МРНТИ 10.31.35
УДК 347.91/.95
JEL K41

https://doi.org/10.46914/2959-4197-2025-1-1-38-47

АЛАЕВА Г.Т.,[1]
к.ю.н., профессор.
e-mail: g.alayeva@turan-edu.kz
ORCID ID: 0000-0003-1672-2238
КАБДОЛДИНА Е.В.,*[1]
магистрант.
*e-mail: 23242635@turan-edu.kz
ORCID ID: 0009-0007-9919-1036
[1]Университет «Туран»,
г. Алматы, Казахстан

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В СУДЕБНОЙ ЭКСПЕРТИЗЕ В КАЗАХСТАНЕ И В МИРЕ: ПЕРСПЕКТИВЫ И ВЫЗОВЫ

Аннотация

Глобальная цифровизация затрагивает все сферы жизни, включая правоохранительную и судебную системы. В области судебной экспертизы цифровизация представляет собой внедрение новых технологий для анализа, хранения и защиты цифровых доказательств. Данная статья рассматривает виды компьютерных преступлений и сферы их проявления, а также появление в связи с этим нового типа доказательств – «цифровые» доказательства, а именно «цифровой» след. В статье рассматриваются категории цифровых следов и их носителей. Также приведен мониторинг роста преступлений с использованием информационно-телекоммуникационных технологий в Казахстане за 2022–2023 гг., 2023–2024 гг., где наглядно приведены цифры, указывающие на увеличивающуюся прогрессию таких преступлений из года в год. Учитывая увеличение числа киберпреступлений, их стремительный рост, появление новых видов доказательств – «цифровых» доказательств, в статье предлагаются конкретные меры по исследованию компьютерных средств и систем, где будет собрана криминалистическая дефиниция цифровых следов, их виды и способы собирания, исследования, оценки их использования с целью установления обстоятельств, имеющих значение для законного, обоснованного и справедливого разрешения дела; унификация и нормативная регламентация цифровых баз с возможностью их использования как в Казахстане, так и на международном уровне. А также предложены меры по цифровизации сфер судебно-экспертной и криминалистической отраслей с целью объединения их в единые АИПС (Автоматизированные информационно-поисковые системы) для наиболее эффективного учета цифровых следов (АИПС криминалистического и судебно-экспертного назначения).

Ключевые слова: цифровизация, судебно-экспертная деятельность, компьютерные технологии, киберпреступления, компьютерные преступления, фишинг, цифровые доказательства.

Введение

Появление преступлений с использованием компьютерных технологий связано с бурным ростом цифровизации в конце XX века. Первые компьютерные преступления касались кражи данных, взлома систем безопасности и несанкционированного доступа к информации. На рубеже 90-х годов XX века с распространением Интернета преступления приобрели транснациональный характер, поскольку Интернет позволил злоумышленникам совершать действия за пределами национальных границ. Такие преступления нового времени, как киберпреступления, направленные на системы безопасности компьютерных сетей; взломы (несанкционированный доступ к информации); распространение вредоносных программ (вирусов, троянов, программ-шифровальщиков); атаки на информационные системы (DoS/DDoS атаки); мошенничество в Интернете (преступления, связанные с обманом пользователей для получения финансовой выгоды, включая фишинг (кража личных данных через ложные сайты), онлайн-мошенничество (ложные интернет-магазины, инвестиционные схемы); кража криптовалют и другие формы

цифрового мошенничества; кибербуллинг и распространение незаконного контента: преступления, связанные с распространением порнографии, оскорблениями, угрозами, дискредитацией и другими противоправными действиями в Интернете; преступления, связанные с нарушением авторских прав: незаконное копирование, распространение и использование программного обеспечения, фильмов, музыки, электронных книг и других цифровых продуктов; преступления в финансовой сфере: финансовые злоупотребления, включая отмывание денег, манипуляции с банковскими картами, электронными переводами и платежными системами, становятся обычным явлением в наши дни [2].

Компьютерные преступления затрагивают различные секторы экономики и социальной жизни, такие как финансовые организации: банки, биржи, криптовалютные платформы; государственные учреждения: атаки на государственные информационные системы и базы данных (кибершпионаж); частные компании: кража коммерческой тайны, нарушение конфиденциальности данных клиентов; социальные сети: распространение незаконного контента, кибербуллинг и дискредитация, а также они могут коснуться любого человека независимо от возраста, пола, социальной принадлежности и др.

Материалы и методы

При исследовании данного вопроса были подробно проанализированы действующие нормы как национального, так и международного законодательства, регламентирующие использование специальных знаний в уголовном судопроизводстве. Особое внимание уделено специализированной литературе и криминалистической методологии, охватывающей широкий спектр научных подходов и методов. Среди них использовались методы диалектической и формальной логики, которые позволяют системно анализировать явления и процессы, связанные с цифровизацией следов преступлений.

Методологическая основа исследования включает общенаучные и специальные методы криминалистики, которые способствуют глубокой интерпретации данных, а также общеэкспертные и частноэкспертные методы, используемые в судебной компьютерно-технической экспертизе. Для более полного охвата исследуемой проблемы были привлечены данные мониторинга следственной и оперативно-розыскной практики, что позволило выявить актуальные тенденции и практические аспекты применения цифровых технологий в уголовных расследованиях. Результаты опросов и анкетирования специалистов в области IT-технологий дополнили эмпирическую базу исследования, подчеркнув растущую роль экспертов в данной сфере.

Анализ показал, что специалисты в области IT-технологий востребованы не только при расследовании преступлений, непосредственно связанных с неправомерным доступом к компьютерной информации, разработкой и использованием вредоносных программ, но также активно привлекаются к следственным действиям и оперативно-розыскным мероприятиям в рамках дел о традиционных видах преступлений. Это включает мошенничество различных форм, незаконную организацию азартных игр, незаконный оборот наркотических средств, тяжкие преступления против личности, такие как убийства, а также расследование случаев заведомо ложных сообщений об актах терроризма.

Основные тенденции, составляющие предмет данного исследования, включают ряд ключевых аспектов, отражающих динамику развития криминалистической практики в условиях цифровизации:

- Тенденция возникновения, существования и утраты цифровых следов в компьютерных средствах и системах, которые содержат криминалистически значимую информацию. Эти следы могут исчезать в результате целенаправленных действий злоумышленников или технических факторов, что усложняет их выявление и исследование.
- Тенденция отражения в компьютерных системах цифровых следов, связанных с событиями преступлений и правонарушений. Такие следы могут включать логи системы, метаданные файлов, остаточные данные на носителях информации и другие артефакты, которые служат важными источниками доказательств.
- Тенденция фиксации информации о способах совершения преступлений, связях действий и их результатах, повторяемости действий в схожих ситуациях, а также стереотипах по-

ведения преступников. Анализ таких данных позволяет выявлять закономерности и прогнозировать действия преступных группировок.

◆ Развитие информационно-компьютерных технологий, обеспечивающих процессы выявления, фиксации, изъятия, сохранения и исследования криминалистически значимой информации. Это включает использование специализированного программного обеспечения, методов цифровой криминалистики и инструментов для восстановления утраченной информации.

◆ Тенденция возникновения и развития обстоятельств, связанных с преступлениями, совершенными с использованием компьютерных технологий, значимых для расследования. Важным аспектом является изучение не только цифровых следов самого преступления, но и цифрового контекста, в котором оно было совершено.

◆ Оценка и использование криминалистически значимой информации для целей розыска и доказательства. Здесь особое внимание уделяется вопросам допустимости и надежности цифровых доказательств в судебных процессах.

◆ Информационно-компьютерное обеспечение тактики и технологии проведения следственных и судебных действий. Современные технологии позволяют оптимизировать процесс расследования, повышая его эффективность и точность.

◆ Развитие методик расследования преступлений, включая создание информационно-компьютерных моделей для анализа преступлений, совершенных с использованием компьютерных технологий. Такие модели помогают систематизировать информацию и выявлять скрытые взаимосвязи.

◆ Информационно-компьютерное обеспечение гражданского и административного судопроизводства, что подчеркивает универсальность и широкую применимость цифровых технологий в правоприменительной практике.

Согласно мнению Е.Р. Россинской [3], теория информационно-компьютерного обеспечения криминалистической деятельности включает в себя несколько ключевых компонентов:

1. Концепция теории, охватывающая ее предмет, задачи и объекты исследования. Эта концепция формирует теоретическую основу для системного анализа роли информационных технологий в криминалистике.

2. Учение о способах совершения компьютерных преступлений и правонарушений. Эти способы зачастую являются полноструктурными, включающими тщательно продуманные этапы подготовки, реализации и сокрытия преступления. Подготовительные действия направлены на минимизацию рисков обнаружения и максимизацию эффективности преступных действий. Закономерности, характеризующие способы совершения компьютерных преступлений, включают:

◆ связь способа с личностью преступника, его мотивацией и уровнем технической подготовки;

◆ зависимость способа от конкретных обстоятельств совершения преступления, таких как уровень защищенности информационных систем и наличие уязвимостей;

◆ отражение в компьютерных системах информации о действиях преступника, их результатах, повторяемости действий в различных ситуациях и стереотипах поведения.

3. Учение о цифровых следах как источниках криминалистически значимой информации. Цифровые следы могут включать широкий спектр данных – от логов и метаданных до остаточных файлов и сетевых артефактов. Их анализ требует специализированных знаний и навыков в области цифровой криминалистики.

4. Учение об информационно-компьютерных криминалистических моделях видов компьютерных преступлений.

5. Учение о криминалистическом исследовании компьютерных средств и систем, реализуемое в новом разделе криминалистической техники.

6. Учение об информационно-компьютерном криминалистическом обеспечении тактики следственных и судебных действий.

7. Учение об информационно-компьютерном криминалистическом обеспечении методик расследования компьютерных преступлений.

8. Учение о взаимосвязях и разграничениях цифровизации судебно-экспертной и криминалистической деятельности.

Данные теоретические выкладки рассматриваются также в работах таких авторов, как О.А. Зайцев, П.С. Пастухов «Формирование новой стратегии расследования преступлений в эпоху цифровой трансформации» [4], Т.В. Пинкевич «Предупреждение преступлений, совершаемых в сфере оборота цифровой валюты (криптовалюты)» [5].

Полагаем, что данная теория обладает высокой актуальностью для современного общества, учитывая стремительное развитие информационных технологий и их влияние на криминальную среду. Она должна быть предметом всестороннего исследования и активного внедрения в научные основы национальной криминалистики и судебной экспертологии, что позволит повысить эффективность расследования преступлений и качество судебных экспертиз.

Результаты и обсуждение

С появлением в обществе такого вида преступности появился и новый феномен – цифровое доказательство, а именно цифровой след.

Цифровой след* – это совокупность всех данных, которые оставляет пользователь при взаимодействии с электронными системами. Это могут быть лог-файлы с веб-сайтов, информация о перемещениях, цифровые документы, переписки в социальных сетях и даже записи с видеокамер наблюдения. Практически каждая деятельность в цифровом пространстве оставляет след, который может стать важным доказательством при расследовании преступлений. Нам импонирует определение понятия «цифровой след» Россинской Е.Р., которая описывает его «как новый объект судебной экспертизы. Его можно определить как криминалистически значимую компьютерную информацию о каких-либо событиях или действиях, отраженную в материальной среде в процессе возникновения, обработки, хранения и передачи этой информации» [6].

Цифровой след может включать в себя разнообразные данные, оставляемые пользователями при взаимодействии с цифровыми системами, и может стать решающим фактором в расследовании преступлений. Классифицируя цифровые следы, их можно выделить по следующим категориям [7]:

1. Метаданные файлов – информация о создании и изменении файлов, включая данные об авторе и времени, которые позволяют отслеживать источники и историю документации.
2. Интернет-следы – данные о действиях пользователей в сети, такие как посещение веб-страниц и загрузка файлов. Эта информация может быть найдена в истории браузера и других местах и используется для установления активности подозреваемого.
3. Метаданные изображений – включают информацию о месте, времени и устройстве, с которого была сделана фотография, что помогает в установлении подлинности изображений.
4. Мобильные следы – данные о звонках, сообщениях и геолокации, получаемые через операторов связи и анализ на самом устройстве, полезные для отслеживания перемещений подозреваемого.
5. Следы социальных сетей включают профили, комментарии и связи пользователя, что позволяет раскрывать его круг общения и возможные мотивы.
6. Системные логи – информация о действиях пользователей в операционных системах, таких как команды и ошибки, применяемая для выявления несанкционированного доступа и следов изменения данных.

Однако необходимо отметить, что цифровой след неотделим от его носителя, так как сам он не обладает материальной природой. Если рассмотреть более детально, то можно сделать логическое умозаключение, что носители цифровых следов – это устройства или среды, на которых сохраняются и передаются цифровые следы, представляющие собой электронные данные об активности пользователей. Эти носители могут включать как физические устройства, так и программные компоненты, которые фиксируют и хранят информацию, имеющую значение в правовом и судебном контексте: компьютерные устройства: жесткие диски (HDD) и твердотельные накопители (SSD) на компьютерах, которые содержат данные о файлах, метаданные и лог-файлы, фиксирующие пользовательские действия и настройки системы; мобильные устройства: смартфоны и планшеты фиксирующие данные о звонках, сообщениях, геолокации и активности приложений, которые являются важными для расследования инцидентов и анализа перемещений; сетевые и облачные сервисы: облачные серверы, веб-сайты и приложения, ко-

торые собирают интернет-следы, включая историю посещений, cookies и загруженные файлы, которые могут служить доказательствами в цифровом формате; лог-файлы и системные журналы: логи системных событий, действия операционных систем и приложений, которые фиксируются в системных файлах, позволяя восстанавливать хронологию событий и идентифицировать потенциальные нарушения; цифровые коммуникации: электронная почта, мессенджеры и социальные сети, фиксирующие переписки и другие действия, которые могут стать важными доказательствами в делах, связанных с киберпреступностью и мошенничеством; камеры наблюдения и системы видеонаблюдения: записи с камер представляют собой аудиовизуальные данные, которые документируют время и место событий и могут быть важны для идентификации участников и обстоятельств.

Для экспертов, работающих по данным направлениям судебных экспертиз, необходимо разрабатывать соответствующие методики экспертного исследования, включающие в себя технологии работы с носителями цифровых следов для их сохранности и пригодности с последующим их доказательственным значением в выводах экспертиз.

Для наглядности давайте проведем мониторинг роста преступлений с использованием информационно-телекоммуникационных технологий в Казахстане за 2022–2023 гг. Мы увидим, что в Казахстане наблюдался значительный рост преступлений, связанных с использованием информационно-телекоммуникационных технологий (ИКТ). Согласно данным Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан, в 2022 г. было зарегистрировано 13 000 интернет-преступлений [8].

В первом полугодии 2023 г. количество таких преступлений достигло 12 900, что на 46,3% больше по сравнению с аналогичным периодом 2022 г., когда было зафиксировано 8900 случаев [9].

За первые семь месяцев 2023 г. в Казахстане зарегистрировано 9000 преступлений, связанных с интернет- и телефонными мошенниками, из которых раскрыто только 2000, что составляет 22,2% [10].

Эти данные свидетельствуют о значительном увеличении количества преступлений с использованием ИКТ в Казахстане в 2023 г. по сравнению с 2022 г., подчеркивая необходимость усиления мер по обеспечению кибербезопасности и повышению эффективности правоохранительных органов в данной сфере.

Если провести такой же мониторинг за 2023 и 2024 гг., то мы увидим следующие данные: в 2023 г. в Республике Казахстан количество зарегистрированных киберпреступлений возросло на 46,3% по сравнению с предыдущим годом. Только в первом полугодии 2023 г. было зафиксировано около 12 900 таких преступлений, тогда как за аналогичный период 2022 г. их число составляло 8900 [11]. В 2024 г. тенденция к росту киберпреступлений продолжилась. По данным различных источников, количество атак и правонарушений, связанных с киберугрозами, увеличилось еще более интенсивно, затрагивая как частные компании, так и государственные организации Казахстана.

Рассмотрим, как данные проблемы решаются в международном пространстве. Ведущие страны мира, такие как США, Великобритания и члены Европейского союза, уже внедрили современные методы работы с цифровыми данными и разработали стандарты, регулирующие их использование в судебных процессах. Здесь приведем ключевые примеры международного опыта и потенциальные направления для Казахстана.

Опыт США: искусственный интеллект и автоматизация

В США широко применяются технологии искусственного интеллекта (ИИ) и автоматизированные системы для анализа доказательств. Например, системы для анализа ДНК и баллистических данных на основе ИИ позволяют сократить время обработки и снизить вероятность человеческой ошибки [12]. Важную роль играет и анализ цифровых следов: переписка, история посещения сайтов, данные лог-файлов – все это может использоваться как доказательства при расследовании киберпреступлений.

Опыт США подчеркивает, что успешная работа с ИИ требует как технической инфраструктуры, так и сертифицированных специалистов. Применение подобных технологий в Казахстане возможно при условии разработки стандартов и обязательной сертификации программного обеспечения, а также обучения специалистов.

Европейский союз: стандарты по цифровым доказательствам и правовая допустимость

В Европейском союзе особое внимание уделяется стандартизации и допустимости цифровых доказательств. Директива 2016/679 (GDPR) регулирует защиту данных и требует строгого соблюдения стандартов при работе с цифровыми доказательствами [13]. Регламенты Европола и Евроюста обеспечивают единые протоколы для трансграничных расследований, что важно для взаимодействия стран ЕС в борьбе с киберпреступностью.

Казахстан может использовать этот опыт для создания единого законодательства, регулирующего цифровые доказательства, чтобы обеспечить их правовую допустимость в судах. Это также важно для интеграции в международное сообщество и обмена данными по киберпреступлениям с другими странами.

Великобритания: централизованные цифровые платформы для хранения доказательств.

Великобритания разработала платформу Digital Evidence Vault, которая служит единым хранилищем цифровых доказательств и позволяет полицейским и судебным экспертам безопасно загружать, хранить и управлять доказательствами. Эта централизованная система обеспечивает сохранность данных, снижает вероятность их утраты и упрощает доступ к ним для участников расследования [14].

Для Казахстана создание подобной платформы могло бы помочь структурировать и защитить цифровые доказательства, снизить затраты на обработку данных и обеспечить более эффективное взаимодействие между ведомствами. Важным шагом при этом является разработка стандартов безопасности и шифрования данных.

Австралия: Национальный центр кибербезопасности.

Австралия внедрила Национальный центр кибербезопасности, который занимается как координацией киберанализа, так и обучением специалистов [15]. Центр разрабатывает новые методики для анализа киберугроз и исследует цифровые данные, а также взаимодействует с правоохранительными органами.

Казахстану было бы полезно создать аналогичный центр, который бы координировал деятельность по кибербезопасности и судебной экспертизе в цифровой сфере. Это позволит объединить усилия правоохранительных органов и повысить готовность киберэкспертов к работе с новыми угрозами.

В числе общих рекомендаций по учету вышеуказанного международного опыта можно обобщить до следующего:

1. Создание правовой базы. Казахстану необходимо разработать единое законодательство по цифровым доказательствам, включая правила их сбора, хранения и допустимости в суде. При этом можно ориентироваться на стандарты ЕС и США.

2. Внедрение сертификации программного обеспечения. Чтобы обеспечить надежность используемых технологий, Казахстану следует ввести обязательную сертификацию программ для судебной экспертизы. Это повысит доверие к результатам цифровых экспертиз.

3. Централизация хранения данных. Создание единой национальной платформы для хранения цифровых доказательств может облегчить доступ к данным, повысить их защиту и снизить затраты на их обработку. Опыт Великобритании показывает, что такие платформы позволяют эффективно управлять доказательствами.

4. Подготовка кадров и обучение. Важно разработать образовательные программы по кибербезопасности и судебной экспертизе для подготовки специалистов, способных работать с цифровыми доказательствами. Совместные проекты с международными организациями могли бы усилить качество подготовки кадров.

5. Международное сотрудничество и обмен данными. Подписание соглашений о международном обмене цифровыми доказательствами и признание экспертиз, проведенных в других странах, позволят Казахстану интегрироваться в мировое сообщество и более эффективно бороться с киберпреступностью.

Можно сказать, что международный опыт показывает, что цифровизация судебно-экспертной деятельности требует не только технологических инноваций, но и глубоких изменений в правовой базе и системе подготовки кадров. Казахстану полезно учитывать успешные примеры США, ЕС, Великобритании и Австралии, чтобы создать устойчивую и эффективную систему цифровой судебной экспертизы, способную справляться с новыми вызовами цифрового мира.

Заключение

Учитывая вышесказанное, можно выделить следующие важные аспекты по цифровизации судебно-экспертной деятельности в РК:

1. Разработать новый вид криминалистического учения, по исследованию компьютерных средств и систем, где будет собрана криминалистическая дефиниция цифровых следов, их виды и способы собирания.

2. В судебной экспертологии разработать новую частную теорию – теорию цифровизации судебно-экспертной деятельности, которая наряду с другими теориями (судебно-экспертной идентификации, судебно-экспертной диагностики и др.) имела бы общий характер для всех родов и видов судебных экспертиз, где предметом данной теории являются закономерности судебно-экспертного исследования цифровых следов, образующихся вследствие возникновения, движения и преобразования компьютерной информации, имеющее доказательственное или розыскное значение в уголовном, гражданском, административном судопроизводстве, а его объектами – цифровые следы и компьютерные средства и системы как носители розыскной и доказательно значимой информации.

3. Усовершенствование методологических разработок, методов и средств с учетом комплексирования цифровых следов по различным родам и видам судебных экспертиз.

4. Унификация и нормативная регламентация цифровых баз с возможностью их использования как в Казахстане, так и на международном уровне.

5. Разработка и использования справочно-информационных фондов (СИФ)1, основанных на цифровых технологиях, и нормативное регулирование их как государственными, так и негосударственными судебно-экспертными учреждениями, в т.ч. и на международном уровне.

6. Разработка современного программного обеспечения (ПО), которое позволит осуществлять хранение, обработку результатов исследований и обмен данными с неограниченным кругом пользователей в экспертном сообществе, в т.ч. и на международном уровне.

7. Цифровизация сфер судебно-экспертной и криминалистической отраслей с целью объединения их в единые АИПС (автоматизированные информационно-поисковые системы) для наиболее эффективного учета цифровых следов (АИПС криминалистического и судебно-экспертного назначения).

ЛИТЕРАТУРА

1 Уголовно-процессуальный Кодекс Республики Казахстан (с изменениями и дополнениями по состоянию на 12.09.2023 г.). Ст. 121 п. 1.

2 Понятие и виды преступлений в сфере информационных технологий в России и зарубежных странах: из истории в современность // Криминологический журнал. – 2023. – № 4. – С. 45. URL: https://cyberleninka.ru/article/n/ponyatie-i-vidy-prestupleniy-v-sfere-informatsionnyh-tehnologiy-v-rossii-i-zarubezhnyh-stranah-iz-istorii-v-sovremennost

3 Россинская Е.Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского Института МВД России. – 2019. – № 2(89). – С. 198–199.

4 Зайцев О.А., Пастухов П.С. Формирование новой стратегии расследования преступлений в эпоху цифровой трансформации // Вестник Пермского университета. Юридические науки. – 2019.

5 Пинкевич Т.В. Предупреждение преступлений, совершаемых в сфере оборота цифровой валюты (криптовалюты) // Право и государство: теория и практика. – 2021.

6. Россинская Е.Р. Учение о цифровизации судебно-экспертной деятельности и проблемы судебно-экспертной дидактики // Вестник ун-та им. О.Е. Кутафина (МГЮА). – 2020. – № 4(62). – С. 91.

[1] СИФы – это автоматизированные информационно поисковые системы по конкретным объектам криминалистического и судебно-экспертного исследования.

7. Гайдаш О.В. Феномен цифрового следа в современном обществе, вестник магистратуры. – 2020. – № 6(105). – С. 11.

8 Казинформ. URL: https://www.inform.kz/ru/za-7-mesyacev-2022-goda-v-rk-zaregistrirovano-11-tys-internet-prestupleniy_a3967587

9 Мир финансов. URL: https://wfin.kz/publikatsii/kazakhstan-v-tsifrakh/91787-v-kazakhstane-rastjot-chislo-kiber-prestuplenij.html

10 Курсив. URL: https://kz.kursiv.media/2023-07-17/lnsh-raskryvaemost/

11 URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/

12 Holt T.J., Bossler A.M. Cybercrime in Progress. Routledge, 2019.

13 European Commission. General Data Protection Regulation. 2016.

14 Home Office Digital. Digital Evidence Vault Initiative. UK, 2020.

15 Australian Cyber Security Centre. National Cyber Security Strategy. 2021.

REFERENCES

1 Ugolovno-processual'nyj Kodeks Respubliki Kazahstan (s izmenenijami i dopolnenijami po sostojaniju na 12.09.2023 g.). St. 121 p. 1. (In Russian).

2 Ponjatie i vidy prestuplenij v sfere informacionnyh tehnologij v Rossii i zarubezhnyh stranah: iz istorii v sovremennost' // Kriminologicheskij zhurnal. 2023. No. 4. P. 45. URL: https://cyberleninka.ru/article/n/ponyatie-i-vidy-prestupleniy-v-sfere-informatsionnyh-tehnologiy-v-rossii-i-zarubezhnyh-stranah-iz-istorii-v-sovremennost. (In Russian).

3 Rossinskaja E.R. (2019) Teorija informacionno-komp'juternogo obespechenija kriminalisticheskoj dejatel'nosti: koncepcija, sistema, osnovnye zakonomernosti // Vestnik Vostochno-Sibirskogo Instituta MVD Rossii. No. 2(89). P. 198–199. (In Russian).

4 Zajcev O.A., Pastuhov P.S. (2019) Formirovanie novoj strategii rassledovanija prestuplenij v jepohu cifrovoj transformacii // Vestnik Permskogo universiteta. Juridicheskie nauki. (In Russian).

5 Pinkevich T.V. (2021) Preduprezhdenie prestuplenij, sovershaemyh v sfere oborota cifrovoj valjuty (kriptovaljuty) // Pravo i gosudarstvo: teorija i praktika. (In Russian).

6. Rossinskaja E.R. (2020) Uchenie o cifrovizacii sudebno-jekspertnoj dejatel'nosti i problemy sudebno-jekspertnoj didaktiki // Vestnik un-ta im. O.E. Kutafina (MGJuA). No. 4(62). P. 91. (In Russian).

7. Gajdash O.V. (2020) Fenomen cifrovogo sleda v sovremennom obshhestve, vestnik magistratury. No. 6(105). P. 11. (In Russian).

8 Kazinform. URL: https://www.inform.kz/ru/za-7-mesyacev-2022-goda-v-rk-zaregistrirovano-11-tys-internet-prestupleniy_a3967587. (In Russian).

9 Mir finansov. URL: https://wfin.kz/publikatsii/kazakhstan-v-tsifrakh/91787-v-kazakhstane-rastjot-chislo-kiber-prestuplenij.html. (In Russian).

10 Kursiv. URL: https://kz.kursiv.media/2023-07-17/lnsh-raskryvaemost/. (In Russian).

11 URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/. (In English).

12 Holt T.J., Bossler A.M. (2019) Cybercrime in Progress. Routledge, . (In English).

13 European Commission. General Data Protection Regulation. 2016. (In English).

14 Home Office Digital. Digital Evidence Vault Initiative. UK, 2020. (In English).

15 Australian Cyber Security Centre. National Cyber Security Strategy. 2021. (In English).

АЛАЕВА Г.Т.,[1]
з.ғ.к., профессор.
e-mail: g.alayeva@turan-edu.kz
ORCID ID: 0000-0003-1672-2238
КАБДОЛДИНА Е.В.,*[1]
магистрант.
*e-mail: 23242635@turan-edu.kz
ORCID ID: 0009-0007-9919-1036
[1]«Туран» университеті,
Алматы қ., Қазақстан

ҚАЗАҚСТАНДА ЖӘНЕ ӘЛЕМДЕ СОТ САРАПТАМАСЫНДА ЦИФРЛЫҚ ТЕХНОЛОГИЯЛАРДЫ ҚОЛДАНУ: ПЕРСПЕКТИВАЛАР МЕН СЫН-ҚАТЕРЛЕР

Аңдатпа

Адам өмірінің барлық саласын қамтыған жалпы цифрландыру қылмыстық, азаматтық және әкімшілік істер бойынша дәлелдерді жинау және зерттеу үдерістеріне, әсіресе криминалистика және сот-сараптамалық қызмет салаларына арнайы ғылыми білімдерді қолдану арқылы енгізілуде. Бұл мақалада компьютерлік қылмыстардың түрлері және олардың көрініс табатын салалары, сонымен қатар жаңа дәлел түрі – «цифрлық» дәлелдер, атап айтқанда, «цифрлық іздің» пайда болуы қарастырылады. Мақалада цифрлық іздер мен олардың тасымалдаушылардың категориялары талданады. Сондай-ақ, мақалада Қазақстанда 2022–2023, 2023–2024 жылдар аралығында ақпараттық-коммуникациялық технологияларды пайдалану арқылы жасалған қылмыстардың өсуіне мониторинг жүргізіліп, мұндай қылмыстардың жылдан-жылға артып келе жатқанын көрсететін нақты мәліметтер келтірілген. Киберқылмыстардың санының көбеюін, олардың қарқынды өсуін, жаңа «цифрлық» дәлелдер түрлерінің пайда болуын ескере отырып, мақалада компьютерлік құралдар мен жүйелерді зерттеуге арналған нақты шаралар ұсынылады. Онда цифрлық іздердің криминалистикалық анықтамасы, олардың түрлері мен жинау әдістері, цифрлық базаларды Қазақстанда және халықаралық деңгейде қолдануға мүмкіндік беретін нормативтік реттеу және біріздендіру ұсынылады. Сонымен қатар, цифрлық іздерді тиімді есепке алу мақсатында сот-сараптамалық және криминалистикалық салаларды цифрландыруды, оларды бірыңғай АІЗЖ (Автоматтандырылған ақпараттық-іздеу жүйелері) жүйесіне біріктіру шаралары ұсынылады (криминалистикалық және сот-сараптамалық мақсаттағы АІЗЖ).

Тірек сөздер: цифрландыру, сот-сараптамалық қызмет, компьютерлік технологиялар, киберқылмыстар, компьютерлік қылмыстар, фишинг, цифрлық дәлелдер.

ALAYEVA G.T.,[1]
c.l.s., professor.
e-mail: g.alayeva@turan-edu.kz
ORCID ID: 0000-0003-1672-2238
KABDOLDINA Y.V.,*[1]
master's student.
*e-mail: 23242635@turan-edu.kz
ORCID ID: 0009-0007-9919-1036
[1]Turan University,
Almaty, Kazakhstan

USE OF DIGITAL TECHNOLOGIES IN FORENSIC EXPERTISE IN KAZAKHSTAN AND WORLDWIDE: PROSPECTS AND CHALLENGES

Abstract

The widespread digitalization that has encompassed all spheres of human life is also being integrated into the processes of gathering and examining evidence in criminal, civil, and administrative cases using specialized scientific knowledge, particularly in the fields of forensics and forensic expertise. This article explores types of computer crimes and their spheres of occurrence, as well as the emergence of a new type of evidence – "digital" evidence,

specifically the “digital” trace. The article examines categories of digital traces and their carriers. It also includes a monitoring of the increase in crimes involving information and telecommunication technologies in Kazakhstan for 2022–2023 and 2023–2024, clearly presenting figures that indicate a growing trend in these types of crimes year by year. Given the increase in cybercrime and its rapid growth, along with the emergence of new types of evidence – “digital” evidence – the article proposes specific measures for investigating computer devices and systems, where a forensic definition of digital traces, their types, and methods of collection are outlined, along with the unification and regulatory standardization of digital databases for potential use in Kazakhstan and internationally. Additionally, measures are proposed for the digitalization of forensic and investigative fields, aiming to integrate them into unified AIPS (Automated Information Retrieval Systems) for the most effective tracking of digital traces (AIPS for forensic and forensic expert purposes).

Key words: digitalization, Forensic expert activity, Computer technology, Cybercrime, Computer crime, Phishing, Digital evidence.