ст. / Могилев. ин-т М-ва внутр. дел Респ. Беларусь ; редкол.: И. А. Демидова (отв. ред.) [и др.]. – Могилев, 2022. – С. 432–438.

8. Дыжова, А.А. Проблемы правового воспитания студенческой молодежи / А.А. Дыжова // Вестн. Фак. бизнеса и права. – 2019. – № 1. – С. 119–125.

9. Об основах деятельности по профилактике правонарушений [Электронный ресурс] : Закон Республики Беларусь, 4 янв. 2014, № 122-З : в ред. от 17.07.2023 г. № 292-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

К ВОПРОСУ ПРИМЕНЕНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В КРИМИНАЛИСТИКЕ

Мамекин Д.Н., Цехновецкая В.М.

В современном мире цифровые технологии играют значительную роль в различных сферах жизни общества, включая криминалистику. В Республике Беларусь, как и во многих других государствах, законодательство регулирует использование цифровых технологий при расследовании преступлений. В данной статье рассмотрим основные аспекты применения цифровых технологий в криминалистических исследованиях в соответствии с действующим законодательством Республики Беларусь.

Использование цифровых технологий в сфере криминалистики в Беларуси регулируется Уголовно-процессуальным кодексом, Законом «О судебно-экспертной деятельности», а также другими нормативными правовыми актами. В этих документах определены основные принципы и правила применения электронных устройств и информационных ресурсов при расследовании уголовных дел.

1) Одним из основных направлений применения цифровых технологий является сбор и использование электронных (цифровых) доказательств. Электронные (цифровые) доказательства могут включать различные данные, хранящиеся на компьютерах, мобильных устройствах, серверах и других носителях информации. Важным аспектом является то, что электронные (цифровые) доказательства должны быть собраны, сохранены и использованы в соответствии с требованиями законодательства.

В современном мире, где технологии стали неотъемлемой частью повседневной жизни, множество преступлений оставляют цифровые следы. Так, например, почти у каждого дома есть электронные устройства (робот-пылесос, умный дом и т.д), на которых хранится информация о местоположении, активности и поведении как жертв, так и преступников. Все это может служить как источником доказательств, так и местом совершения преступления.

Использование цифровых доказательств в криминалистической тактике включает в себя сбор, анализ и интерпретацию данных, полученных из различных источников. Это может быть изъятие информации с компьютеров, мобильных устройств, видеонаблюдения, интернет-трафика и так далее. От детального изучения метаданных до восстановления удаленной информации - криминалисты используют широкий спектр инструментов для получения цифровых доказательств. Они могут установить связи между подозреваемыми и жертвами, подтвердить место нахождения в определенное время, обнаружить удаленную информацию или даже определить психологический профиль преступника [1].

С увеличением использования цифровых технологий важность кибербезопасности также возрастает. Это включает в себя защиту цифровых доказательств от взлома, а также обеспечение защиты персональных данных.

Для проведения экспертизы электронных устройств, связанных с расследованием преступлений, привлекаются специалисты в области информационных технологий и компьютерной техники.

Для того, чтобы обнаруженные следы, а также иная значимая для дела информация стали допустимыми доказательствами, важно соблюдать процессуальные и технические

правила работы с ними.

На вооружении правоохранительных органов имеются такие технико-криминалистические средства, с помощью которых можно:

– извлекать всю имеющуюся информацию из памяти устройства, в том числе удаленную;

– устанавливать местонахождение конкретного электронного устройства и соответственно лица, которое в данный момент им пользуется. (с помощью геоданных, метаданных фото-видеофайлов, по приемным и передающим модулям систем GPS, по беспроводным сетям Wi-Fi);

– проводить анализ контактов участников преступных групп и сообществ, устанавливать наиболее активных участников, выявлять лидеров, доказывать период общения ее участников.

Однако, на практике возникает вопрос что же точно будет относиться к электронным доказательствам, поскольку в Уголовно-процессуальном кодексе нет такого понятия. В связи с этим, согласно Уголовно-процессуальному кодексу Республики Беларусь, доказательства - - любые фактические данные, полученные в предусмотренном законом порядке, на основе которых орган, ведущий уголовный процесс, устанавливает наличие или отсутствие общественно опасного деяния, предусмотренного уголовным законом, виновность лица, совершившего это деяние, либо его невиновность и иные обстоятельства, имеющие значение для правильного разрешения уголовного дела. Доказательствами являются материалы фото- и киносъемки, звуко- и видеозаписи, а также иные носители информации, полученные и предъявленные в порядке, установленном законом. Такие материалы могут отражать ход проведения каких-либо следственных или оперативных действий, или факты и события предполагаемого преступления, и поэтому их обычно подразумевают под понятием электронных доказательств.

В Республике Беларусь, как и в большинстве стран постсоветского пространства, еще не сложилась устоявшаяся практика расследования преступлений с использованием цифровых данных, но, стоит отметить, правовое регулирование использования цифровой информации развивается, однако, на сегодняшний день отсутствует норма, регулирующая данные правоотношения.

2) Современные цифровые технологии, такие как искусственный интеллект и машинное обучение, также находят применение в криминалистике. Криминалистика всегда отличалась высокой восприимчивостью к технологиям, потенциально полезным в выявлении и раскрытии преступлений, так что рассмотрение перспектив использования искусственного интеллекта должно представлять для нее интерес.

Одним из основных способов использования искусственного интеллекта в криминалистике является обработка и анализ больших массивов данных, таких как отпечатки пальцев, ДНК и видеофайлы. Алгоритмы машинного обучения позволяют автоматически выявлять узоры и связи, которые могли бы остаться незамеченными для человека.

Кроме того, искусственный интеллект используется для разработки программного обеспечения, которое помогает в расследовании преступлений. Например, с помощью нейронных сетей и компьютерного зрения можно автоматически распознавать лица на видеозаписях, что значительно ускоряет процесс идентификации подозреваемых [2].

Также искусственный интеллект используется для предсказания преступлений и анализа тенденций. Алгоритмы могут анализировать статистические данные и выявлять общие закономерности, что помогает в принятии мер по предотвращению преступлений и улучшению общественной безопасности.

Современной криминалистике известны разные проекты, компьютеризирующие решение некоторых задач, возникающих в процессе раскрытия и расследования преступлений. Наиболее известными являются проект ученых Нижегородского университета им. Лобачевского «ФОРВЕР», позволяющий формировать наиболее перспективные версии о личности преступника.

Помимо этого, в практике раскрытия и расследования преступлений активно используются автоматизированные информационно-поисковые системы, позволяющие получать информацию о возможных направлениях расследования. Так, например, в соответствии с рекомендациями, разработанными ФАТФ, Росфинмониторинг создал программу «Прозрачный блокчейн» в 2021 году, основным направлением которой является обеспечение возможности двигаться по цепочке – увидеть отправителя и получателя средств денежных средств при преступных схемах. «Прозрачный блокчейн» представляет собой цифровую книгу записей, которые упорядочены в блоки и связаны с помощью криптографии. Преимуществами блокчейна являются: прозрачность, эффективность, неизменность и децентрализацию, что делает его идеальным инструментом для борьбы с коррупцией. Так, данную программу в 2023 году запустили не только на территории Российской Федерации, а и в ряде центрально-азиатских стран [3].

Таким образом, цифровые технологии играют важную роль в криминалистике Беларуси, обеспечивая сбор и анализ электронных доказательств, проведение экспертиз электронных устройств и применение искусственного интеллекта. Однако использование этих технологий должно осуществляться в соответствии с действующими законодательными нормами, которые постоянно совершенствуются, чтобы обеспечить объективность и достоверность результатов расследований. Так, с целью совершенствования работы следственных групп и экспертов-криминалистов в ходе следственных действий мы предлагаем следующее:

1. Цифровые данные могут использоваться как источник доказательств в уголовном процессе. Но для этого требуются совершенствование национального законодательства и разработка специальных методов проведения следственных действий по сбору, хранению и использованию таких доказательств. Необходимо, с одной стороны, привлекать к работе специалистов, обладающих техническими знаниями, а с другой стороны, надлежащим образом разрабатывать правила и алгоритмы по сбору цифровых данных с информационных платформ (запрос к оператору, распоряжения о предоставлении информации, привлечение специалистов для раскодирования информации).

2. Современная криминалистика неразрывно связана с современными технологиями. В связи с этим целесообразно внедрять различные программы для решения задач при расследовании преступлений. В частности, Республике Беларусь необходимо последовать примеру Российской Федерации и запустить программу «Прозрачный блокчейн» с целью более углубленного анализа субъектов преступлений в экономической сфере, а также международного сотрудничества в рамках рекомендаций ФАТФ, являющейся основой для создания эффективных систем ПОД/ФТ. Использование программы «Прозрачный блокчейн» поможет в расследовании преступлений, связанных с коррупционной деятельностью.

Литература:

1. Цифровые данные как новый источник доказательств в уголовном процессе [Электронный ресурс]. – Режим доступа: http://edoc.bseu.by:8080/bitstream/edoc/97431/– Дата доступа: 06.12.2023.

2. Искусственный интеллект в криминалистике: состояние и перспективы использования [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-kriminalistike-sostoyanie-i-perspektivy-ispolzovaniya. – Дата доступа: 06.12.2023.

3. Прозрачный блокчейн [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/Продукт:Прозрачный_блокчейн. –Дата доступа: 06.12.2023.