

Научная статья

УДК 343. 98.06

EDN GEFZJT

DOI 10.17150/2500-4255.2024.18(4).398-411



К ВОПРОСУ О СОЗДАНИИ ЦИФРОВОЙ КРИМИНАЛИСТИЧЕСКОЙ МОДЕЛИ ДЛЯ СБОРА ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

У.А. Мусаева¹, Т.Б. Нгуен², Т.Х.Ч. Нгуен³, А.А. Светличный⁴,
Т.В. Толстухина⁴, В.Х. Тью⁵

¹ Академия государственного управления при Президенте Азербайджанской Республики,
г. Баку, Азербайджанская Республика

² Юридический университет Хюэ, г. Хюэ, Социалистическая Республика Вьетнам

³ Федерация адвокатов Вьетнама, г. Ханой, Социалистическая Республика Вьетнам

⁴ Тульский государственный университет, г. Тула, Российская Федерация

⁵ Академия социальных наук, г. Ханой, Социалистическая Республика Вьетнам

Информация о статье

Дата поступления

10 марта 2024 г.

Дата принятия в печать

27 сентября 2024 г.

Дата онлайн-размещения

15 октября 2024 г.

Ключевые слова

Кибербезопасность; цифровая
криминалистическая модель;
цифровая трансформация;
киберпространство;
киберпреступления; электронные
доказательства

Аннотация. В статье рассматривается проблема создания цифровой криминалистической модели для сбора электронных доказательств при расследовании транснациональных киберпреступлений. Посредством использования метода сравнения проводится анализ уголовного законодательства некоторых государств, позволивший выявить общие направления государственной деятельности по противодействию данным преступлениям, а также сформулировать авторское определение киберпреступлений. В статье также анализируются конкретные составы преступлений, предусмотренных уголовном законодательством Социалистической Республики Вьетнам, Российской Федерации и Азербайджанской Республики.

В работе приводятся результаты статистических исследований, отражающие динамику совершения и раскрытия преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации с 2018 по 2023 г. На основании анализа современного состояния киберпреступности формулируются тенденции, которые будут определять ее специфику до 2030 г.

Авторы приходят к выводу, что на государственном уровне руководители правоохранительных структур и ведомств расценивают задачу противодействия киберпреступности как первоочередную, при этом достаточно пристальное внимание проблемам борьбы с киберпреступностью в условиях цифровизации в последние годы уделяется и в научной литературе. Тем не менее раскрытие и расследование киберпреступлений всегда сталкиваются со множеством трудностей и ограничений, особенно при сборе электронной криминалистически значимой информации.

Для решения данной проблемы авторами уточняются необходимость и принципиальные требования к предлагаемой криминалистической модели для сбора электронных доказательств по указанным преступлениям, оцениваются преимущества и недостатки групп уже существующих цифровых криминалистических моделей, в том числе группы «общие цифровые криминалистические модели» при расследовании всех уголовных дел рассматриваемых видов преступлений. Эта группа моделей определяет этапы и подэтапы расследования, проводимые последовательно. Предлагается группа моделей, определяющая этапы и подэтапы предыдущей, характеризуемой как группа «моделей по этапам расследования конкретных видов преступлений», и группа «цифровых криминалистических моделей во многих других средах по технологическим и законодательным требованиям». Кроме того, авторами предлагается модель абстрактного уровня, которая направлена на сбор электронных доказательств, объединенная со знаниями отраслей и прикладных юридических наук (оперативно-розыскной деятельностью, криминологией, судебной экспертизой, уголовным процессом и др.) и существующими технологическими платформами.

Original article

ON THE ISSUE OF CREATING A DIGITAL FORENSIC MODEL FOR COLLECTING ELECTRONIC EVIDENCE IN THE INVESTIGATION OF CYBERCRIMES

Ulduz A. Musaeva¹, Thi Binh Nguyen², Thi Huen Chang Nguyen³, Alexander A. Svetlichny⁴, Tatyana V. Tolstukhina⁴, Van Hung Tew⁵

¹ Academy of Public Administration under the President of the Republic of Azerbaijan, Baku, the Republic of Azerbaijan

² Hue University of Law, Hue, the Socialist Republic of Vietnam

³ Vietnam Bar Federation, Hanoi, the Socialist Republic of Vietnam

⁴ Tula State University, Tula, the Russian Federation

⁵ Academy of Social Sciences, Hanoi, the Socialist Republic of Vietnam

Article info

Received

2024 March 10

Accepted

2024 September 27

Available online

2024 October 15

Keywords

Cybersecurity; digital forensic model; digital transformation; cyberspace; cybercrimes; electronic evidence

Abstract. The authors consider the problem of creating a digital forensic model for collecting electronic evidence in the investigation of transnational cybercrimes. A comparison method was used to analyze the criminal legislation of some countries, which made it possible to identify common areas of state activity to counteract such crimes, as well as to formulate the authors' definition of cybercrime. The authors also analyze specific elements of crimes provided for in the criminal legislations of the Socialist Republic of Vietnam, the Russian Federation and the Republic of Azerbaijan. The paper presents the results of statistical research reflecting the dynamics of committing and solving crimes involving the use of information and telecommunications technologies or in the field of computer information from 2018 to 2023. Based on the analysis of the current state of cybercrime, the authors formulate trends that will determine the specifics of cybercrime until 2030.

The authors come to the conclusion that, at the state level, heads of law enforcement agencies and departments regard the task of countering cybercrime as a priority, and that authors of research publications have been paying close attention to the problems of combating cybercrime in the context of digitalization in recent years. Nevertheless, the disclosure and investigation of cybercrimes involves overcoming numerous difficulties and limitations, especially in connection with collecting criminally significant electronic information. To solve this problem, the authors clarify the necessity and fundamental requirements for the proposed forensic model of collecting electronic evidence for these crimes, assess the advantages and disadvantages of groups of existing digital forensic models, including the group «general digital forensic models» in the investigation of all criminal cases for the crimes under consideration. This group of models will define the stages and sub-stages of the investigation, conducted sequentially. A group of models is proposed that defines the stages and sub-stages of the previous group, which is described as a group of «models for the stages of investigation of specific types of crimes» and a group of «digital forensic models in many other environments according to technological and legislative requirements.» In addition, the authors propose an abstract-level model aimed at collecting electronic evidence, combined with the knowledge of various branches of law and applied legal sciences (operational investigative activities, criminology, forensic expertise, criminal procedure, etc.) and existing technological platforms.

В современном мировом пространстве активное участие в промышленной революции 4.0 и проведении национальной цифровой трансформации является неременным объективным требованием для создания возможностей для социально-экономического развития при эффективном решении проблем национальной безопасности и правового порядка страны. Правильное осознание рисков и проблем, связанных с киберпространством, поможет нам активно защищать свои законные права и интересы при участии в цифровом пространстве и цифровом

обществе. При нынешних быстрых темпах развития и применения информационных технологий состояние кибербезопасности во многих странах будет видоизменяться, а количество киберпреступлений — неизменно возрастать, широко распространяясь во все сферы жизни страны.

В законодательстве Социалистической Республики Вьетнам (СРВ), Российской Федерации (РФ) и других стран киберпреступления можно определить как широкий спектр преступной деятельности, которые осуществляются с использованием цифровых устройств и/или сетей. В

информационном пространстве киберпреступности вычислительное устройство может быть как целью преступления, так и инструментом для совершения преступления.

Согласно положениям Уголовного кодекса СРВ, Уголовного кодекса РФ и Уголовного кодекса Азербайджанской Республики, киберпреступление — это использование киберпро-

странства, информационных технологий или электронных средств для совершения преступлений (табл. 1).

Существуют и иные преступления, связанные с киберпространством, например мошенничество.

На сегодняшний день каждое государство в той или иной степени подвержено атакам ки-

Таблица 1 / Table 1

**Сравнительный анализ норм уголовного законодательства
СРВ, РФ и Азербайджанской Республики**

**Comparative analysis of criminal law norms in the Socialist Republic of Vietnam,
the Russian Federation and the Republic of Azerbaijan**

Уголовный кодекс СРВ / Criminal Code of the Socialist Republic of Vietnam	Уголовный кодекс РФ / Criminal Code of the Russian Federation	Уголовный кодекс Азербайджанской Республики / Criminal Code of the Republic of Azerbaijan
Статья 285. Производство, покупка, продажа, обмен или дарение инструментов, оборудования и программного обеспечения для использования в незаконных целях	Статья 272. Неправомерный доступ к компьютерной информации	Статья 271. Неправомерный доступ к компьютерной системе
Статья 286. Распространение программ информационных технологий, наносящих вред работе компьютерных сетей, телекоммуникационных сетей и электронных носителей	Статья 273. Создание, использование и распространение вредоносных компьютерных программ	Статья 272. Неправомерное за- владение компьютерной инфор- мацией
Статья 287. Препятствование или нарушение работы компьютерных сетей, телекоммуникационных сетей и электронных средств массовой информации	Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации	Статья 273. Неправомерное вмешательство в компьютерную систему или компьютерную информацию
Статья 288. Незаконная передача или использование информации в компьютерных сетях и сетях телекоммуникаций	Статья 274.2. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования	Статья 273-1. Оборот средств, изготовленных для совершения киберпреступлений
Статья 289. Несанкционированный доступ в компьютерную сеть, телекоммуникационную сеть или электронные средства другого лица		Статья 273-2. Фальсификация компьютерных данных
Статья 290. Использование компьютерных сетей, сетей телекоммуникаций и электронных средств для совершения актов присвоения имущества		

Окончание табл. 1 / The End of the Table 1

Уголовный кодекс СРВ / Criminal Code of the Socialist Republic of Vietnam	Уголовный кодекс РФ / Criminal Code of the Russian Federation	Уголовный кодекс Азербайджанской Республики / Criminal Code of the Republic of Azerbaijan
Статья 291. Незаконный сбор, хранение, обмен, торговля и разглашение информации о банковских счетах		
Статья 293. Незаконное использование радиочастот исключительно в целях чрезвычайной ситуации, обеспечения безопасности, поиска, спасения, спасения, национальной обороны и безопасности		
Статья 294. Умышленное создание вредных помех		

берпреступников. Согласно данным «Лаборатории Касперского», топ-10 стран по доле атакованных пользователей выглядит следующим образом¹ (табл. 2).

Также на основе данных «Лаборатории Касперского» был проведен анализ развития информационных угроз по всему миру по кварталам, за период третий квартал 2019 г. — второй квартал 2022 г.² (табл. 3).

При этом в третьем квартале 2023 г. решения «Лаборатории Касперского» предотвратили запуск вредоносных программ, предназначенных для кражи денежных средств с банковских

счетов, на компьютерах 76 551 уникального пользователя³.

Согласно отчету, опубликованному Вьетнамской национальной компанией по технологиям кибербезопасности (NCS), количество кибератак на учреждения и организации СРВ в 2023 г. увеличилось на 9,5 % по сравнению с 2022 г. В среднем происходит 1 160 кибератак в месяц⁴. По статистическим данным Министерства общественной безопасности СРВ, в 2023 г. правоохранительными органами возбуждено

1 Данные Kaspersky Security Network. URL: <https://securelist.ru/it-threat-evolution-q2-2023-non-mobile-statistics/107861>.

2 Данные Kaspersky Security Network. URL: <https://securelist.ru/it-threat-evolution-in-q1-2022-mobile-statistics/105235>.

3 Данные Kaspersky Security Network. URL: <https://securelist.ru/it-threat-evolution-q3-2023-non-mobile-statistics/108475> (дата обращения: 18.12.2023).

4 Nguyễn Thu. Năm 2023: số vụ tấn công mạng nhắm vào các hệ thống tại Việt Nam tăng 9,5 %. URL: <https://m.antoanthongtin.gov.vn/an-toan-thong-tin/nam-2023-so-vu-tan-cong-mang-nham-vao-cac-he-thong-tai-viet-nam-tang-95-109609>.

Таблица 2 / Table 2

Топ-10 стран по доле атакованных пользователей
Top 10 countries by the share of attacked users

Страна / Country	Доля атакованных пользователей, % / Share of attacked users, %
Афганистан / Afghanistan	3,9
Туркменистан / Turkmenistan	3,5
Китай / China	2,4
Таджикистан / Tajikistan	2,1
Йемен / Yemen	1,7
Египет / Egypt	1,5
Таиланд / Thailand	1,5
Венесуэла / Venezuela	1,4
Сирия / Syria	1,4
Парагвай / Paraguay	1,3

Таблица 3 / Table 3

**Развитие информационных угроз по всему миру по кварталам (Q)
за период третий квартал 2019 г. — второй квартал 2022 г.**

**Global dynamics of information threats by quarter (Q),
in the third quarter of 2019 — second quarter of 2022**

Квартал / Quarter	Мобильные угрозы / Mobile threats	Новые модификации шифровальщиков / New modifications of encryptors	Мобильные бан- ковские троянцы / Mobile bank Trojans	Мобильные троянцы- вымогатели / Mobile Trojans- extortionists
Q3 2019	1 598 196	13 693	19 748	108 073
Q4 2019	1 479 967	18 305	13 606	17 355
Q1 2020	1 322 578	5 236	18 912	8 787
Q2 2020	1 744 244	7 620	61 045	14 119
Q3 2020	1 305 015	5 195	55 101	13 075
Q4 2020	1 001 019	8 632	18 501	24 020
Q1 2021	905 174	5 222	29 841	27 928
Q2 2021	753 550	16 017	13 899	23 294
Q3 2021	870 617	13 138	13 129	13 179
Q4 2021	980 993	17 686	15 410	5 406
Q1 2022	1 152 662	5 225	42 115	4 339
Q2 2022	1 245 894	4 406	38 951	3 805
Темп роста Q2 2022 к Q3 2019, %	78	32	197	4

1 600 уголовных дел, связанных с киберпреступлениями (рост на 203,61 % по сравнению с 2022 г.), задержано 478 лиц (больше на 48,91 % по сравнению с 2022 г.)⁵. В частности, правоохранительными органами СВБ были раскрыты и расследованы многие уголовные дела, связанные с киберпреступлениями, совершенные с применением новых методов и способов, а также связанные с мошенническим присвоением имущества, азартными играми, многоуровневым маркетингом, торговлей виртуальной валютой, золотом, иностранной валютой и ценными бумагами, торговлей людьми, брокерской проституцией, незаконным оборотом наркотиков и т.д. в киберпространстве.

Интересен сравнительный анализ количества совершенных и раскрытых преступлений подобного рода в РФ (рис.).

Стабильный рост количества совершенных преступлений объясняется все большим вовлечением общества в цифровое пространство, которое становится удобной площадкой для совершения преступных деяний. А поскольку это пространство не находится в ведении отдель-

ного государства, в нем, как справедливо отмечается исследователями, еще недостаточно эффективен контроль за содержательной направленностью информационного контента, что открывает достаточно широкие возможности для противозаконной деятельности [1, с. 56].

На наш взгляд, прогноз состояния киберпреступности до 2030 г. имеет следующие тенденции:

1. Хакеры усиливают целевые кибератаки (APT), чтобы получить доступ к информации; DDoS-атаки; атаки с использованием вредоносных программ, особенно программ-вымогателей, нацелены на критически важные информационные системы. Целью атак являются агентства, ведомства и крупные экономические корпорации с целью кражи персональных данных, данных клиентов, сведений о документах, составляющих государственную тайну и др.

2. Деятельность по распространению вредной и недостоверной информации в киберпространстве продолжает влиять на все аспекты общественной жизни, серьезно ущемляя законные права и интересы организаций и частных лиц. В ближайшее время эта активность будет возрастать, что потребует от пользователей повышения бдительности и осторожности при доступе к информации в киберпространстве, чтобы не стать жертвами фейковых новостей.

⁵ Hương Giang. Năm 2023: Phạm tội tham nhũng, chức vụ nhiều hơn 51 %. URL: <https://thanhtra.com.vn/phong-chong-tham-nhung/ho-so-tu-lieu/nam-2023-pham-toi-tham-nhung-chuc-vu-nhieu-hon-51-216346.html>.



Динамика совершения и раскрытия преступлений в РФ, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации с 2018 по 2023 г.

Dynamics of committing and solving crimes in the Russian Federation, committed with the use of information-telecommunication technologies or in the sphere of computer information in 2018-2023

3. Мошеннические преступления в Интернете, связанные с присвоением собственности, имеют тенденцию к увеличению, становятся все более сложными и включают в себя множество изощренных методов и способов транснационального характера, нанося большой ущерб организациям и лицам.

4. Распространяются азартные игры и расширяется деятельность игорных организаций посредством финансовых ставок через бинарные опционы «БО».

5. Кредитная деятельность «черного кредита» в киберпространстве с высокими процентными ставками с целью получения нелегальной прибыли представляет собой множество потенциальных угроз безопасности и порядку во многих населенных пунктах по всей стране. В настоящее время в мировом киберпространстве наблюдается тенденция существенного роста заявок на онлайн-кредитование (через сайты, через приложения в GooglePlay, AppStore).

6. Незаконная деятельность с целью присвоения собственности в сфере электронной коммерции продолжает усложняться, субъекты используют социальные сети и платформы электронной коммерции для продажи контрафактных, фальсифицированных и контрабандных товаров, оружия, взрывчатых веществ, нарко-

тических и психотропных средств, поддельных документов.

7. Взрыв интеллектуальных устройств, искусственного интеллекта (ИИ), особенно приложений для смартфонов, станет угрозой сетевой безопасности, социальному порядку и безопасности из-за того, что пользователи предоставляют слишком много прав доступа, а также личную информацию в социальных сетях и приложениях, что способствует присвоению собственности в нарушение закона.

Перечень указанных выше норм доказывает, что государства расценивают задачу противодействия киберпреступности как первоочередную, что неоднократно отмечалось на самом высоком государственном уровне. Например, в своем выступлении на коллегии в 2021 г. председатель Следственного комитета России А.И. Бастрыкин акцентировал внимание руководителей на необходимости противодействия киберпреступлениям в современных условиях с учетом роста числа атак на российские сайты⁶. В марте 2023 г. на расширенном заседании коллегии Генеральной прокуратуры при участии президента РФ В.В. Путина генеральный

⁶ В СК России состоялось заседание коллегии, на котором подведены итоги работы за 2021 год. URL: <https://sledcom.ru/news/item/1661498/?print=1>.

прокурор РФ И.В. Краснов отметил: «...прогрессивное развитие цифровых технологий, включая искусственный интеллект и большие базы данных, к сожалению, влечет за собой разного рода риски, увеличение числа кибератак. ...Очевидна необходимость дальнейшего развития данного направления, усиление его кадрами, обладающими универсальным набором компетенций в юриспруденции, компьютерных технологиях»⁷.

Достаточно пристальное внимание проблемам борьбы с киберпреступностью в условиях цифровизации в последние годы уделяют и ученые. Данные вопросы анализируются комплексно, с точки зрения и криминалистики [2, с. 26–31; 3, с. 12; 4, с. 109–113; 5, с. 24–29; 6, с. 184–191; 7, с. 3–6; 8, с. 19–21; 9; 10, с. 89–95], и криминологии [11, с. 152–154], что, на наш взгляд, является правильным.

Тем не менее процесс раскрытия и расследования киберпреступлений всегда сталкивается со множеством трудностей и ограничений, особенно при сборе электронной криминалистически значимой информации.

В этой связи требуется, как отмечает А.А. Бессонов, пристальное изучение и анализ рассматриваемых преступлений на систематической основе, выявление закономерностей их совершения, разработка новейших и соответствующих реалиям криминалистических способов, приемов и методов противодействия, в том числе, создание цифровой криминалистической модели для сбора электронных доказательств в киберпространстве, что можно расценивать как одну из первоочередных и современных задач [12, с. 3].

Отметим, что криминалистические проблемы расследования киберпреступлений (выделение данного рода преступлений в отдельную группу в системе криминалистической классификации противоправных деяний; описание характеристик отдельных элементов методики их расследования; выявление и раскрытие закономерностей совершения преступлений, обусловленных особенностями использования возможностей технологических процессов сети Интернет; изучение информационно-следовой картины преступных деяний, связанных с виртуальными следами, и др.) рассматривались В.Ю. Агibalовым, М.А. Бабаковой, А.А. Бессоновым, В.Б. Веховым, А.С. Вражновым, А.А. Васильевым, А.Ю. Головиным, В.В. Крыловым,

А.А. Косынкиным, Т.К. Ли, В.А. Мещеряковым, У.А. Мусaeвой, Т.Б. Нгуен, Т.Н. Нгуен, Х.Ч. Нгуен, В.В. Поповой, Д.А. Илюшиным, А.А. Светличным, В.В. Степановым, А.И. Семикаленовой, Т.В. Толстухиной, В.Х. Тью, А.И. Усовым и другими учеными. Научные труды указанных авторов внесли значительный вклад в исследование уголовно-правовых и криминалистических аспектов проблем, связанных с противодействием киберпреступности, и имеют высокую теоретическую и научно-практическую значимость по борьбе с преступностью в целом.

Мы полагаем, что именно криминалистика России внесла наиболее значительный вклад в понимание сущности киберпреступлений, механизма их подготовки, совершения и сокрытия, а также в разработку криминалистических основ расследования преступлений данной категории, так как киберпреступность в современном мире объявлена глобальной международной проблемой, о чем свидетельствуют принятые международные договоренности, предусматривающие совместные шаги в данном направлении. Опасность киберпреступности как для мирового сообщества, так и для России признают и российские правоохранительные органы. Как отмечают некоторые ученые, киберпреступность (преступность в сфере высоких технологий) в настоящее время является одной из наиболее серьезных угроз национальной безопасности Российской Федерации в информационной сфере [13, с. 21]. Об этом свидетельствуют и данные Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД РФ.

Именно российские научные достижения по борьбе с киберпреступностью могут быть положены в основу развития цифровой криминалистической модели для сбора электронных доказательств о киберпреступлениях в мировом пространстве.

Как отмечают многие ученые, основой механизма образования цифровых следов является их электронно-цифровое отображение, происходящее в искусственно созданных материальных средах цифрового пространства — памяти электронных носителей информации средств цифрового взаимодействия, каналах цифровых инфраструктур передачи информации, объединяющих, в том числе и информационно-телекоммуникационные сети и информационные ресурсы [14–17].

В настоящее время возрастает необходимость использования электронных доказа-

⁷ Расширенное заседание коллегии Генеральной прокуратуры 15 марта 2023 г. URL: <http://www.kremlin.ru/events/president/transcripts/70678>.

тельств, поскольку значительная доля человеческого общения осуществляется в сфере информационных технологий. Сбор электронных доказательств является одним из этапов процесса криминалистической деятельности. Важным требованием является создание цифровой криминалистической модели для сбора криминалистически значимой информации.

В процесс собирания электронной информации вовлечено также множество субъектов, так как необходимость создания цифровой криминалистической модели — неизбежное требование самого процесса получения информации, обеспечивающего объективность, полноту и всесторонность.

В процессе разработки и создания цифровой криминалистической модели в деятельности правоохранительных органов следует учитывать следующие вопросы:

1. Создание этой модели неразрывно связано с теоретическими положениями криминалистики по изучению закономерностей подготовки, совершения и раскрытия преступлений, возникновения и существования следов, собирания, исследования, оценки и использования доказательств для предупреждения, раскрытия и расследования преступлений, а также при рассмотрении уголовных дел в судах. Мы полагаем, что разработка цифровой криминалистической модели собирания криминалистически значимой информации должна являться неотъемлемой частью криминалистики.

2. Целью создания данной модели является оптимизация сбора электронных следов преступлений, их преобразование в доказательства при расследовании преступлений в киберпространстве, что в конечном итоге способствует установлению виновного и раскрытию преступления. Мы полностью согласны с мнением А.А. Бессонова, который, отмечая ключевую роль этой модели, писал, что «в достижении цели противодействия киберпреступности она должна позволять анализировать различные специфические объекты цифровой среды, к примеру, фото- и видеоконтент, текстовый контент, нестандартную сетевую активность, паттерны поведения в Интернет-пространстве и т.п. Модель должна являться инструментом установления криминального события того или иного вида по его цифровым следам» [18, с. 59].

3. Одной из важных основ создания этой модели служат достижения науки и техники в

области информационных (цифровых и квантовых) технологий, искусственного интеллекта и т.п. Интеграция этих достижений в криминалистику позволит создать оптимальную модель сбора электронных доказательств в нынешний период цифровизации.

4. Под цифровой криминалистической моделью, на наш взгляд, следует понимать систему криминалистически значимых признаков и их закономерных связей между собой, выраженных в электронном формате. Объектами изучения при создании данной модели должны выступать: преступная деятельность, относящаяся к категории киберпреступлений; различные источники криминалистически значимой информации (прежде всего вновь появляющиеся); «большие данные» как самостоятельное явление современной действительности; собственно цифровая (виртуальная) среда.

В теории и практике некоторых зарубежных стран отмечается единство наук криминалистики и судебной экспертизы. В частности, во Вьетнаме многие ученые понятие судебной экспертизы отождествляют с понятием криминалистики [19; 20]. Тем не менее следует отметить различные предметы этих наук, объекты исследования, цели и задачи. В силу методологической самостоятельности судебной экспертизы во многих странах она признана самостоятельной прикладной юридической наукой. Поэтому ее отождествление с криминалистикой мы считаем несостоятельным. Данная наука обозначена как самостоятельная и в перечне научных специальностей.

В зарубежных журналах опубликовано множество цифровых криминалистических моделей. Мы считаем, что нужно проанализировать необходимость создания данных моделей, а также оценить их преимущества и недостатки, выбрать наиболее подходящую или создать новую модель. Для удобства оценки и анализа модели процесса цифрового расследования мы разделили их на группы, в каждой из которых были выбраны типовые модели (табл. 4).

Следует отметить, что у трех вышеперечисленных групп моделей имеется один существенный недостаток — отсутствие единой терминологии. В каждой модели используется разная терминология и разные объяснения [33, с. 77]. Таким образом, проведенный выше анализ обосновывает необходимость создания типовой цифровой криминалистической модели для решения обозначенных проблем.

Таблица 4 / Table 4

Современные цифровые криминалистические модели
Contemporary digital criminalistic models

№	Группа цифровых криминалистических моделей / Group of digital criminalistic models	Цифровая криминалистическая модель / Digital criminalistic model	Оценка / Assessment
1	Группа «Общие цифровые криминалистические модели» для всех уголовных дел. Эта группа моделей определяет этапы и подэтапы расследования	<p>1. Цифровая модель осмотра места преступления — Scientific Crime Scene Investigation model [21]. Она включает в себя следующие этапы:</p> <ul style="list-style-type: none"> – распознавание; – идентификация; – индивидуализация; – реконструкция. <p>2. Цифровой интегрированный процесс расследования — Integrated Digital Investigation Process (IDIP) [22]. Включает в себя следующие этапы:</p> <ul style="list-style-type: none"> – подготовка; – развертывание; – физическое расследование + цифровое расследование; – оценка. <p>3. Цифровая модель судебной экспертизы — Modelling of Digital Forensic Process Models (DFPM) [23]. Включает в себя следующие этапы:</p> <ul style="list-style-type: none"> – распознавание инцидентов; – оценка; – идентификация и изъятие; – сохранение; – исследование; – анализ; – отчетность. <p>4. Расширенный цифровой интегрированный процесс расследований — The Enhanced Digital Investigation Process Model (EIDIP) [24]. Подразумевает следующие этапы:</p> <ul style="list-style-type: none"> – подготовка; – развертывание; – обратная связь; – анализ. <p>5. Цифровая модель судебной экспертизы — The NIJ Digital Forensic Examination [25]. Включает следующие этапы:</p> <ul style="list-style-type: none"> – идентификация; – сбор; – перевозка; – хранение; – проверка и поиск следов; – представление; – разрушение 	<p>Модели группы 1 являются базовыми, в основном выполняются последовательно и не демонстрируют повторяемости (в криминалистике повторяемость моделей имеет важное значение). Модель этой группы также не отвечает потребностям сбора электронных доказательств, что является центром криминалистики на различных технологических платформах, а также не решает проблем, связанных с природой электронных доказательств каждого типа электронных данных. Модель группы 1 не демонстрирует реализацию электронного сбора доказательств в соответствии с требованиями законодательства</p>
2	Группа моделей по этапам расследования конкретных видов преступлений	<p>1. Расширенная модель расследования киберпреступлений — An Extended Model of Cybercrime Investigations [26]. Содержит следующие этапы: осведомленность, разрешение, планирование, уведомление, поиск и выявление доказательств, сбор доказательств, перевозка доказательств, хранение доказательств, проверка гипотезы, представление гипотезы, доказывание/защита гипотезы, распространение информации;</p>	<p>Модели группы 2 глубже демонстрируют различные сильные стороны каждой модели, не принимая во внимание технологические и правовые требования.</p>

Окончание табл. 4 / The End of the Table 4

№	Группа цифровых криминологических моделей / Group of digital criminalistic models	Цифровая криминологическая модель / Digital criminalistic model	Оценка / Assessment
		<p>2. Цифровая модель процесса судебно-экспертной сортировки — Digital Forensic Triage Process Model [27]. Включает этапы: планирование, исследование, использование технических средств и методов, профиль пользователя, оценка полученных результатов.</p> <p>3. Цифровая судебная модель процесса расследования в Малайзии — Digital Forensic Model Based On Malaysian Investigation Process [28]. Включает в себя следующие этапы: планирование, идентификация, разведка, анализ, результаты, доказывание и защита, распространение информации.</p> <p>4. Системная цифровая модель судебной экспертизы и криминологии — Systematic Digital Forensic Investigation Model (SRDFIM) [29]. Составляет из следующих этапов: подготовка, охрана места происшествия, обследование и документирование, запись места происшествия, изоляция СМИ, сбор электронных доказательств, сохранение, тестирование, анализ, презентация, результаты и оценка.</p> <p>5. Цифровой интегрированный режим судебной экспертизы — Integrated Digital Forensic Process Mode [30]. Включает в себя этапы:</p> <ul style="list-style-type: none"> – подготовка; – обнаружение инцидентов; – реагирование на инциденты; – судебно-экспертное исследование; – оценка; – представление 	
3	Группа цифровых криминологических моделей во многих других средах по технологическим и законодательным требованиям	<p>1. Мультидисциплинарная модель судебной экспертизы — A multidisciplinary digital forensic investigation process model [31]. Данная модель создается на основе мобильных устройств, связанных с компьютерными средами, компьютерными сетями, облаками и виртуальными компьютерами.</p> <p>2. Стандартизированная модель судебной экспертизы — The Standardised Digital Forensic Investigation Process Model (SDFIPM) [32]. Данная модель применяется от этапа сбора электронных доказательств до этапа их представления, что является в ней циклическим процессом. Каждый этап — это отдельный процесс</p>	<p>Модели группы 3 являются прогрессивными, отвечающими требованиям мультитехнологической платформы и правовым требованиям, но упоминаются в каждой модели отдельно. Например, модель MDFIPM демонстрирует криминологию на цифровой мультитехнологической платформе, но она все еще находится в зачаточном состоянии; тем более что правовые требования в настоящее время еще не разработаны. Модель SDFIPM пока не полностью отвечает требованиям нескольких технологических платформ, а ее этапы представляют собой процесс, начинать который со стадии тестирования нецелесообразно</p>

Создание цифровой криминалистической модели является актуальной проблемой для сбора электронных доказательств. Необходимость в разработке модели абстрактного уровня обусловлена целью сбора электронных доказательств. Эта модель отражает интеграционный процесс юридических наук уголовно-правового цикла (оперативно-розыскная деятельность, криминалистика, судебно-экспертная деятельность, криминология, уголовный процесс и др.) и базируется на существующих технологических платформах с целью сбора электронных доказательств.

Цифровая криминалистическая модель для сбора электронных доказательств при расследовании киберпреступлений включает в себя этапы (элементы), представленные в табл. 5.

Следует констатировать, что приведенная модель не является оптимальной, однако ее разработка обеспечит эффективность раскрытия и расследования киберпреступлений.

Подводя итог сказанному, можно сделать вывод, что киберпреступления относятся к преступлениям высокого интеллектуального уровня. Следовательно, в настоящее время одной из самых больших сложностей в борьбе с киберпреступностью является проблема сбора электронных доказательств. Данный процесс должен осуществляться интеграционно квалифицированными специалистами в сфере информационных технологий и на основе достижений современной науки и техники, информатики, информационных технологий, искусственного интеллекта, Интернета и др.

Таблица 5 / Table 5

Этапы (элементы) цифровой криминалистической модели для сбора электронных доказательств при расследовании киберпреступлений
Stages (elements) of the digital criminalistic model for the collection of electronic evidence in the investigation of cybercrimes

№	Название этапа (элемента) / Name of stage (element)	Организационно-тактические действия / Organizational and tactical actions
1	Оперативно-розыскное обеспечение сбора электронных доказательств	На данном этапе необходимо осуществлять следующие оперативно-розыскные мероприятия, обеспечивающие сбор электронных доказательств: опрос; наведение справок; исследование предметов и документов; наблюдение; отождествление личности; обследование помещений, зданий, сооружений, участков местности и транспортных средств; контроль почтовых отправлений, телеграфных и иных сообщений; прослушивание телефонных переговоров; снятие информации с технических каналов связи; оперативное внедрение и др.
2	Обеспечение сбора электронных доказательств при помощи следственных действий	На данном этапе нужно осуществлять следующие следственные действия: осмотр места происшествия, обыск, выемка, допрос, следственный эксперимент в киберпространстве, сбор образцов для сравнительного исследования, назначение судебной экспертизы и др. Организационный этап собирания электронных следов должен осуществляться на всех стадиях: при подготовке, охране места происшествия, документировании, фото- и видеофиксации места происшествия, обеспечении сохранности электронных следов (доказательств) и др.
3	Обеспечение сбора электронных доказательств при помощи специальных знаний	Основными формами использования специальных знаний при расследовании киберпреступлений являются: участие специалиста в следственных действиях (см. 2-й этап), а также производство судебной экспертизы. В зависимости от обстоятельств дела могут назначаться следующие виды компьютерно-технической экспертизы: аппаратно-компьютерная; программно-компьютерная; информационно-компьютерная; компьютерно-сетевая экспертиза

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Girard J. Criminalistics: Forensic Science, Crime and Terrorism / J. Girard. — Jones, Bartlett Publishers, 2011. — 520 p.
2. Бычков В.В. К вопросу об актуальности научных исследований проблем противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационных сетей / В.В. Бычков. — EDN WAYXAI // Проблемы противодействия киберпреступности : материалы Междунар. науч.-практ. конф., Москва, 28 апр. 2023 г. — Москва, 2023. — С. 26–31.
3. Цифровые следы преступлений / А.М. Багмет, В.В. Бычков, С.Ю. Скобелин, Н.Н. Ильин. — Москва : Проспект, 2023. — 168 с. — EDN MDHESX.

4. Толстухина Т.В. Формализация научного криминалистического и судебно-экспертного знания в условиях цифровизации / Т.В. Толстухина, И.В. Устинова. — EDN HCRSFD // Криминалистика и судебная экспертиза: наука, практика, опыт : сб. науч. тр. / сост. И.В. Тишутина. — Москва, 2021. — С. 109–113.
5. Светличный А.А. Новации в терминологическом аппарате криминалистики: потребность науки и практики или дань моде? / А.А. Светличный. — DOI 10.18572/1813-1190-2022-5-24-29. — EDN OOTAPL // Юридическое образование и наука. — 2022. — № 5. — С. 24–29.
6. Светличный А.А. Эволюционные процессы терминологического аппарата криминалистики: всегда ли все закономерно? / А.А. Светличный. — DOI 10.51965/20767919_2022_1_3_184. — EDN VGJAGT // Вестник Волжского университета им. В.Н. Татищева. — 2022. — Т. 1, № 3 (102). — С. 184–191.
7. Рудых А.А. Трансформация криминалистической и преступной деятельности в условиях развития информационных технологий / А.А. Рудых. — DOI 10.18572/1812-3783-2020-2-3-6. — EDN QDOOZO // Российский следователь. — 2020. — № 2. — С. 3–6.
8. Усачева Е.А. Особенности преступной деятельности, совершаемой с использованием информационно-телекоммуникационных технологий в сфере железнодорожной транспортной инфраструктуры / Е.А. Усачева. — EDN HSQNSU // Глаголь правосудия. — 2022. — № 2. — С. 19–21.
9. Головин А.Ю. Актуальные проблемы расследования преступлений в сфере компьютерной информации / А.Ю. Головин, У.А. Мусаева, Т.В. Толстухина. — Тула : Изд-во Тульского гос. ун-та, 2001. — 108 с.
10. Давыдов В.О. Цифровое пространство как место совершения преступлений экстремистской направленности / В.О. Давыдов. — DOI 10.17150/2500-4255.2024.18(1).89-95. — EDN ZCLINS // Всероссийский криминологический журнал. — 2024. — Т. 18, № 1. — С. 89–95.
11. Кравцов Д.А. Латентная преступность в сети «Интернет» и ее детерминанты / Д.А. Кравцов, Т.А. Дворникова, Ю.А. Колесинская. — EDN CUGPVQ // Advanced Science : материалы VIII Междунар. науч.-практ. конф. Пенза, 23 мая 2019 г. : в 2 т. — Пенза, 2019. — Т. 2. — С. 152–154.
12. Бессонов А.А. Частная теория криминалистической характеристики преступлений : автореф. дис. ... д-ра юрид. наук : 12.00.12 / А.А. Бессонов. — Москва, 2017. — 45 с.
13. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений : дис. ... канд. юрид. наук : 12.00.12 / Е.С. Шевченко. — Москва, 2016. — 249 с.
14. Brian J. Network File System Forensic Analysis / J. Brian. — London : Addison-Wesley Professional, 2005. — 600 p.
15. Easttom C. Digital Forensics, Investigation and Response / C. Easttom. — Jones, Bartlett Learning, 2021. — 403 p.
16. Nelson B. Guide to Computer Forensics and Investigations / B. Nelson, C. Steuart, A. Phillips. — Course Technology, 2018. — 688 p.
17. Ham J. Network Forensics: Tracking Hackers through Cyberspace / J. Ham, S. Davidoff. — Pearson Education, 2012. — 576 p.
18. Бессонов А.А. Цифровая криминалистическая модель преступления как основа противодействия киберпреступности / А.А. Бессонов. — EDN CHQQUAU // Академическая мысль. — 2020. — № 4 (13). — С. 58–61.
19. Usoff Y. Common Phases of Computer Forensics Investigation Models / Yu. Yusoff, R. Ismail, Z. Hassan // International Journal of Computer Science and Information Technology. — 2011. — Vol. 3, no. 3. — URL: <https://www.airccse.org/journal/jcsit/0611csit02.pdf>.
20. Du X. Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service / X. Du, K.N.A. Le, M. Scanlon // Computer Science. — 2017. — URL: <https://doi.org/10.48550/arXiv.1708.01730>.
21. The Green Revolution: Botanical Contributions to Forensics and Drug Enforcement / H. Miller Coyle, C. Ladd, T. Palmbach, H.C. Lee // Croat Med J. — 2001. — No. 42. — P. 340–345.
22. Carrier B. Getting Physical with the Digital Investigation Process / B. Carrier, E.H. Spafford // International Journal of Digital Evidence. — 2003. — Vol. 2, iss. 2. — URL: https://www.researchgate.net/publication/220542528_Getting_Physical_with_the_Digital_Investigation_Process.
23. Michal Köhn. Modelling of Digital Forensic Process Models (DFPMs) / Michal Köhn, Jan H.P. Eloff, Martin S. Olivier // Conference: Proceedings of the ISSA 2008 Innovative Minds Conference, ISSA 2008, Gauteng Region (Johannesburg), South Africa, 7–9 July 2008. — URL: https://www.researchgate.net/publication/220803382_UML_Modelling_of_Digital_Forensic_Process_Models_DFPMs.
24. Baryamureeba V. The Enhanced Digital Investigation Process Model (EIDIP) / V. Baryamureeba, F. Tushabe // ResearchGate. — 2004. — URL: https://dfrws.org/wpcontent/uploads/2019/06/2004_USA_paper_the_enhanced_digital_investigation_process_model.pdf.
25. Cohen F. The NIJ Digital Forensic Examination / F. Cohen. — ASP Press, 2009. — 504 p.
26. Ciardhuáin S.Ó. An Extended Model of Cybercrime Investigations / S.Ó. Ciardhuáin // ResearchGate. — 2004. — URL: https://www.researchgate.net/publication/220542517_An_Extended_Model_of_Cybercrime_Investigations.
27. Computer Forensics Field Triage Process Model / M.K. Rogers, J. Goldman, R. Mislan [et al.]. — DOI 10.15394/jdf-sl.2006.1004 // Forensics, Security and Law. — 2006. — Vol. 1 (2). — P. 19–37.
28. Sundresan Perumal. Digital Forensic Model Based on Malaysian Investigation Process / Sundresan Perumal // Journal of Computer Science and Network Security. — 2009. — Vol. 9, no. 8. — P. 38–44.
29. Systematic Digital Forensic Investigation Model / A. Agarwal, M. Gupta, S. Gupta, S.C. Gupta // ResearchGate. — 2011. — URL: https://www.researchgate.net/publication/228410430_Systematic_Digital_Forensic_Investigation_Model.
30. Kohn M.D. Integrated Digital Forensic Process Mode / M.D. Kohn, M. Eloff, J. Eloff // Computers & security. — 2013. — URL: <https://doi.org/10.1016/j.cose.2013.05.001>.
31. Lutui R. A Multidisciplinary Digital Forensic Investigation Process Model / R. Lutui. — DOI 10.1016/j.bushor.2016.08.001 // Business Horizons. — 2016. — Vol. 59 (6). — P. 593–604.

32. The Standardised Digital Forensic Investigation Process Model (SDFIPM) / Reza Montasari, Richard Hill, Victoria Carpenter, Amin Hosseini-Far // *Blockchain and Clinical Trial* / Hamid Jahankhani, Stefan Kendzierskyj, Arshad Jamal, Gregory Epiphaniou, Haider Al-Khateeb (eds.). — Springer, 2019. — P. 169–209.

33. Lê Tấn Quân. Pháp luật Việt Nam về chứng cứ điện tử. Luận án tiến sĩ, Trường Đại học Kinh tế TP. — Hồ Chí Minh, 2022. — URL: <https://digital.lib.ueh.edu.vn/handle/UEH/65599>. [Ле Тан Куан. Вьетнамский закон об электронных доказательствах : дис. д-ра / Ле Тан Куан. — Хошимин, 2022. — URL: <https://digital.lib.ueh.edu.vn/handle/UEH/65599>].

REFERENCES

1. Girard J. *Criminalistics: Forensic Science, Crime and Terrorism*. Jones, Bartlett Publishers, 2011. 520 p.
2. Bychkov V.V. On the Relevance of Researching the Problems of Counteracting Extremist Crimes Committed with the Use of Information-Telecommunication Networks. *Problems of Counteracting Cybercrime. Materials of International Scientific Conference, Moscow, April 28, 2023*. Moscow, 2023, pp. 26–31. (In Russian). EDN: WAYXAI.
3. Bagmet A.M., Bychkov V.V., Skobelin S.Yu., Il'in N.N. *Digital Traces of Crime*. Moscow, Prospekt Publ., 2023. 168 p. EDN: MDHESX.
4. Tolstukhina T.V., Ustinova I.V. Formalization of Scientific Criminalistic and Forensic Knowledge in the Conditions of Digitization. In Tishutina I.V. (ed.). *Criminalistics and Forensic Expertise: Science, Practice, Experience. Collected Papers*. Moscow, 2021, pp. 109–113. (In Russian). EDN: HCRSFD.
5. Svetlichny A.A. Novelties in the Terminology of Criminalistics: A Requirement of Science and Practice or a Tribute to Fashion? *Yuridicheskoe obrazovanie i nauka = Juridical Education and Science*, 2022, no. 5, pp. 24–29. (In Russian). EDN: OOTAPL. DOI: 10.18572/1813-1190-2022-5-24-29.
6. Svetlichny A.A. Evolutionary Processes of the Terminological Apparatus of Criminology: Is Everything Always Natural? *Vestnik Volzhskogo universiteta im. V.N. Tatishcheva = Vestnik of Volzhsky University after V.N. Tatishchev*, 2022, vol. 1, no. 3, pp. 184–191. (In Russian). EDN: VGJAGT. DOI: 10.51965/20767919_2022_1_3_184.
7. Rudykh A.A. Transformation of Criminalistic and Criminal Activities in the Information Technology Development Conditions. *Rossiiskii sledovatel' = Russian Investigator*, 2020, no. 2, pp. 3–6. (In Russian). EDN: QDOOZO. DOI: 10.18572/1812-3783-2020-2-3-6.
8. Usacheva E.A. Features of Criminal Activity Completed With the Use of Information and Telecommunication Technologies in the Sphere of Railway Transport Infrastructure. *Glagol Pravosudiya = The Verb of Justice*, 2022, no. 2, pp. 19–21. (In Russian). EDN: HSQNSU.
9. Golovin A.Yu., Musaeva U.A., Tolstukhina T.V. *Topical Problems of Investigating Crimes in the Sphere of Computer Information*. Tula State University Publ., 2001. 108 p.
10. Davydov V.O. Digital Space as a Scene of Extremist Crimes. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2024, vol. 18, no. 1, pp. 89–95. (In Russian). DOI: 10.17150/2500-4255.2024.18(1).89-95. EDN: ZCLINS.
11. Kravtsov D.A., Dvornikova T.A., Kolesinskaya Yu.A. Latent Crime in a Network "The Internet" and its Determinants. *Advanced Science. Materials of the VIII International Scientific Conference, Penza, May 23, 2019*. Penza, 2019. Vol. 2. Pp. 152–154. (In Russian). EDN: CUGPVQ.
12. Bessonov A.A. *Special Theory of Criminalistic Description of Crimes. Doct. Diss. Thesis*. Moscow, 2017. 45 p.
13. Shevchenko E.S. *The Tactics of Investigative Actions in the Investigation of Cybercrimes. Cand. Diss.* Moscow, 2016. 249 p.
14. Brian J. *Network File System Forensic Analysis*. London, Addison-Wesley Professional, 2005. 600 p.
15. Easttom C. *Digital Forensics, Investigation and Response*. Jones, Bartlett Learning, 2021. 403 p.
16. Nelson B., Steuart C., Phillips A. *Guide to Computer Forensics and Investigations*. Course Technology, 2018. 688 p.
17. Ham J., Davidoff S. *Network Forensics: Tracking Hackers through Cyberspace*. Pearson Education, 2012. 576 p.
18. Bessonov A.A. Digital Forensic Crime Model as a Basis for Countering Cybercrime. *Akademicheskaya Mysl' = Academic Thought*, 2020, no. 4, pp. 58–61. (In Russian). EDN: CHQQUA.
19. Usoff Y., Ismail R. Common Phases of Computer Forensics Investigation Models. *International Journal of Computer Science and Information Technology*, 2011, vol. 3, no. 3. URL: <https://www.airccse.org/journal/jcsit/0611csit02.pdf>.
20. Du X., Le K.N.A., Scanlon M. Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service. *Computer Science*. 2017. URL: <https://doi.org/10.48550/arXiv.1708.01730>.
21. Miller Coyle H., Ladd C., Palmbach T., Lee H.C. The Green Revolution: Botanical Contributions to Forensics and Drug Enforcement. *Croat Med J*, 2001, no. 42, pp. 340–345.
22. Carrier B., Spafford E.H. Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence*, 2003, vol. 2, iss. 2. URL: https://www.researchgate.net/publication/220542528_Getting_Physical_with_the_Digital_Investigation_Process.
23. Eloff J.H.P., Olivier M.S. Modelling of Digital Forensic Process Models (DFPMs). *Conference: Proceedings of the ISSA 2008 Innovative Minds Conference, ISSA 2008, Gauteng Region (Johannesburg), South Africa, 7–9 July 2008*. URL: https://www.researchgate.net/publication/220803382_UML_Modelling_of_Digital_Forensic_Process_Models_DFPMs.
24. Baryamureeba V., Tushabe F. The Enhanced Digital Investigation Process Model (EIDIP). *ResearchGate*, 2004. URL: https://dfrws.org/wpcontent/uploads/2019/06/2004_USA_paper_the_enhanced_digital_investigation_process_model.pdf.
25. Cohen F. *The NIJ Digital Forensic Examination*. ASP Press, 2009. 504 p.
26. Ciardhuain S.Ó. An Extended Model of Cybercrime Investigations. *ResearchGate*, 2004. URL: https://www.researchgate.net/publication/220542517_An_Extended_Model_of_Cybercrime_Investigations.
27. Rogers M.K., Goldman J., Mislan R., Wedge T., Debrota S. Computer Forensics Field Triage Process Model. *Journal of Digital Forensics, Security and Law*, 2006, Vol. 1 (2), pp. 19–37. DOI:10.15394/jdfl.2006.1004.
28. Sundresan Perumal. Digital Forensic Model Based On Malaysian Investigation Process. *Journal of Computer Science and Network Security*, 2009, vol. 9, no. 8, pp. 38–44.
29. Agarwal A., Gupta M., Gupta S., Gupta S.C. Systematic Digital Forensic Investigation Model. *ResearchGate*, 2011. URL: https://www.researchgate.net/publication/228410430_Systematic_Digital_Forensic_Investigation_Model.

30. Kohn M.D., Eloff M., Eloff J. Integrated Digital Forensic Process Mode. *Computers & Security*, 2013. URL: <https://doi.org/10.1016/j.cose.2013.05.001>.
31. Lutui R. A Multidisciplinary Digital Forensic Investigation Process Model. *Business Horizons*, 2016, vol. 59 (6), pp. 593–604. DOI: 10.1016/j.bushor.2016.08.001.
32. Montasari R., Hill R., Carpenter V., Hosseinian-Far A. The Standardised Digital Forensic Investigation Process Model (SD-FIPM). In Hamid Jahankhani, Stefan Kendzierskyj, Arshad Jamal, Gregory Epiphaniou, Haider Al-Khateeb (eds.). *Blockchain and Clinical Trial*. Springer, 2019, pp. 169–209.
33. Le Tan Quan. *Vietnamese law on electronic evidence. Doct. Diss*, Ho Chi Minh City, 2022. URL: <https://digital.lib.ueh.edu.vn/handle/UEH/65599>.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Мусаева Улдуз Алияровна — старший преподаватель кафедры права Академии государственного управления при Президенте Азербайджанской Республики, кандидат юридических наук, г. Баку, Азербайджанская Республика; e-mail: dia.121@mail.ru.

Нгуен Тхи Бинь — заведующий кафедрой уголовного права Юридического университета Хюэ, кандидат юридических наук, г. Хюэ, Социалистическая Республика Вьетнам; e-mail: law245@gmail.com.

Нгуен Тхи Хуен Чанг — адвокат, член Федерации адвокатов Вьетнама, директор юридической фирмы «Вьен Ань», кандидат юридических наук, г. Ханой, Социалистическая Республика Вьетнам; e-mail: tranglawyer1972@gmail.com.

Светличный Александр Алексеевич — заведующий кафедрой судебной экспертизы и таможенного дела Тульского государственного университета, кандидат юридических наук, доцент, г. Тула, Российская Федерация; e-mail: alexandrsvetl@rambler.ru.

Толстухина Татьяна Викторовна — профессор кафедры судебной экспертизы и таможенного дела Тульского государственного университета, доктор юридических наук, профессор, г. Тула, Российская Федерация; e-mail: tat_tolstuhina@mail.ru.

Тью Ван Хунг — преподаватель юридического факультета Академии социальных наук, кандидат юридических наук, г. Ханой, Социалистическая Республика Вьетнам; e-mail: chuvanhung051092@gmail.com.

ВКЛАД АВТОРОВ

Все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

ДЛЯ ЦИТИРОВАНИЯ

К вопросу о создании цифровой криминалистической модели для сбора электронных доказательств при расследовании киберпреступлений / У.А. Мусаева, Т.Б. Нгуен, Т.Х.Ч. Нгуен, А.А. Светличный, Т.В. Толстухина, В.Х. Тью. — DOI 10.17150/2500-4255.2024.18(4).398-411. — EDN GEFZJT // Всероссийский криминологический журнал. — 2024. — Т. 18, № 4. — С. 398–411.

INFORMATION ABOUT THE AUTHORS

Musayeva, Ulduz A. — Senior Lecturer, Department of Law, Academy of Public Administration under the President of the Republic of Azerbaijan, Ph.D. in Law, Baku, the Republic of Azerbaijan; e-mail: dia.121@mail.ru.

Nguyen, Thi Binh — Head, Department of Criminal Law, Hue University of Law, Ph.D. in Law, the Socialist Republic of Vietnam; e-mail: law245@gmail.com.

Nguyen, Thi Huen Chang — Lawyer, Vietnam Bar Federation, Director, Vien Anh Law Firm, Ph.D. in Law, Hanoi, the Socialist Republic of Vietnam; e-mail: tranglawyer1972@gmail.com.

Svetlichny, Alexander A. — Head, Department of Forensic Examination and Customs Affairs, Tula State University, Ph.D. in Law, Ass. Professor, Tula, the Russian Federation; e-mail: alexandrsvetl@rambler.ru.

Tolstukhina, Tatyana V. — Professor, Department of Forensic Examination and Customs Affairs, Tula State University, Doctor of Law, Professor, Tula, the Russian Federation; e-mail: tat_tolstuhina@mail.ru.

Tew, Van Hung — Lecturer, Faculty of Law, Academy of Social Sciences, Ph.D. in Law, Hanoi, the Socialist Republic of Vietnam; e-mail: chuvanhung051092@gmail.com.

CONTRIBUTION OF THE AUTHORS

The authors contributed equally to this article. The authors declare no conflicts of interests.

FOR CITATION

Musayeva U.A., Nguyen T.B., Nguyen H.C., Svetlichny A.A., Tolstukhina T.V., Tew V.H. On the Issue of Creating a Digital Forensic Model for Collecting Electronic Evidence in the Investigation of Cybercrimes. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2024, vol. 18, no. 4, pp. 398–411. (In Russian). EDN: GEFZJT. DOI: 10.17150/2500-4255.2024.18(4).398-411.