

КИБЕРПРЕСТУПНОСТЬ И ТЕНДЕНЦИИ РАЗВИТИЯ КРИМИНАЛИСТИКИ

научный руководитель: д.ф.н., профессор кафедры истории, философии
и социальных наук Золотухин В.М.

В данной статье рассматриваются тенденции развития криминалистики в связи с появлением киберпреступности. Затрагивается вопрос о изменении криминалистических методов с внедрение передовых информационно-коммуникационных технологий в повседневную жизнь. Подчеркивается, что киберпреступность представляет собой одну из наиболее динамично развивающихся форм противоправной деятельности. Акцентируется внимание на различные основания классификация киберпреступлений, их особенности и характер проявления.

Ключевые слова: криминалистика, информация, киберпреступность, интеллектуальные системы, инновационные технологии, COVID-19..

Современное общество переживает фундаментальную трансформацию, характеризующуюся всеобъемлющей цифровизацией социальных процессов. Масштаб этих изменений представляет собой повсеместное внедрение передовых информационно-коммуникационных технологий в повседневную жизнь граждан. Биометрическая аутентификация, включающая распознавание лиц (Face ID) и дактилоскопическая идентификация (Touch ID), уже стала неотъемлемой частью взаимодействия человека с цифровыми устройствами, обеспечивая не только безопасный доступ к персональным данным, но и совершение финансовых операций через системы электронных платежей. Концепция Internet of Things реализуется в интеллектуальных системах домашней автоматизации, формируя качественно новую парадигму организации жилого пространства, в основании которой – новый тип рациональности. Ему характерно то, «что прежние принципы формализма и прагматизма входят во взаимодействие с принципами функционирования инновационных технологий, образуя сложный гибрид. Во всех типах формальной рациональности, включая цифровую рациональность, присутствуют компоненты эффективности, калькулируемости, предсказуемости и контроля, способствуя развитию целерациональных действий, что создает более эффективные формы власти и управления, иниции-

рут предсказуемые и контролируемые поведенческие акты. Однако одновременно идет нарастание “иррациональной рациональности”, дегуманизации, социальной безответственности. Этому способствует “глобальный цифровой риск” (У. Беку), специфический, “неожиданный” риск, проявляющийся вне конкретного пространства и времени, побуждающий людей некритически, как само собой разумеющееся, воспринимать информацию» [Кравченко, 2024; С. 69].

Катализатором ускоренной цифровой адаптации общества послужила глобальная пандемия COVID-19, подвинувшая общество к поиску альтернативных способов реализации базовых потребностей [Золотухин, Козырева, 2016; Скрипко, Якунина, 2022; Золотухин, Золотухин, Скрипко, 2023; Золотухин, Михайлов, 2023]. Это привело к значительному росту востребованности цифровых сервисов: электронной коммерции, дистанционного банковского обслуживания, образовательных платформ и государственных услуг в электронном формате. Для большей наглядности, отобразим влияние пандемии на востребованность цифровых сервисов в таблице 1. [Госуслуги, 2020; В России, 2024]

Таблица 1

ВЛИЯНИЕ ПАНДЕМИИ COVID-19 НА ВОСТРЕБОВАННОСТЬ ЦИФРОВЫХ СЕРВИСОВ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Сфера	Показатель	Изменение
Электронная коммерция	Общий объем онлайн-торговли в России	+58% (2020 vs 2019)
	Новые пользователи онлайн-магазинов	+40%
	Оборот Wildberries	+96% (до 437,2 млрд руб.)
Онлайн-банкинг	Пользователи мобильного банкинга	+51%
	Доля безналичных платежей	Достигла 70%
	Цифровые банковские карты	Рост в 3 раза
Образовательные платформы	Пользователи Coursera	+640%
	Аудитория "Учи.ру"	Рост в 2,5 раза
	Участники конференций Zoom	с 10 млн до 300 млн
Госуслуги	Новые пользователи портала	+24 млн
	Электронные заявления	Рост в 3 раза
	Активные пользователи	56% россиян

Стремительное формирование новой цифровой реальности вызывает необходимость создания актуальной нормативно-правовой базы [Золотухин, 2023]. В рамках адаптации к современным требованиям закона была создана национальная программа «Цифровая экономика Российской Федерации», в ней разрабатывается комплексное правовое регулирование общественных отношений, возникающих в процессе цифровой трансформации общества [Zolotukhin, Zhukova, 2018].

В современном мире киберпреступность представляет собой одну из наиболее динамично развивающихся форм противоправной деятельности. Согласно определению, предложенному Конвенцией Совета Европы о киберпреступности, под киберпреступностью понимается совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем и компьютерных сетей, а также иных средств доступа к киберпространству [Конвенция, 2001].

Классификация киберпреступлений может быть проведена по различным основаниям. Наиболее распространенной является следующая типология [Цифровая, 2024]:

1. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (хакерские атаки, DDoS-атаки, распространение вредоносного ПО);
2. Преступления, связанные с использованием компьютерных средств (компьютерное мошенничество, компьютерный шпионаж);
3. Преступления, связанные с контентом (распространение противоправной информации);
4. Преступления, связанные с нарушением авторских и смежных прав.

Особенностями киберпреступлений как объекта криминалистического исследования являются: высокая латентность; трансграничный характер; сложность обнаружения, фиксации и изъятия криминалистически значимой информации; возможность совершения преступлений в автоматизированном режиме; постоянное появление новых способов совершения преступлений.

Традиционная криминалистика, сформировавшаяся в XX веке, базируется на четырех основных разделах: общая теория криминалистики, криминалистическая техника и тактика, а также методика расследования отдельных видов преступлений. Однако цифровизация общественных отношений привела к существенной трансформации криминалистической науки. Влияние цифровизации проявляется в следующих аспектах [Цифровая, 2024]:

1. Появление новых объектов исследования:

- ✓ Цифровые следы;
- ✓ Виртуальные следы;
- ✓ Электронные документы;
- ✓ Криптовалюты и иные цифровые активы.

2. Развитие новых методов исследования:

- ✓ Компьютерно-техническая экспертиза;
- ✓ Анализ больших данных;
- ✓ Применение искусственного интеллекта;
- ✓ Использование облачных технологий.

3. Формирование новых направлений криминалистических исследований:

- ✓ Цифровая криминалистика;
- ✓ Сетевая криминалистика;
- ✓ Мобильная криминалистика;
- ✓ Облачная криминалистика.

В современных условиях происходит интеграция традиционных криминалистических знаний с достижениями информационных технологий. Это приводит к формированию новых научных подходов и методологических принципов исследования преступной деятельности в цифровой среде.

Особое значение приобретает разработка методов обнаружения, фиксации и исследования цифровых следов преступления. При этом важно отметить, что цифровые следы обладают рядом специфических характеристик:

- Волатильность (возможность быстрого изменения или уничтожения);
- Копируемость без потери качества;

- Возможность удаленного доступа;
- Зависимость от программно-аппаратной среды.

Таким образом, современное состояние криминалистики характеризуется активной трансформацией под влиянием процессов цифровизации. Происходит как модернизация традиционных криминалистических методов, так и формирование принципиально новых направлений исследований, что требует постоянного совершенствования теоретической и методологической базы.

Как новое направление криминалистической науки, сформировавшееся в ответ на вызовы цифровой эпохи ее предметом являются закономерности собирания, исследования и использования цифровых доказательств в процессе раскрытия и расследования преступлений.

Методологический аппарат цифровой криминалистики включает следующие основные группы методов [Цифровая, 2024]:

1. Методы обнаружения цифровых следов:

- Сканирование сетевого трафика
- Мониторинг системных журналов
- Анализ метаданных файлов
- Поиск скрытой информации

2. Методы фиксации цифровых следов:

- Создание образов носителей информации
- Протоколирование действий в информационных системах
- Снятие цифровых слепков оперативной памяти
- Извлечение данных из облачных хранилищ

3. Методы исследования цифровых доказательств:

- Восстановление удаленных данных
- Декодирование зашифрованной информации
- Анализ временных меток и системных артефактов
- Исследование сетевых протоколов

Современный этап развития криминалистики характеризуется активным внедрением передовых технологических решений, среди которых особое место

занимают искусственный интеллект, технологии больших данных и облачные вычисления. Эти инновации существенно расширяют возможности криминалистической науки и практики, позволяя решать все более сложные задачи в условиях цифровой трансформации преступной деятельности.

Использование искусственного интеллекта (ИИ) открывает принципиально новые возможности в области криминалистических исследований. Современные системы ИИ способны осуществлять автоматизированный анализ больших массивов информации различного типа. В работе с текстовыми данными это позволяет эффективно анализировать электронную переписку, документацию и активность в социальных сетях. При исследовании визуальной информации искусственный интеллект демонстрирует впечатляющие результаты в распознавании лиц в видеопотоке, идентификации объектов на изображениях и восстановлении поврежденных файлов. Не менее важны достижения в области анализа аудиоданных, где ИИ успешно справляется с задачами идентификации голоса, выявления монтажа аудиозаписей и распознавания речи в сложных акустических условиях.

Важным аспектом развития современной криминастики является интеграция различных технологических решений. Создаются комплексные платформы криминалистического анализа, обеспечивающие интеграцию различных источников данных, автоматизацию рутинных процессов и эффективную визуализацию результатов. Системы управления цифровыми доказательствами решают задачи хранения, каталогизации и контроля целостности собранных данных.

Среди перспективных направлений развития особого внимания заслуживают квантовые вычисления, открывающие новые возможности в области криptoанализа и моделирования сложных систем. Технологии распределенного реестра находят применение в анализе блокчейн-транзакций и обеспечении неизменности цифровых доказательств. Развитие нейроморфных систем создает предпосылки для качественного скачка в области распознавания сложных паттернов и адаптивного анализа данных.

Интеграция новых технологий в криминалистическую практику требует комплексного подхода, учитывающего не только технические, но и организационные аспекты. Особое значение приобретает подготовка специалистов, способных эффективно использовать современные технологические решения в практической деятельности. При этом важно соблюдать баланс между применением передовых технологий и обеспечением достоверности и допустимости полученных доказательств.

Таким образом, внедрение новых технологий существенно расширяет возможности современной криминастики, создавая предпосылки для повышения эффективности раскрытия и расследования преступлений в условиях цифровой трансформации общества. При этом важно понимать, что технологические решения являются не заменой, а дополнением к традиционным криминалистическим методам, позволяя комплексно решать задачи противодействия современной преступности.

В условиях стремительного развития информационных технологий и цифровизации общества происходит существенная трансформация криминалистических методик. Данный процесс охватывает как адаптацию традиционных подходов к новым реалиям, так и формирование принципиально новых методов расследования.

Адаптация традиционных криминалистических методик к цифровой среде затрагивает все аспекты следственной работы. Особенно заметные изменения происходят в методике проведения осмотра места происшествия. В современных условиях само понятие «место происшествия» существенно расширилось и теперь включает не только физическое, но и виртуальное пространство. При проведении осмотра следователи сталкиваются с необходимостью фиксации волатильных данных и соблюдения особого порядка работы с электронными устройствами. Для решения этих задач активно внедряются новые технические средства фиксации, включая специализированное программное обеспечение для создания цифровых копий, блокаторы записи и средства документирования сетевых параметров.

Существенной модификации подверглась и тактика допроса по делам о киберпреступлениях. Специфика подготовки к допросу теперь включает тщательный анализ технических данных, обязательные консультации со специалистами и подготовку технической документации. Особое значение приобретает правильное использование технической терминологии и умение работать с цифровыми доказательствами в процессе допроса. Документирование показаний часто требует применения схем и диаграмм для наглядного отображения технических аспектов преступной деятельности.

В области экспертных исследований наблюдается появление новых видов компьютерно-технических экспертиз. Активно развиваются такие направления как экспертиза вредоносного программного обеспечения, анализ сетевого трафика, исследование облачных сервисов и криптографическая экспертиза. Происходит существенная модернизация методик исследования за счет автоматизации рутинных процессов и применения специализированных программных комплексов.

Параллельно с адаптацией традиционных методик происходит разработка принципиально новых методов расследования. Особое внимание уделяется методикам расследования преступлений в сфере криптовалют. Данное направление требует глубокого понимания механизмов работы блокчейн-технологий, умения анализировать криптовалютные транзакции и выявлять связи между ними. Специфика доказывания в таких делаах связана с необходимостью достоверного установления владельцев криптовалютных активов и документирования движения цифровых средств. Технические аспекты такого расследования включают мониторинг теневых площадок, деанонимизацию пользователей и отслеживание криптовалютных транзакций. Особую роль играет оперативная работа, связанная с внедрением в закрытые сообщества и документированием противоправной деятельности.

Расследование инцидентов информационной безопасности также требует специфических подходов. Процесс расследования включает этапы первичного реагирования, сбора цифровых доказательств, анализа вредоносного программ-

ного обеспечения и восстановления хронологии инцидента. Особое внимание уделяется правильному документированию всех этапов расследования, включая фиксацию следов атаки и сохранение системных журналов.

Важнейшей тенденцией в развитии современной криминалистики становится реализация междисциплинарного подхода. Происходит активная интеграция знаний из различных областей, включая информационные технологии, компьютерную безопасность и психологию киберпреступности. Это приводит к формированию новых направлений исследований, таких как поведенческая криминалистика, криминалистическая кибернетика и криминалистическая аналитика. Практическая реализация междисциплинарного подхода требует решения ряда организационных вопросов, связанных с формированием междисциплинарных следственных групп и координацией взаимодействия экспертов различного профиля.

Важным аспектом развития криминалистики в современных условиях становится подготовка специалистов нового поколения. Разрабатываются междисциплинарные учебные программы, организуются стажировки и обмен опытом между специалистами различных профилей. Это позволяет формировать новое поколение следователей и экспертов, способных эффективно работать в условиях цифровой трансформации преступной деятельности.

Развитие международной кооперации представляется одним из ключевых направлений совершенствования криминалистической деятельности [Драгунов, Жандаров, Золотухин, 2024; Помогалов, Шмидт, Золотухин, 2024]. Создание международных баз данных киберпреступлений и разработка унифицированных протоколов международного взаимодействия позволяют существенно повысить эффективность расследования трансграничных преступлений. Организация совместных международных исследовательских проектов и формирование международных центров по борьбе с киберпреступностью будут способствовать развитию систем быстрого реагирования на трансграничные киберпреступления при условии, чтобы международная борьба с киберпреступностью проводилась на равноправной основе и доступности информации.

Особое значение приобретает подготовка специалистов нового поколения, формирование соответствующего уровня правовой культуры [Красиков, Овчаров, Золотухин, Казаков, Чирун, Востриков, 2007; Золотухин, Суслова, 2011]. Модернизация образовательных программ в области цифровой криминалистики и внедрение практико-ориентированного подхода в обучении [Золотухин, Съедина, 2015] позволяют сформировать компетентных специалистов, способных эффективно противодействовать современным киберугрозам. Развитие системы непрерывного повышения квалификации, создание специализированных центров подготовки и организация международных стажировок обеспечат постоянное совершенствование профессиональных навыков криминалистов. Только при условии системного решения существующих проблем и планомерного развития перспективных направлений возможно обеспечить эффективное противодействие киберпреступности и дальнейшее развитие криминалистики как науки.

Библиографический список

1. В России выросла доля пользователей цифровых банковских сервисов. 10.11.2024. // Regnum.ru : [сайт]. – URL: <https://regnum.ru/news/3024780?ysclid=m2utlrlz7g936610447> (дата обращения: 29.10.2024).
2. Госуслуги в цифрах 2020 год. – Текст : электронный // Государственные и муниципальные услуги : [сайт]. – URL: <https://www.mfc45.ru/news/1234.html> (дата обращения: 22.10.2024).
3. Драгунов В.В., Жандаров А.В., Золотухин В.М. Сравнительный анализ методов криминалистики в России и Китая. / Проблемы экономики и управления: социокультурные, правовые и организационные аспекты. Сб. статей магистрантов и преподавателей КузГТУ. – Кемерово, 2024. – С. 226–232
4. Золотухин В. М. Социально-философский и культурологический аспекты устойчивого развития цифровых экосистем. / Проблемы экономики и управления: социокультурные, правовые и организационные аспекты. Сб. статей магистрантов и преподавателей КузГТУ. – Кемерово, 2023. – С. 89–99.
5. Золотухин В.М., Козырева М.В. Социокультурные основания реализации и регламентации потребностей в контексте исследования качества жизни. // Вестник Кемеровского государственного университета культуры и искусств, 2016.– № 37-1. – С. 68–75.
6. Золотухин В. М., Золотухин М. В., Скрипко В. Е. Проблемы цифровизации экономики и их взаимосвязь с образовательной средой. / Проблемы экономики и управления: социокультурные, правовые и организационные аспекты. Сб. статей магистрантов и преподавателей КузГТУ. – Кемерово, 2023. – С. 100–108
7. Золотухин В.М., Суслова С.В. Правовая культура и образование. // Вестник Кемеровского государственного университета. 2011. – № 2 (46). – С. 178–181.
8. Золотухин В.М., Съедина Н.В. Готовность студентов к самоконтролю как процесс педагогического взаимодействия субъектов воспитательно-образовательного процесса. // Профессиональное образование в России и за рубежом. 2015. – № 3 (19). – С. 48–54.

9. Золотухин М. В., Михайлов В. Г. Цифровизация экономики: проблемы, тенденции и перспективы. / Проблемы экономики и управления: социокультурные, правовые и организационные аспекты. Сб. статей магистрантов и преподавателей КузГТУ. – Кемерово, 2023. – С. 420–425
10. Кравченко С. А. Синергия сложности как императивный принцип организации власти в цифровую эпоху: новые вызовы человеческому капиталу. // Полис. Политические исследования, 2024. № 2. С. 65-79. <https://doi.org/10.17976/jpps/2024.02.06>. EDN: GDHVVD.
11. Красиков В.И., Овчаров А.А., Золотухин В.М., Казаков Е.Ф., Чирун С.Н., Востриков К.В. Этюды социальной (культурной) антропологии. – Кемерово, 2007. –290 с.
12. Конвенция о преступности в сфере компьютерной информации (ETS № 185) [заключена в г. Будапеште 23.11.2001] // Совет Европы и Россия. – 2002. – № 1. – С. 48–73.
13. Помогалов Н. А., Шмидт О. Е., Золотухин В. М. Сравнительный анализ методов криминалистики в России и странах Западной Европы. / Проблемы экономики и управления: социокультурные, правовые и организационные аспекты. Сб. статей магистрантов и преподавателей КузГТУ. – Кемерово, 2024. – С. 251–265.
14. Скрипко В. Е., Якунина Ю. С. ВЕБ-инструменты лидогенерации в маркетинге формирования спроса. // Экономика и управление инновациями. 2022. – № 2 (21). – С. 77–88
15. Цифровая криминалистика : учебник для вузов / В. Б. Вехов [и др.] ; под редакцией В. Б. Вехова, С. В. Зуева. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 490 с. Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: <https://urait.ru/bcode/533155> (дата обращения: 24.10.2024).
16. Zolotukhin V. M., Zhukova O. I. Problem of relations between human and society in conditions of social transformations: В сборнике: The European Proceedings of Social and Behavioural Sciences EpSBS. Collection of conference materials. Future Academy, 2018. C. 1085-1091.

*P.A. Kovalenko, D. A. Kovalchuk
T.F. Gorbachev Kuzbass State Technical University, Kemerovo, Russia*

CYBERCRIME AND TRENDS IN THE DEVELOPMENT OF CRIMINOLOGY

supervisor: D. F. N., Professor of history, philosophy and social Sciences Zolotukhin V. M.

This article examines the trends in the development of criminology in connection with the emergence of cybercrime.. The issue of changing forensic methods with the introduction of advanced information and communication technologies into everyday life is raised. It is emphasized that cybercrime is one of the most dynamically developing forms of illegal activity. Attention is focused on the various grounds for the classification of cybercrimes, their features and the nature of their manifestation.

Keywords: criminalistics, information, cybercrime, intelligent systems, innovative technologies, COVID-19.

Сведения об авторах

КОВАЛЕНКО ПОЛИНА АНДРЕЕВНА – студентка (гр. БЭс-201) ФГБОУ ВО «Кузбасский государственный технический университет имени Т.Ф. Горбачева», Институт Экономики и управления г. Кемерово, e-mail:

КОВАЛЬЧУК ДАНИИЛ АЛЕКСАНДРОВИЧ – студент (гр. БЭс-201) ФГБОУ ВО «Кузбасский государственный технический университет имени Т.Ф. Горбачева», Институт Экономики и управления г. Кемерово, e-mail

ЗОЛОТУХИН ВЛАДИМИР МИХАЙЛОВИЧ (научный руководитель) – доктор философских наук, профессор, Строительный институт, профессор кафедры истории, философии и социальных наук, ФГБОУ ВО «Кузбасский государственный технический университет имени Т.Ф. Горбачева», г. Кемерово. e-mail: zvm64@mail.ru

Information about the authors

KOVALENKO POLINA ANDREEVNA – student (BEs-201 class), *T.F. Gorbachev Kuzbass State Technical University, Institute of Economics and Management, Kemerovo, Russia*, e-mail:

KOVALCHUK DANIIL ALEXANDROVICH – student (BEs-201 class), *T.F. Gorbachev Kuzbass State Technical University, Institute of Economics and Management, Kemerovo, Russia*, e-mail:

ZOLOTUKHIN VLADIMIR MIKHAILOVICH supervisor: D. F. N., professor, *T.F. Gorbachev Kuzbass State Technical University, Construction Institute, professor of history, philosophy and social Sciences*, e-mail: zvm64@mail.ru