следует относить, например, компьютерную информацию, программное обеспечение, информационно-телекоммуникационные сети. При этом программное обеспечение или информационно-телекоммуникационная сеть не могут функционировать как самостоятельные компоненты без определенного компьютерного устройства (электронно-вычислительной машины). Из этого следует, что образуется цепочка, связывающая несколько компонентов (устройство – сеть – программа), при этом определять средство совершения преступления следует из контекста самого состава преступления. «У преступника, посягающего на охраняемые законом интересы в сфере компьютерной информации, в части использования средств совершения преступлений может полностью отсутствовать материальная составляющая в связи с тем, что средство совершения преступления является виртуальным и не существует в физическом мире в качестве материи (например, ст. 273 УК РФ и ст. 379 УК Туркменистана)»[9].

В соответствии с п. 2 Постановления Пленума Верховного Суда РФ от 15 декабря 2022 года № 37 к компьютерным устройствам могут быть отнесены персональные компьютеры, ноутбуки, мобильные телефоны, смартфоны, цифровые аппараты с вычислительным устройством[10]. Все вышеперечисленные устройства являются материальными средствами совершения преступлений. Исходя из изложенного, средства совершения преступлений в сфере компьютерной информации можно разделить на две группы: материальные – компьютерные устройства; нематериальные – вредоносное программное обеспечение, информационно-телекоммуникационные сети.

В Законе Туркменистана «О правовом регулировании развития сети ‘‘Интернет’’и оказания интернет-услуг в Туркменистане» от 20 декабря 2014 года к средствам совершения преступлений относят средства электронно-вычислительной (компьютерной) техники, веб-серверы (компьютер, подключенный к сети «Интернет»), информационно-телекоммуникационные сети[11]. Вместе с тем в законодательстве Туркменистана в качестве средств совершения преступления в сфере оказания интернет услуг (ст. 381 УК Туркменистана) приводятся веб-страницы; веб-сайты, применяемые с целью получения частной или иной информации обманным путем; средства криптографической защиты, применяемые для хранения и передачи запрещенной к распространению законодательством Туркменистана информации[12].

Согласно ст. 11 Закона Туркменистана от 3 мая 2014 года № 72-V «Об информации и ее защите», все средства совершения преступлений обозначаются единым термином «информационные технологии». Частью таких информационных технологий являются любые устройства, предоставляющие возможность поиска, получения, передачи, сбора, хранения, распространения информации[13]. Среди таких выделяют электронные коммуникационные сети (линейные и многоуровневые). С точки зрения безопасности многоуровневые сети являются небезопасными для передачи информации в связи с тем, что специфика их работы заключается в иерархичной системе передачи информации, поэтому существуют риски модификации такой информации. При этом вспомогательным оборудованием таких сетей являются сетевые кабели, маршрутизаторы, роутеры.

Большое разнообразие компьютерных технических средств порождает множество различных классификаций, например по законности их происхождения, по техническому наполнению, а также по технологии использования[14].

По законности происхождения средства совершения преступлений могут быть законные, т. е. компьютеры, телефоны, флеш-карты, смартфоны, ноутбуки, программное обеспечение, произведенные с сертификацией и в соответствии с техническими требованиями страны реализации, а равно промышленным производством. Незаконными средствами в соответствии с п. 2 Постановления являются устройства, произведенные кустарным способом, например компьютер или смартфон, собранный собственноручно из различных комплектующих[15]. По технологии использования выделяют устройства, дающие возможность совершать действия удаленным способом (компьютеры и мобильные устройства с программным обеспечением, позволяющим взаимодействовать с основным устройством на расстоянии), и устройства с отсутствием удаленного доступа[16]. По техническому наполнению это могут быть периферийные аппараты – дополнительные вспомогательные устройства, которые подключаются к компьютерному устройству для расширения его функциональных

[9] См.: Конявский В. А., Лопаткин С. В. Компьютерная преступность.: в 2 т. Т. 1 [4].
[10] Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации...» [11].
[11] Закон Туркменистана «О правовом регулировании развития сети ‘‘Интернет’’ и оказания интернет-услуг в Туркменистане» от 20.12.2014 № 159-V [12].
[12] Там же.
[13] Закон Туркменистана «Об информации и ее защите» от 3 мая 2014 года № 72-V [13].
[14] См.: Поляков В. В., Лапин С. А. Средства совершения компьютерных преступлений [5].
[15] Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации...» [11].
[16] Россинская Е. Р., Рядовский И. А. Современные способы компьютерных преступлений и закономерности их реализации [15]; Поляков В. В., Лапин С. А. Средства совершения компьютерных преступлений [5].

возможностей (например, сканер, графический планшет), устройства для ввода информации в компьютерное устройство, дополнительные USB-порты. В совокупности данные устройства следует определять как вспомогательные к основному средству совершения преступлений, они могут использоваться, например, с целью ввода информации в компьютерное устройство.

Другая классификация средств совершения преступлений касается разделения на типы применения данных средств: в одних случаях умысел направлен на компьютерное устройство, в данном случае имеется в виду причинение вреда компьютерному устройству или группе устройств с помощью умышленного внедрения вредоносных программ, в других случаях это может быть совершение информационной атаки для целенаправленного воздействия на сервера, маршрутизаторы, коммуникационные сети и иные информационные системы, образующие критическую инфраструктуру государства (ст. 274.1. УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации», ст. 376 УК Туркменистана «Нарушение нормальной работы информационной системы и информационно-телекоммуникационной сети»).

В соответствии с Конвенцией о компьютерных преступлениях от 23.11.2001 под компьютерными устройствами понимаются любые устройства, осуществляющие обработку автоматизированных данных[17]. На региональном уровне в соответствии с Соглашением о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20.11.2013, участниками которого являются Российская Федерация и Туркменистан, средствами совершения преступлений в сфере компьютерной информации признаются программно-технические средства, обеспечивающие сбор, воспроизводство, обработку, копирование, передачу информации[18]. Однако конкретный перечень таких средств в нормативных правовых актах отсутствует.

Отсутствие таких перечней подтверждает огромное количество нетривиальных способов совершения преступлений в сфере компьютерной информации. При этом совершение преступлений в сфере компьютерной информации вне зависимости от использования определенного средства совершения преступлений следует определять как умышленное действие субъекта преступления, совершенное путем проникновения в информационную систему, или путем воздействия на компьютерное устройство, или путем внедрения вредоносного программного обеспечения в информационную систему, компьютерное устройство, информационно-телекоммуникационную сеть[19]. В этом смысле, по нашему мнению, в уголовном законодательстве Российской Федерации и Туркменистана можно выделить три группы средств совершения преступлений: вредоносные ПО, в частности троянские программы, черви, шпионские программы, рекламные программы, вирусы, ботнеты, гибридные программы, логические бомбы; системы связи, в частности системы телефонной связи IP-телефонию, глобальную информационно-телекоммуникационную сеть «Интернет» и сложные нейронные сети, а также разнообразные компьютерные устройства, включая ПК, ноутбуки, мобильные компьютеры (такие как планшеты и смартфоны), встроенные системы, специализированные промышленные вычислительные машины, мощные суперкомпьютеры, веб-серверы, прокси-серверы. На основании аналитики компании «Касперский»[20] следует отметить, что представленный выше список является актуальным на сегодняшний день перечнем средств совершения преступлений, которыми активно пользуются преступники для реализации преступного умысла.

Представленная нами классификация средств совершения преступлений в сфере компьютерной информации в соответствии с уголовным законодательством Российской Федерации и Туркменистана является по своей сути триадой, образующей единое целое (средства совершения) из различных по своей природе информационных технологий. Цель использования данной триады – нанесение damnum общественным отношениям, охраняемым уголовным законодательством. В этом и заключается unitas (единство) этих средств, разных по своей природе (материальных и нематериальных), техническим особенностям функционирования, с точки зрения дополнительных компонентов, способствующих их работе. В этом и заключается их differentia.

Исходя из вышеизложенного, важно отметить, что информационные технологии, которые преступники используют как средство совершения противоправного умысла, являются весьма разнообразными в Российской Федерации и Туркменистане, о чем свидетельствует действующее законодательство двух стран. При этом распространение релевантных видов компьютерных преступлений происходит быстрее, чем реагирование со стороны правоохранительной системы[21]. Одними из новых технологических средств совершения преступлений являются нейронные сети[22], но, несмотря на только развивающуюся сферу, та-

[17] См.: Волеводз А. Г. Конвенция о киберпреступности: новации правового регулирования [1].
[18] Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20.11.2013 № 13-1536-н [14].
[19] Cybercrime regulation across BRICS countries. URL: https://cyberbrics.info/cybercrime-regulation-across-brics-countries (дата обращения: 22.10.2024).
[20] См.: Что такое киберпреступность? Защита киберпреступности [8].
[21] См.: Выступление Генерального прокурора Российской Федерации в ходе саммита руководителей прокурорских служб «G20» на тему новые технологии и борьба с транснациональной преступностью» [10].
[22] Там же.

кие сети уже используются преступниками, например для отмывания денег, в том числе цифровой валюты. Исходя из этого, проблема определения средств совершения преступлений в сфере компьютерной информации является релевантной для Российской Федерации и Туркменистана. Предложенная нами классификация и перечень основных средств совершения преступлений в сфере компьютерной информации являются актуальными на сегодняшний день как в Российской Федерации, так и в Туркменистане, а также позволяют унифицировать подходы к определению таких средств совершения преступлений. Однако стоит обратить внимание на тот факт, что число способов совершения таких преступлений увеличивается с каждым годом, а тенденция быстрого технологического развития приводит к появлению новых видов потенциальных средств совершения преступлений. Иными словами, нужно понимать, что перечень таких преступлений не является исчерпывающим и будет пополняться.

Библиографический список

1. Волеводз А. Г. Конвенция о киберпреступности: новации правового регулирования // Правовые вопросы связи. 2007. № 2. С. 17–25. URL: https://mgimo.ru/library/publications/113908/?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru; https://www.elibrary.ru/item.asp?id=19413856. EDN: https://www.elibrary.ru/qivrfr.

2. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / под ред. акад. Б. П. Смагоринского. Москва: Право и закон, 1996. 182 с. URL: https://polyglotlife.ru/wp-content/uploads/2023/10/Viekhov-V.B.-Kompiutiernyie-p-Miha.pdf.

3. Григорян Г. Р. Мошенничество в сфере компьютерной информации: проблемы криминализации, законодательной регламентации и квалификации: дис. ... канд. юрид. наук: 12.00.08. Самара, 2021. 243 с. URL: http://repo.ssau.ru/handle/Dissertacii-Zakryto/Moshennichestvo-v-sfere-komputernoi-informaciiproblemy-kriminalizacii-zakonodatelnoireglamentacii-i-kvalifikacii-91274.

4. Конявский В. А., Лопаткин С. В. Компьютерная преступность: в 2 т. Т. 1. Москва: РФК-Имидж Лаб, 2006. 560 с. URL: https://www.okbsapr.ru/upload/iblock/de1/de158ab8f902a750a319a422816090e8.pdf.

5. Поляков В. В., Лапин С. А. Средства совершения компьютерных преступлений // Доклады Томского государственного университета систем управления и радиоэлектроники. 2014. № 2 (32). С. 162–166. URL: https://journal.tusur.ru/storage/44777/31.pdf?1465976922; https://www.elibrary.ru/item.asp?id=21571481. EDN: https://www.elibrary.ru/sebgtl.

6. Путин заявил о необходимости цифровой трансформации России. URL: https://tass.ru/ekonomika/10172635 (дата обращения: 18.10.2024).

7. Цифровизация – ключевой фактор экономического развития. URL: https://www.turkmenistan.gov.tm/ru/post/86889/cifrovizaciya-klyuchevoj-faktor-ekonomicheskogo-razvitiya (дата обращения: 18.10.2024).

8. Что такое киберпреступность? Защита от киберпреступности. URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (дата обращения: 22.10.2024).

9. Уголовное право. Общая часть / под ред. А. И. Рарога. Москва, 1997. С. 99.

10. Выступление Генерального прокурора Российской Федерации в ходе саммита руководителей прокурорских служб «G20» на тему новые технологии и борьба с транснациональной преступностью». URL: https://t.me/genprocrf/4330 (дата обращения: 22.10.2024).

11. Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» // СПС «КонсультантПлюс». URL: https://www.vsrf.ru/documents/own/31913/ (дата обращения: 22.10.2024).

12. Закон Туркменистана «О правовом регулировании развития сети «Интернет» и оказания интернет – услуг в Туркменистане» от 20.12.2014. URL: https://www.parahat.info/law/2014-12-29-zakon-turkmenistana-o-pravovom-regulirovanii-razvitiya-seti-internet-i-okazaniya-internet-uslug-v-turkmenistane (дата обращения: 22.10.2024).

13. Закон Туркменистана «Об информации и ее защите» от 3 мая 2014 года № 72-V. URL: https://base.spinform.ru/show_doc.fwx?rgn=85142 (дата обращения: 29.01.2025).

14. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20.11.2013 № 13-1536-н. URL: http://publication.pravo.gov.ru/Document/View/0001201506040007 (дата обращения: 22.10.2024).

15. Россинская Е. Р., Рядовский И. А. Современные способы компьютерных преступлений и закономерности их реализации // Lex Russica. 2019. № 3. 87–99. DOI: https://doi.org/10.17803/1729-5920.2019.148.3.087-099. EDN: https://elibrary.ru/ualfop.

16. Гальчун Е. А. Средства и орудия совершения преступления: понятие и уголовно-правовое значение // Инновации. Наука. Образование. 2021. № 36. С. 717–721. EDN: https://elibrary.ru/omdmry.

References

1. Volevodz A. G. *Konventsiya o kiberprestupnosti: novatsii pravovogo regulirovaniya* [Convention on cybercrime: innovations in legal regulation]. *Pravovye voprosy svyazi*, 2007, no. 2, pp. 17–25. Available at: https://mgimo.ru/library/publications/113908/?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru; https://www.elibrary.ru/item.asp?id=19413856. EDN: https://www.elibrary.ru/qivrfr [in Russian].

2. Vekhov V. B. *Komp'yuternye prestupleniya: sposoby sovershеniya i raskrytiya. Pod red. akad. B. P. Smagorinskogo* [Computer crimes: methods of committing and detection. Smagorinsky B. P. (ed.)]. Moscow: Pravo i zakon, 1996, 128 p. Available at: https://polyglotlife.ru/wp-content/uploads/2023/10/Viekhov-V.B.-Kompiutiernyie-p-Miha.pdf [in Russian].

3. Grigoryan G. R. *Moshennichestvo v sfere komp'yuternoi informatsii: problemy kriminalizatsii, zakonodatel'noi reglamentatsii i kvalifikatsii: dissertatsiya ... kand. yurid. nauk: 12.00.08* [Fraud in the field of computer information: problems of criminalization, legislative regulation and qualification: Candidate's of Legal Sciences thesis: 12.00.08]. Samara, 2021, 243 p. Available at: http://repo.ssau.ru/handle/Dissertacii-Zakryto/Moshennichestvo-v-sfere-komputernoi-informaciiproblemy-kriminalizacii-zakonodatelnoireglamentacii-i-kvalifikacii-91274 [in Russian].

4. Konyavskiy V. A., Lopatkin S. V. *Komp'yuternaya prestupnost':мv 2 t. T. 1* [Computer crime: in 2 vols. Vol. 1]. Moscow: RFK-Imidzh Lab, 2006, 560 p. Available at: https://www.okbsapr.ru/upload/iblock/de1/de158ab8f902a750a319a422816090e8.pdf [in Russian].

5. Polyakov V. V., Lapin S. A. *Sredstva sovershеniya komp'yuternykh prestuplenii* [Means of committing computer crimes]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki* [Proceedings of the TUSUR University], 2014, no. 2 (32), pp. 162–166. Available at: https://journal.tusur.ru/storage/44777/31.pdf?1465976922; https://www.elibrary.ru/item.asp?id=21571481. EDN: https://www.elibrary.ru/sebgtl [in Russian].

6. *Putin zayavil o neobkhodimosti tsifrovoi transformatsii Rossii* [Putin announced the need for digital transformation of Russia]. Available at: https://tass.ru/ekonomika/10172635 (accessed 22.10.2024) [in Russian].

7. Tsifrovizatsiya – klyuchevoi faktor ekonomicheskogo razvitiya [Digitalization is a key factor in economic development]. Available at: https://www.turkmenistan.gov.tm/ru/post/86889/cifrovizaciya-klyuchevoj-faktor-ekonomicheskogo-razvitiya (accessed 22.10.2024) [in Russian].

8. *Chto takoe kiberprestupnost'? Zashchita ot kiberprestupnosti* [What is cybercrime? Cybercrime defense]. Available at: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (accessed 22.10.2024) [in Russian].

9. *Ugolovnoe pravo. Obshchaya chast'. Pod red. A. I. Raroga* [Rarog A. I. (ed.) Criminal law. General part]. Moscow, 1997, p. 99 [in Russian].

10. *Vystuplenie General'nogo prokurora Rossiiskoi Federatsii v khode sammita rukovoditelei prokurorskikh sluzhb «G20» na temu novye tekhnologii i bor'ba s transnatsional'noi prestupnost'yu»* [Speech by the Prosecutor General of the Russian Federation during the G20 summit of heads of prosecutorial services on the topic of new technologies and the fight against transnational crime]. Available at: https://t.me/genprocrf/4330 (accessed 22.10.2024) [in Russian].

11. *Postanovlenie Plenuma Verkhovnogo Suda RF ot 15.12.2022 № 37 «O nekotorykh voprosakh sudebnoi praktiki po ugolovnym delam o prestupleniyakh v sfere komp'yuternoi informatsii, a takzhe inykh prestupleniyakh, sovershennykh s ispol'zovaniem elektronnykh ili informatsionno-telekommunikatsionnykh setei, vklyuchaya set' «Internet»* [Decision of the Plenum of the Supreme Court of the Russian Federation as of 15.12.2022 № 37 «On some issues of judicial practice in criminal cases on crimes in the field of computer information, as well as other crimes committed using electronic or information and telecommunication networks, including the Internet»]. *Retrieved from legal reference system «ConsultantPlus»*. Available at: https://www.vsrf.ru/documents/own/31913 (accessed 22.10.2024) [in Russian].

12. *Zakon Turkmenistana «O pravovom regulirovanii razvitiya seti "Internet" i okazaniya internet – uslug v Turkmenistane» ot 20.12.2014* [Law of Turkmenistan «On legal regulation of the development of the Internet and the provision of Internet services in Turkmenistan» dated December 20, 2014]. Available at: https://www.parahat.info/law/2014-12-29-zakon-turkmenistana-o-pravovom-regulirovanii-razvitiya-seti-internet-i-okazaniya-internet-uslug-v-turkmenistane (accessed 22.10.2024) [in Russian].

13. *Zakon Turkmenistana «Ob informatsii i ee zashchite» ot 3 maya 2014 goda № 72-V* [Law of Turkmenistan «On information and its protection» dated May 3, 2014 № 72-V]. Available at: https://base.spinform.ru/show_doc.fwx?rgn=85142 (accessed 22.10.2024) [in Russian].

14. *Soglashenie o sotrudnichestve gosudarstv – uchastnikov Sodruzhestva Nezavisimykh Gosudarstv v oblasti obespecheniya informatsionnoi bezopasnosti ot 20.11.2013 № 13-1536-n* [Agreement on cooperation between member states of the Commonwealth of Independent States in the field of information security dated November 20, 2013 № 13-1536-n]. Available at: http://publication.pravo.gov.ru/Document/View/0001201506040007 (accessed 22.10.2024) [in Russian].

15. Rossinskaya E. R., Ryadovskiy I. A. S*ovremennyye sposoby komp'yuternykh prestupleniy i zakonomernosti ikh realizatsii* [Modern methods of computer crimes and patterns of their implementation]. *Lex Russica*, 2019, no. 3, pp. 87–99. DOI: https://doi.org/10.17803/1729-5920.2019.148.3.087-099. EDN: https://elibrary.ru/ualfop [in Russian].

16. Galchun E. A. *Sredstva i orudiya sovershеniya prestupleniya: ponyatiye i ugolovno-pravovoye znacheniye* [Means and instruments of committing a crime: the concept and criminal legal significance]. *Innovations. Science. Education*, 2021, no. 36, pp. 717–721. EDN: https://elibrary.ru/omdmry .