Научная статья
УДК 343.98

Криминалистическая кодификация преступлений в сфере компьютерной информации и ее роль в унификации процесса расследования

Зарина Ирековна Харисова, кандидат технических наук, доцент

Уфимский юридический институт МВД России
Уфа (450103, ул. Муксинова, д. 2), Российская Федерация
Уфимский университет науки и технологий
Уфа (450076, ул. Заки Валиди, д. 32), Российская Федерация
zarinaid@mail.ru
https://orcid.org/0000-0002-3902-3459

Аннотация:
Введение. *В настоящее время преступления в сфере компьютерной информации отличаются не только широкой распространенностью, но и своим многообразием, что обусловлено использованием преступниками большого спектра высокотехнологичных средств и способов совершения преступных деяний. Имеющиеся правовые механизмы и методики расследования указанных преступлений зачастую не успевают адаптироваться под их эволюцию и трансформацию. Необходимо найти возможность для анализа обстоятельств криминального деяния и систематизации сведений о нем, чтобы сформировать максимально эффективную методику расследования. Рассматриваемый вид преступлений благодаря своей связи с цифровой формой информации может способствовать формированию принципиально новой системы унификации процесса расследования: присвоению криминальным актам уникальных кодов, однозначно идентифицирующих как распространенные в настоящее время, так и вновь появляющиеся средства и способы совершения преступных деяний во всем их многообразии.*
Методы. *Для обобщения и анализа эмпирического материала в рамках исследования использовался ряд общих методов научного познания (описание, обобщение и сравнение), а также совокупность общенаучных и частнонаучных методов (анализ, синтез, моделирование, формализация, описание, обобщение, сравнение, классификация и пр.).*
Результаты. *Предложена система кодификации преступлений в сфере компьютерной информации, использование которой может стать основой формирования эффективных методик их расследования в условиях постоянной трансформации способов совершения преступных деяний. Предлагаемый подход будет способствовать разработке новых и совершенствованию существующих технико-криминалистических средств на основе технологий искусственного интеллекта и методов анализа больших и разнородных данных, выступая связующим звеном между юридическими и техническими аспектами расследования.*

Ключевые слова:
кодификация преступлений, компьютерные преступления, киберпреступления, алгоритмизация расследования, унификация расследования, технико-криминалистические средства

Для цитирования:
Харисова З. И. Кодификация преступлений в сфере компьютерной информации и ее роль в унификации процесса расследования // Вестник Санкт-Петербургского университета МВД России. 2025. № 4 (108). С. 164–172.

**Статья поступила в редакцию 23.07.2025;
одобрена после рецензирования 30.09.2025;
принята к публикации 25.12.2025.**

Original article

Codification of computer information crimes and its role in unifying the investigation process

Zarina I. Kharisova, Cand. Sci. (Techn.), Docent

Ufa Law Institute of the MIA of Russia
2, Muksinova str., Ufa, 450103, Russian Federation
Ufa University of Science and Technology
32, Zaki Validi str., Ufa. 450076, Russian Federation
zarinaid@mail.ru
https://orcid.org/0000-0002-3902-3459

ISSN 2949-1150 (online)
2071-8284 (print)

Abstract:
Introduction. *Nowadays, crimes in the field of computer information are both pervasive and multifaceted. This is largely due to a broad spectrum of high-tech tools and methods of committing criminal acts used by criminals. Current legal tools, mechanisms and investigation techniques often fall short in adapting to the fast evolution and transformation of the crimes. To develop the most effective investigation techniques, it is essential to devise a method for analysing the circumstances of a criminal act and systematising information about it. Given its connection to digital data, this particular type of crime may potentially lead to the formation of a new unification system of investigation process: assigning unique codes to criminal acts, thereby ensuring the clear identification of both the currently pervasive and the recently emergent means and methods of committing criminal acts, encompassing their entire spectrum.*
Methods. *In summarising and analysing the empirical material within the framework of the study, general scientific methods of cognition (description, generalisation and comparison) were used, as well as a set of general scientific and private scientific methods (analysis, synthesis, modelling, formalisation, description, generalisation, comparison, classification, etc.).*
The results. *A codification system of crimes in the field of computer information is proposed, the use of which can become the basis for the formation of effective investigation techniques of these crimes in the context of the constant evolution of methods of committing criminal acts. This approach will contribute to the development of new and improved technical-criminalistic tools based on artificial intelligence technologies and big data analysis methods, acting as a link between the legal and technical aspects of the investigation.*

Keywords:
codification of crimes, computer crimes, cybercrime, algorithmisation of investigation, unification of investigation, technical and criminalistic tools

For citation:
Kharisova Z. I. Codification of computer information crimes and its role in unifying the investigation process // Vestnik of Saint Petersburg University of the MIA of Russia. 2025. № 4 (108). P. 164–172.

The article was submitted July 23, 2025; approved after reviewing September 30, 2025; accepted for publication December 25, 2025.

Введение

Эволюция информационных технологий неизменно опережает темпы формирования правовых механизмов, что создает колоссальный разрыв между возможностями преступников и инструментами, доступными правоохранительным органам. Подобный дисбаланс требует адаптации правовых механизмов к динамичной природе преступлений в сфере компьютерной информации, что обеспечит гибкость системы уголовного правосудия в условиях стремительно развивающихся технологий. Следовательно, необходима модернизация отдельных направлений криминалистики в соответствии со способами, средствами и условиями совершаемых преступлений.

Преступления в сфере компьютерной информации – это законодательное определение преступных деяний, предусмотренных главой 28 Уголовного кодекса Российской Федерации[1] (далее – УК РФ), объединяющей ст. 272, 272[1], 273, 274, 274[1], 274[2]. Рассмотрение вопросов противодействия преступлениям в сфере компьютерной информации обусловлено их существенным увеличением за последние несколько лет[2], что преимущественно связано с неправомерным доступом к охраняемой законом информации (ст. 272 УК РФ), ростом утечек конфиденциальных данных, способных нанести ущерб объектам критической информационной инфраструктуры Российской Федерации (ст. 274[1] УК РФ), хищением персональных данных граждан, их неправомерным использованием и распространением (ст. 272[1] УК РФ), противоправным применением информационно-телекоммуникационных технологий организованными преступными группами, которые все чаще используют вредоносное программное обеспечение (ст. 273 УК РФ), нарушением правил эксплуатации технических средств и информационно-телекоммуникационных сетей (ст. 274 УК РФ), а также несоблюдением порядка централизованного управления средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети «Интернет» и сетей связи (ст. 274[2] УК РФ).

Вопросы совершенствования методик расследования преступлений в сфере компьютерной информации, в т. ч. интеграции различных информационных технологий в процесс расследования, в последние годы рассматривались часто и подробно (Е. П. Ищенко, Е. Р. Россинская, В. Я. Колдин, В. Б. Вехов, С. А. Ковалев, А. А. Бессонов, Л. В. Бертовский, А. В. Нестеров, А. Б. Смушкин и др.). Однако рассматриваемые преступления отличаются многообразием и трансформацией с течением времени, что объясняет сложность в определении эффективных мер противодействия им. Стоит также отметить недостаток имеющихся сегодня сведений по систематизации методик расследований в зарубежной литературе (B. Carrier, S. Reyes, J. Hansen, C. Hooper,

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 24.06.2025) // Собрание законодательства Российской Федерации (далее – СЗ РФ). 1996. № 25. Ст. 2954.

[2] Комплексный анализ состояния преступности в Российской Федерации по итогам 2024 года и ожидаемые тенденции ее развития : аналитический обзор / Гончарова М. В., Бабаев М. М., Черкасов Р. В. [и др.]. Москва : ВНИИ МВД России, 2025. С. 54.

P. Hunton, V. Kebande, I. Yaqoob, P. Sharma A. Harisha и др.). Часть исследований по решению имеющихся проблем носит шаблонный, односторонний характер. Часто при выявлении тех или иных особенностей расследования преступлений в сфере компьютерной информации изучается лишь отдельно взятое преступное деяние. Как следствие, формируется узконаправленная методика расследования именно рассмотренного криминального акта. Вопросы интеграции информационных технологий в процесс расследования часто носят рекомендательный характер и, как правило, не затрагивают промежуточные процессы систематизации и анализа разнородных данных по той или иной группе преступных деяний.

Думается, назрела необходимость структурировать имеющиеся сведения по рассматриваемой теме и систематизировать особенности учета указанных преступных деяний для унификации процесса их расследования. В связи с этим ставится задача формирования универсальной криминалистической кодификации преступлений (в значении упорядочивания), в целях реализации адаптированных методик их расследования в условиях постоянной трансформации и эволюции преступлений в сфере компьютерной информации.

Методы

В процессе исследования использовалась совокупность общих методов научного познания (описание, обобщение и сравнение), ряд общенаучных (анализ, синтез, моделирование, формализация, описание, обобщение, сравнение и классификация), а также частнонаучных методов (статистический и кибернетический и пр.), применение которых позволило провести обобщение и анализ материала, а также систематизировать методы учета разнообразных преступлений в сфере компьютерной информации с возможностью унификации процесса их расследования.

Результаты

Классификация как метод научного познания выступает одним из ключевых инструментов криминалистического исследования механизма преступного деяния [1, с. 33]. Именно в рамках классификации формируется наиболее полная систематизированная форма криминалистических категорий, детерминирующих преступление как объект криминалистического познания. Такой подход служит основой для последующего анализа криминального деяния, обеспечивая системно-структурное представление результатов исследования, поиск аналогий, сравнение сложившихся обстоятельств с ранее возникавшими следственными ситуациями, а также формирование наиболее подходящей методики расследования.

На фоне стабильного роста количества преступлений, совершаемых в сфере компьютерной информации и с использованием информационно-телекоммуникационных технологий, процессы синергии в криминалистике резко возросли, что обусловлено развитием теории информационно-компьютерного обеспечения криминалистической деятельности [2, с. 35] и появлением новых закономерностей и механизмов следообразования, современных технологий, позволяющих собирать, анализировать и оценивать криминалистически значимую информацию с применением относительно новых подходов криминалистической тактики и методики. Объектами указанной теории являются технические средства и информационные системы как носители доказательственной информации, а также система действий и отношений в механизмах преступлений с использованием технических средств, а также различных информационных технологий, применяемых в целях поиска, фиксации, изъятия и анализа криминалистически значимой компьютерной информации.

Учитывая целостность предмета и системы криминалистики, для исследования технических средств и информационных систем необходим особый комплекс специальных знаний [3, с. 146], откуда возникает необходимость формирования системы, позволяющей классифицировать [4, с. 157] и кодифицировать [5, с. 107] рассматриваемые преступления (в значении упорядочивания как одного из видов работ в области инженерии знаний), что даст возможность избежать фрагментарности их учета, сложности обработки больших объемов цифровых данных. Данная кодификация может стать основой универсальной концепции стандартизированного учета преступлений в сфере компьютерной информации, упростив процесс идентификации их составов. Рассмотрим имеющиеся критерии для предлагаемой кодификации.

Концепцией государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-телекоммуникационных технологий[3], рассматриваемые противоправные деяния с учетом критериев их квалификации классифицируются по трем основным типам:

[3] Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий : распоряжение Правительства Российской Федерации от 30 декабря 2024 г. № 4154-р // СЗ РФ. 2025. № 2. Ст. 76.

ISSN 2949-1150 (online)
2071-8284 (print)

– правонарушения и преступления в сфере компьютерной информации (в соответствии с главой 28 УК РФ);

– правонарушения и преступления, криминообразующим или квалифицирующим признаком которых является их совершение с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет»;

– правонарушения и преступления, при совершении которых применение информационно-телекоммуникационных технологий является альтернативным способом.

Для преступлений в сфере компьютерной информации в контексте указания Генпрокуратуры России № 462/11, МВД России № 2 от 25 июня 2024 г.[4] квалифицирующим значением является в т. ч. средство совершения указанных деяний (таблица 1), которое входит в структуру механизма преступления и может указывать на применяемый преступником способ совершения преступления, а также на время и место его осуществления.

Таблица 1

Система кодификации методов (способов) совершения преступного деяния[5]

Table 1

Codification system of methods of committing criminal act [5]

Метод (способ) совершения преступления	**Код (Mxxx*)**
Использование информационно-телекоммуникационной сети «Интернет»	M048
Использование средств мобильной связи	M049
Неправомерное списание средств с банковских карт	M050
Использование вредоносного программного обеспечения	M055
Использование информационно-телекоммуникационных технологий (при использовании различных технологий, не имеющих самостоятельных кодовых значений)	M056
Использование компьютерной техники	M057
Использование пластиковых расчетных карт	M058
Использование программных средств (любое программное обеспечение, установленное на компьютер, смартфон или иную технику)	M059
Использование фиктивных электронных платежей	M060
Создание вредоносного программного обеспечения	M072
Распространение вредоносного программного обеспечения	M073
Использование социальных сетей	M086
Использование интернет-мессенджеров	M087
Использование электронных платежных систем	M088
Операции с цифровой валютой	M089
Использование SIP-телефонии	M092
Неправомерный доступ к информации	M094
Операции с цифровыми финансовыми активами	M095
Использование сети “Darknet”	M126
Фишинговые сайты и ссылки	M127
Программы-шифровальщики	M128
Бот-сети (ботнеты)	M130
DDoS-атаки	M131
Использование технологии «Дипфейк»	M132
Компрометация банковских устройств самообслуживания	M133
Использование информационной инфраструктуры (зарубежных серверов (услуг хостинг-провайдеров, интернет-провайдеров, почтовых серверов), доменных зон, телефонных сетей и т. п.) иностранного государства	M134
Использование информационной инфраструктуры стран-участников Содружества Независимых Государств)	M135

Примечание – * Метод (способ) совершения преступления (*Method Mxxx*).

[4] О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности : указание Генпрокуратуры России № 462/11, МВД России № 2 от 25 июня 2024 г. // Справочно-правовая система (далее – СПС) КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_483902/251f7ac207ca304c6331640eb36b162351c24684/ (дата обращения: 12.07.2025).

[5] В соответствии с перечнем № 25 преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации = [In accordance with list No. 25 of crimes committed using (application) information and telecommunication technologies or in the field of computer information] (URL: https://www.consultant.ru/document/cons_doc_LAW_483902/251f7ac207ca304c6331640eb36b162351c24684 (дата обращения: 12.07.2025)).

Переходя к рассмотрению способов совершения преступления как одного из важнейших элементов криминалистической характеристики преступлений, необходимо отметить, что повсеместное использование информационно-телекоммуникационных технологий и внедрение программного обеспечения за последние два десятка лет потребовало систематизации данных обо всех имеющихся уязвимостях в информационной сфере. Так, некоммерческая компания *Mitre* сформировала набор матриц "*Mitre Att&ck*"[6] (от англ. "*adversarial tactics, techniques & common knowledge*" – тактики, техники и общеизвестные факты о злоумышленниках), представляющий собой основанную на реально существующих наблюдениях базу данных инцидентов безопасности. Каждая составляющая указанной базы представляет собой таблицу с указанием угроз и соответствующих им тактик киберпреступников [6, с. 2].

Матрицы рассматриваемой базы данных, описывающие все возможные способы совершения преступлений, связанных с использованием информационно-телекоммуникационных технологий, объединены в три группы: тактики и техники, применяющиеся злоумышленниками в ходе атак на операционные системы компьютеров [7], на мобильные устройства и на промышленные системы управления.

Основу любой методики расследования составляет криминалистическая характеристика преступлений в виде информационной модели [8, с. 69]. Она строится путем обобщения сведений о криминалистически значимых признаках определенного вида преступного деяния, которые, в свою очередь, формируются на основе анализа уголовных дел [9, с. 589]. Однако различные виды преступлений в сфере компьютерной информации могут совершаться одним и тем же способом, но с применением различных техник и тактик. С учетом сказанного можно отметить, что матрица "*Mitre Att&ck*" по сути является отражением такого ключевого элемента криминалистической характеристики преступления в сфере компьютерной информации как «способ совершения преступления». Содержание матрицы "*Mitre Att&ck*" регулярно обновляется [10, с. 2443] и служит надежным источником информации о новых методах (способах) атак злоумышленников, позволяя адаптироваться к меняющемуся ландшафту киберугроз.

На основе вышесказанного теоретико-правовыми основами классификации и последующей кодификации преступлений в сфере компьютерной информации могут выступить три уровня:

– уровень норм, представленных ст. 272, 272[1], 273, 274, 274[1], 274[2] главы 28 «Преступления в сфере компьютерной информации» УК РФ (таблица 2);

– уровень, представленный способами совершения противоправного деяния, в виде квалифицирующего признака, определяемого в соответствии с перечнем преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации[7] (см. таблица 1);

– уровень, отражающий тактику, приемы и методы (способы), используемые преступниками, а также возможности противодействия им, сформированный на базе матрицы "*Mitre Att&ck*"(таблица 3).

Таблица 2

Система кодификации в соответствии с Уголовным кодексом Российской Федерации

Table 2

Codification system in accordance with the Criminal Code of the Russian Federation

Статья УК РФ	**Наименование преступления**	**Пример преступлений**	**Код (Cx*)**
272	Неправомерный доступ к компьютерной информации	Модификация базы данных информационной системы в целях кражи информации ограниченного доступа, несанкционированный доступ к информационной системе путем завладения учетных данных пользователя и пр.	C1

[6] База данных угроз безопасности информации "Mitre Att&ck" // Mitre : [сайт]. URL: https://attack.mitre.org (дата обращения: 12.07.2025).

[7] В соответствии с перечнем № 25 преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации (URL: https://www.consultant.ru/document/cons_doc_LAW_483902/251f7ac207ca304c6331640eb36b162351c24684/ (дата обращения: 12.07.2025)).

ISSN 2949-1150 (online)
2071-8284 (print)

Окончание таблицы 2

Статья УК РФ	Наименование преступления	Пример преступлений	Код (Cx*)
272[1]	Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения	Распространение персональных данных граждан путем формирования базы данных, создание информационных ресурсов с персональными данными граждан в сети «Интернет» и пр.	C2
273	Создание, использование и распространение вредоносных компьютерных программ	Разработка вредоносного программного обеспечения и его распространение в целях получения доступа к вычислительным ресурсам технических средств, распространение фишинговых ссылок и пр.	C3
274	Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей	Использование ботнет-сетей (сети зараженных компьютеров) в целях реализации DDoS-атак на средства хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей и пр.	C4
274[1]	Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации	Кибератака на оборудование объекта критической информационной инфраструктуры Российской Федерации, игнорирование требований политики безопасности и пр.	C5
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	Невыполнение предписаний уполномоченного органа по внедрению необходимых обновлений в системе противодействия угрозам и пр.	C6
Примечание – * Категория преступления (*Category Cx*).			

Для удобства сопоставления с матрицей “*Mitre Att&ck*” предлагаемую кодификацию (далее – CMT-кодификация) целесообразнее именовать на английском языке.

Общий формат предлагаемой системы кодификации имеет вид:

[Категория преступления (*Category Cx*)] – [Метод (способ) совершения преступления (*Method Mxxx*)] – [Техника Mitre (*Techniques Txxxx*)] – [Подтехника *Mitre* (*Sub-techniques Sxxx*)] – [Способ обнаружения (вероятные места нахождения типичных следов преступления) (*Detection Dxxxx*)] – [Меры реагирования (меры противодействия, исключающие обстоятельства, способствовавшие совершению преступлений)) (*Reaction Rxxxx*)].

Рассмотрим систему кодификации на примере преступления, связанного с несанкционированным распространением вредоносного программного обеспечения в виде фишинговой ссылки, направленной пользователю в мессенджере (например, фишинг с утратой логина и пароля для доступа к единому порталу государственных и муниципальных услуг «Госуслуги») (таблица 3).

Таблица 3

Пример описания фишинга с утратой логина и пароля пользователя в соответствии с CMT-кодификацией

Table 3

Example of phishing with loss of user login and password in accordance with CMT codification

Уровень кодификации	**Описание кода**					
Код категории преступления (Category Cx)	C3 (Создание, использование и распространение вредоносных компьютерных программ)					
Метод (способ) совершения преступления (Method Mxxx) выявленные варианты	M-048 Использование сети «Интернет»; M-049 Использование средств мобильной связи; M-073 Распространение вредоносного программного обеспечения; M-087 Использование интернет-мессенджеров; M-094 Неправомерный доступ к информации; M-127 Фишинговые сайты и ссылки					
Коды по матрице “Mitre Att&ck”	Техника (Techniques Txxxx)	Подтехника (Subtechnique Sxxx)	Способ обнаружения (вероятные места нахождения типичных следов преступления) (Detection Dxxxx)			Меры реагирования (меры противодействия) (Reaction Rxxxx)
	T1566 фишинг	S001 целевой фишинг с вложением	D0015 журналы приложений (содержимое журналов приложений)	D0022 файл (создание файла)	D0029 сетевой трафик: содер-жимое сетевого трафика	R 1021 ограничения для веб-контента, R 1031 предотвращение сетевых вторжений
	T1586 компро-метация учетных записей	S000	D0021 фиктивная личность (социальные сети, мессенджеры)	D0029 сетевой трафик (содержимое сетевого трафика)		R1056 предкомпрометация

Общий случай описания рассматриваемого преступления в соответствии с CMT-кодификацией будет иметь вид: C3-M048-T1566-S001-D0015-R1021.

Расширенный вариант можно представить следующим образом: C3 – [M048 / M049 / M073 / M087 / M094 / M127] – [[T1566-S001 - D0015 / D0022 / D0029 - R1021 / R1031] / [T1586-S000 - D0021 / D0029 - R1056]].

Стоит отметить, что на международном уровне матрицы “*Mitre Att&ck*” используют для декомпозиции преступлений на этапы, что позволяет систематизировать поиск и анализ цифровых доказательств (логи, артефакты памяти, данные сетевого трафика и пр.) [11, с. 780; 12]. Предполагается перспективным интегрировать матрицы “*Mitre Att&ck*” в инструменты цифровой криминалистики, что позволит автоматически маркировать индикаторы компрометации и соотносить их с конкретными тактиками преступников. Кроме того, анализ повторяющихся атак поможет выявить шаблоны совершения преступлений, что возможно использовать для прогнозирования будущих угроз и укрепления имеющихся средств защиты информации.

Результаты проведенного сопоставления категорий преступлений в сфере компьютерной информации и техник матрицы “*Mitre Att&ck*” позволят сформировать новую универсальную криминалистическую кодификацию преступлений (в значении упорядочивания) в целях реализации адаптированных методик их расследования в условиях трансформации и эволюции киберпреступности. Предлагаемая унификация как техника приведения к единообразию всех видов преступлений в сфере компьютерной информации соответствует рекомендациям

ISSN 2949-1150 (online)
2071-8284 (print)

Будапештской конвенции Совета Европы ETS 185[8], поскольку единые стандарты данных являются основой глобального противодействия киберугрозам.

Таким образом, предлагаемая кодификация преступлений способствует формированию единой системы, регулирующей не только ответственность за деяния, совершаемые в киберпространстве, выявление возможных связей личности преступника с предметом посягательства и/или личностью потерпевшего, но и возможные векторы атак [13, с. 30], а также методы противодействия им [14, с. 110]. Обеспечивая предсказуемость правоприменения, она создает основу для адаптации уголовного законодательства к постоянно меняющимся технологическим реалиям.

В основе кодификации лежат признанные на международном уровне принципы, заложенные в матрице "M*itre* Att*&ck*", которая постоянно обновляется. Таким образом появляется механизм учета новых видов преступлений. Наличие подобного единообразного набора правил по учету преступлений может упростить международное сотрудничество в сфере борьбы с киберпреступностью, позволяя эффективнее обмениваться унифицированной информацией. Кроме того, возможно формирование аналогичных национальных матриц [15, с. 44], отчасти схожих с банком данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю (ФСТЭК России).

Предлагаемое решение возможно реализовать в виде программного технико-криминалистического средства, реализованного на основе:

1) технологий искусственного интеллекта: метод глубокого обучения (сверхточные нейронные сети (например, для анализа мультимедийных данных), рекуррентные сети (для исследования сетевого трафика и пр.), трансформеры (для анализа текстовых данных, выявления взаимосвязей между интересующими объектами)), графовые сети (для формирования ветвящихся алгоритмов расследования); обучение без учителя (кластеризация данных); обучение с подкреплением (внедрение программных агентов в процессы расследования и пр.); генеративный (для прогнозирования преступности) и объяснимый искусственный интеллект (для повышения уровня доверия к выдаваемым системой заключениям) и т. п.;

2) технологий анализа данных (визуализация результатов анализа данных, выявление взаимосвязей между ними, реализация дашбордов, наглядно отображающих динамику изменений данных и т. п.);

3) распределенных вычислений и облачных технологий (реализация платформ для обработки больших и разнородных данных, облачных платформ для анализа и хранения цифровых доказательств, масштабирования хранилищ данных и пр.).

Предлагаемая CMT-кодификация преступлений в сфере компьютерной информации, закладываемая в программное технико-криминалистическое средство, может представлять собой не только средство структурирования данных о преступных деяниях и упорядочения существующих их вариантов, но и выступать стратегически важным шагом в создании эффективной системы противодействия преступности.

Система такого рода в дальнейшем сможет заложить новый вектор развития цифровой криминалистики как комплекс специальных знаний, сформированный на основе частной криминалистической теории информационно-компьютерного обеспечения криминалистической деятельности, позволяющий определить наиболее подходящую в соответствии со сложившимися обстоятельствами преступного деяния методику расследования. Стоит также отметить, что предлагаемый подход обеспечит процесс унификации расследования преступлений в сфере компьютерной информации благодаря заложенным в набор данным интеллектуальной системы алгоритмов действий для любой комбинации тактик и техник совершения преступного деяния.

Заключение

Всякая исследовательская деятельность, связанная с систематизацией, направлена на выявление в объекте исследования элементов, структур и связей, что может значительно облегчить его изучение в целях решения поставленных задач. Основными объектами систематизации в криминалистике выступают знания, полученные в результате изучения преступной деятельности как в целом, так и ее отдельных видов механизма образования криминалистически значимой информации, а также совокупность разработанных на основе полученных знаний

[8] Конвенция о преступности в сфере компьютерной информации (заключена в г. Будапеште 23.11.2001) (в ред. от 28.01.2003) // ГАРАНТ.РУ : [сетевое издание]. URL: https://base.garant.ru/4089723/ (дата обращения: 12.07.2025). Россия не участвует.

рекомендаций по выявлению, раскрытию, расследованию и предупреждению преступлений [16, с. 40]. Соответственно, криминалистическая кодификация как процесс систематизации преступлений в сфере компьютерной информации может стать основой формирования систем на основе искусственного интеллекта, которые объединят в себе юридические и технические аспекты расследования. Выступая катализатором эволюции цифровой криминалистики, кодификация может создать условия для внедрения передовых методов и технологий, обеспечивающих достоверность, целостность и допустимость цифровых доказательств в суде.

Предлагаемый подход будет способствовать разработке новых и совершенствованию существующих программных технико-криминалистических средств на основе перспективных информационных технологий, а также методических рекомендаций по их применению в целях эффективного поиска, собирания, фиксации и исследования цифровых доказательств.

Список источников

1. *Головин А. Ю.* Базовые криминалистические классификации преступлений // Известия Тульского государственного университета. Экономические и юридические науки. 2013. № 2-2. С. 31–40.

2. *Россинская Е. Р.* Теория информационно-компьютерного обеспечения судебно-экспертной деятельности как новая частная теория судебной экспертологии // Вестник Университета имени О. Е. Кутафина. 2022. № 2 (90). С. 27–40. https://doi.org/10.17803/2311-5998.2022.90.2.027-040

3. *Россинская Е. Р.* К вопросу об инновационном развитии криминалистической науки в эпоху цифровизации // Юридический вестник Самарского университета. 2019. Т. 5, № 4. С. 144–151. https://doi.org/10.18287/2542-047X-2019-5-4-144-151

4. *Mandal S.* Cybercrime Classification: A Victimology-Based Approach // International Conference on Cyber Warfare and Security. 2024. Vol. 19. No 1. P. 156–167. https://doi.org/10.34190/iccws.19.1.2199

5. *Owen T.* Codifying and Applying the Genetic-Social Framework to Cybercrime and Cyber Terrorism // Cybercrime and Cyber Terrorism: Palgrave Macmillan, Cham, 2025. P. 107–181. https://doi.org/10.1007/978-3-031-87853-4_6

6. *Al-Sada B., Sadighian A., Oligeri G.* Mitre Att&ck: State of the art and way forward // ACM Computing Surveys. 2024. Vol. 57. No 1. P. 1–37. https://doi.org/10.1145/3687300

7. *Branescu I., Grigorescu O., Dascalu M.* Automated mapping of common vulnerabilities and exposures to mitre att&ck tactics // Information. 2024. Vol. 15. No 4. P. 214. https://doi.org/10.3390/info15040214

8. *Россинская Е. Р., Семикаленова А. И.* Информационно-компьютерные криминалистические модели компьютерных преступлений как элементы криминалистических методик (на примере кибершантажа) // Вестник Томского государственного университета. 2021. № 42. С. 68–80. https://doi.org/10.17223/22253513/42/5

9. *Эксархопуло А. А., Макаренко И. А., Зайнуллин Р. И.* Криминалистика. Теоретический курс : монография. Уфа : НИИ ППГ, 2022. 649 с.

10. *Jaouhari S., Tamani N., Jacob R.* Improving ML-based Solutions for Linking of CVE to Mitre Att&ck Techniques / 2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC), Osaka, Japan. 2024. P. 2442–2447. https://doi.org/ 10.1109/COMPSAC61105.2024.00392

11. *Chamkar S. A., Maleh Y., Gherabi N.* Security Operations Centers: Use Case Best Practices, Coverage, and Gap Analysis Based on Mitre Adversarial Tactics, Techniques, and Common Knowledge // Journal of Cybersecurity and Privacy. 2024. Vol. 4. No 4. P. 777–793. https://doi.org/10.3390/jcp4040036

12. *Hargreaves C., Beek H., Casey E.* Solve-it: A proposed digital forensic knowledge base inspired by Mitre Att&ck // Forensic Science International: Digital Investigation. 2025. Vol. 52. P. 301864. https://doi.org/10.1016/j.fsidi. 2025.301864

13. *Веревкин С. А. Федорченко Е. В.* Сравнительный анализ баз данных Mitre Att&ck и Capec // Известия Тульского государственного университета. Технические науки. 2023. № 4. С. 29–39. https://doi.org/10.24412/2071-6168-2023-4-29-39

14. *Akbar K. A. [et al.].* Knowledge mining in cybersecurity: From attack to defense // Sural Sh., Lu H. (eds.) Data and Applications Security and Privacy XXXVI. 36th Annual IFIP WG 11.3 Conference, DBSec 2022, Newark, NJ, USA, July 18–20, 2022. P. 110–122. https://doi.org/10.1007/978-3-031-10684-2_7

15. *Середкин С. П.* Моделирование угроз безопасности информации на основе банка угроз ФСТЭК России // Информационные технологии и математическое моделирование в управлении сложными системами : [электронный журнал]. 2022. № 1 (13). С. 43–54. URL: http://ismm-irgups.ru/toma/113-2022. https://doi.org/10.26731/2658-3704.2022.1(13).43-54

16. *Головин А. Ю.* Криминалистическая систематика : монография. Москва : ЛексЭст, 2002. 305 с.