

Процессуальные документы, составленные при выездных мероприятиях (протокол осмотра места происшествия, протокол обыска и т. д.) либо иные документы, оформленные на бумажном носителе, переводятся в формат PDF с последующим вложением в модуль е-УД незамедлительно, но не позднее 24-х часов после совершения действия.

Процесс ведения досудебного расследования облегчается также наличием в ИС ЕРДР 350 шаблонов базовых процессуальных документов. Следователь ведет уголовное дело, используя указанные шаблоны, но текст документа создает самостоятельно.

Благодаря интеграции ИС ЕРДР с информационной системой Верховного Суда РК «Төрелік» материалы о санкционировании следственных, негласных следственных действий, о санкционировании меры пресечения в отношении подозреваемого лица также направляются в электронном виде.

В настоящее время ведется поэтапное подключение ИВС органов внутренних дел к судам для дистанционного рассмотрения ходатайств о санкционировании содержания под стражей, что повысит исключение рисков побега, экономия бюджетных средств на конвоирование, экономию процессуального времени.

Также с помощью системы информационного обмена государственных, правоохранительных, специальных и иных органов (СИО ПСО) следователь в рамках расследования может получать сведения из 89 баз данных госорганов.

Лицо, ведущее досудебное расследование, имеет возможность при помощи АРМ (автоматическое рабочее место) «Криминалист» и «Экспертиза» назначать все виды криминалистических исследований, судебных экспертиз и получать заключения в режиме онлайн.

При необходимости уведомления участников уголовного процесса следователь может воспользоваться бесплатным SMS-оповещением непосредственно в ИС ЕРДР, которое поступит на мобильный номер либо на электронную почту участника процесса.

Объем необходимых материалов для участников процесса, доступных в режиме онлайн, следователь определяет в соответствии с УПК.

Участники уголовного процесса подписывают процессуальные документы с помощью ЭЦП либо графического планшета, используя стилус.

По завершении досудебного расследования, следователь в соответствии с ч.1 ст. 299 УПК направляет уголовное дело прокурору.

Прокурор по завершении изучения материалов уголовного дела в случае направления его в суд утверждает либо составляет новый обвинительный акт (ст. 302 УПК).

Таким образом, модернизация уголовного процесса посредством перехода на электронный формат повышает его прозрачность и позволяет более доступно реализовывать имеющийся объем прав участников уголовного процесса, граждане в любое время могут получить прямой доступ к процессуальным документам в режиме онлайн, подавать жалобы и ходатайства (функционал «Публичный сектор»). Прозрачность уголовного процесса повысит ответственность сотрудников правоохранительных органов и, как следствие, защиту прав граждан от произвола и незаконных методов расследования.

УДК 343.1

Т.В. Ахраменко

ОСОБЕННОСТИ ОЦЕНКИ ЭЛЕКТРОННОГО ДОКУМЕНТА КАК ИСТОЧНИКА КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ

Электронный документ приобретает значение доказательств в уголовном судопроизводстве, когда он отвечает требованиям относимости, допустимости и достоверности.

Под относимостью понимается отношение установленных доказательств к предмету доказывания или отдельным его элементам. При оценке электронного документа с данной позиции предполагается, что содержащиеся в нем сведения отражают круг обстоятельств, входящих в предмет доказывания по делу, либо выступают в качестве так называемых промежуточных фактов. Иными словами, в данном случае следует вести речь о том, каким образом электронный документ содержательный и логически связан с расследуемым событием и какую лепту он способен внести в общую информационную картину.

Под допустимостью следует понимать пригодность полученного электронного документа в качестве судебных доказательств и возможность его использования в процессе доказывания. Обязательным требованием здесь является то, что доказательства должны быть собраны в соответствии с требованиями закона: надлежащим субъектом, в надлежащем порядке и из надлежащих источников. То есть в уголовном деле должны содержаться данные о том, каким образом тот или иной информационный объект, представленный электронным документом, был приобщен к материалам уголовного дела.

Следует отметить, что вопросы проверки относимости полученных электронных документов к расследуемому событию и исследования процессуальных параметров их допустимости подробно освещены в научной литературе и на практике могут быть решены достаточно эффективно. Гораздо острее представляется проблема достоверности, обуславливаемая прежде всего гносеологической сутью электронного документа.

Документы вообще и электронные документы в частности как источники криминалистически значимой информации могут быть представлены в виде:

протоколов допросов, других следственных и процессуальных действий; заключения эксперта;

иных документов, которые допускаются в качестве доказательств, если изложенные в них сведения имеют значение для установления обстоятельств по делу. При этом они могут содержать сведения, зафиксированные как в письменном, так и в ином виде. К ним могут относиться материалы фото- и киносъемки, аудио- и видеозаписи, иные носители информации;

вещественных доказательств в случаях, если они служили орудиями преступления или сохранили на себе следы преступления, либо были объектом, на который были направлены преступные действия, или если они могут служить средством для обнаружения преступления и установления обстоятельств, имеющих значение для уголовного дела.

В соответствии со ст. 1 Закона Республики Беларусь «Об электронном документе и электронной цифровой подписи» данные (информация), полученные, хранимые, обрабатываемые и передаваемые с помощью автоматизированных информационных и телекоммуникационных систем могут признаваться в качестве документов, имеющих юридическую силу. Для этого такой документ должен быть оформлен с соблюдением норм, установленных соответствующим стандартом. Юридическая сила документа может подтверждаться электронной цифровой подписью. Последняя одновременно служит подтверждением достоверности передаваемой при помощи ЭВМ документации, а также свидетельством того, что она составлена и подписана должным образом уполномоченным лицом. Электронная цифровая подпись является средством защиты, которое позволяет обезопасить информацию от несанкционированного прочтения, изменения и подлога вне зависимости от степени защиты канала связи.

Суть электронной цифровой подписи заключается в персонализации всех возможных физических и юридических лиц, за которыми закрепляются персональные идентификационные номера, и криптографической привязке цифровых данных, подписанных этим лицом, таким образом, что любое изменение содержимого файла-документа с электронной цифровой подписью четко проявляется как нарушение аутентичности данного цифрового документа. Электронная цифровая подпись – это добавляемый к конкретному сообщению (тексту, файлу данных или любому набору битов произвольной длины) блок информации фиксированной длины, который позволяет обеспечить:

- подтверждение аутентичности исходного сообщения путем проверки подлинности его источника;
- подтверждение целостности сообщения (отсутствия его несанкционированных изменений);
- гарантии невозможности отказа от авторства сообщения (подписи).

Если электронной цифровой подписью подписывается файл целиком (причем это может быть файл, содержащий как текст, так и графику), то электронная цифровая подпись обычно формируется в виде отдельного файла, прилагаемого к подписанному документу.

Следует отметить, что электронная цифровая подпись не является универсальным средством защиты электронных документов. В некоторых областях информационной деятельности человека этого может быть вполне достаточно. Например, для всевозможных финансовых операций, в которых документы и электронная цифровая подпись имеют ограниченный срок действия (на время действия лицензии). В то же время множество проблем возникает в правоохранительной сфере, где широко распространенные цифровые формы хранения фотографий, видеозаписей и фонограмм оказываются невостребованными по причине того, что современной форме цифровых записей нет доверия. Даже неспециалисту понятно, что, используя современные технические средства, любую фотографию, видеозапись или фонограмму, выполненные цифровым способом, можно отредактировать таким образом, что их содержание изменится, а видимых и явных следов монтажа не останется.

В качестве альтернативы электронной цифровой подписи отдельными учеными предлагается вводить цифровые «водяные знаки», которые добавляются в структуру того или иного документа. Основное внимание при разработках, связанных с встраиванием «водяных знаков» в электронные документы (такие, как музыкальные записи, видеозаписи, фотографии и т. д.), уделяется не проблеме возможного монтажа этих записей, а проблеме незаметной маркировки самой цифровой записи в целом или ее отдельных фрагментов таким образом, чтобы по этим меткам можно было доказать, что эта цифровая запись принадлежит конкретному автору. При этом должен учитываться тот факт, что электронные документы, имеющие в большинстве случаев очень большой объем, передаются по каналам связи в сжатом или заархивированном виде. Следовательно, эти метки должны сохраняться и в случае компрессии данных, при которой, возможно, будет потеряна часть полезной информации, а вместе с ней и часть информации о внесенных защитных метках. Здесь также возникают определенные проблемы, и мы полагаем, что для «водяных знаков», предназначенных для защиты цифровых записей, необходимы специальные защитные структуры, следы которых статистически достаточно надежно обнаруживались бы на самых малых участках документов, на которых в принципе может производиться монтаж, меняющий содержание документа.

Указанные обстоятельства детерминируют особый порядок оценки достоверности электронных документов, предполагающий выработку определенного алгоритма действий субъекта доказывания, включая использование специальных знаний в области цифровых технологий. Кроме того, учитывая тот факт, что в уголовном судопроизводстве чаще всего имеют место документы, не содержащие вообще никаких средств защиты (документы открытого доступа), следует признать, что проблема использования электронного документа как источника доказательств в настоящее время все более актуализируется и требует дальнейших углубленных исследований, а также разработки комплексных средств защиты от несанкционированного доступа и редактирования в процессе расследования уголовного дела и рассмотрения его в суде.

УДК 343.985

Н.Н. Беломытцев

О СТРУКТУРЕ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ХИЩЕНИЙ, СОВЕРШЕННЫХ ПУТЕМ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОЙ ТЕХНИКИ

Криминалистическая характеристика преступлений в теории криминалистики – абстрактное научное понятие, результат научного анализа определенного вида преступной деятельности (вида или рода преступления), обобщения его типичных признаков и особенностей (Р.С. Белкин). Суть данной характеристики заключается в исключительно поисковом, ориентирующем