**Правовое понятие и виды документов на машинном носителе**

Сегодня очень трудно найти человека, который бы не слышал об электронной почте, электронном переводе денег, электронной странице «Интернет», сайте, пластиковой карте, SMS-сообщении, файле, программе для ЭВМ, базе данных, бездокументарной ценной бумаге, а также цифровой фотосъемке, видео- и аудиозаписи. Документы на машинном носителе прочно вошли в нашу жизнь. Они все чаще становятся предметом и средством совершения различных правонарушений, являются доказательствами в уголовном, гражданском и арбитражном процессе.

Под воздействием стремительного процесса компьютеризации российского общества неуклонно возрастает число физических и юридических лиц, применяющих разнообразные автоматизированные сети и системы для создания, обработки и электронной передачи документированной информации. На смену бумажным технологиям приходят так называемые «безбумажные», основанные на использовании средств электронно–вычислительной техники и электросвязи, одним из продуктов которых являются документы на машинном носителе.

В соответствии со ст. 2 Закона Российской Федерации от 20.02.95 г. № 24-ФЗ «Об информации, информатизации и защите информации» документированная информация (документ) – это зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать. При этом, документом на машинном носителе считается документ, созданный с использованием носителей и способов записи, обеспечивающих обработку его информации электронной вычислительной машиной (ЭВМ)1. Известно, что ЭВМ обрабатывает исключительно компьютерную информацию – сведения о лицах, предметах, фактах, событиях, явлениях и процессах, зафиксированные на машинном носителе в форме, доступной восприятию ЭВМ. Таким образом, документом на машинном носителе можно считать компьютерную информацию, которая имеет реквизиты, позволяющие ее идентифицировать.

С учетом изложенного, в качестве общих юридических признаков документа на машинном носителе можно выделить:

1. Машинный носитель информации;

2. Компьютерную информацию;

3. Реквизиты, позволяющие идентифицировать форму и содержание компьютерной информации.

Рассмотрим их более подробно.

Компьютерная информация всегда опосредована через машинный (физический) носитель информации, вне которого она не может существовать. Машинный носитель информации (МНИ) – это любое техническое устройство либо физическое поле2, предназначенное для фиксации, хранения, накопления, преобразования и передачи компьютерной информации. Наиболее распространены следующие виды машинных носителей информации:

• внутренний накопитель на жестком магнитном или магнитооптическом диске (НЖМД или НМОД – винчестер);

• внешний накопитель на жестком магнитном диске (ЗИП-драйвер);

• внешнее устройство накопления информации (стриммер);

• накопитель на магнитной ленте или специальной металлической нити (в кассетах или бобинах);

• гибкий магнитный диск (ГМД – дискета);

• оптический или магнитооптический диск (лазерный или компакт - диск);

• бумага, полимерная (пластиковая) пленка или тонколистовой металл (в виде карты или ленты);

• интегральная микросхема памяти (ИМСП) – микроэлектронное изделие окончательной или промежуточной формы, предназначенное для выполнения функций электронной схемы памяти ЭВМ и других компьютерных устройств, элементы и связи которого неразрывно сформированы в объеме и (или) на поверхности материала, на основе которого изготовлено изделие3;

• физическое поле – материальный носитель физических взаимодействий искусственного происхождения.

Компьютерная информация может содержаться на машинном носителе в следующих формах, доступных восприятию ЭВМ:

1. Электромагнитных сигналов – средств переноса компьютерной информации в пространстве и во времени с помощью электромагнитных колебаний (волн):4 характеризуется частотой колебаний, измеряемых в герцах (Гц). Из всех видов электромагнитных сигналов для фиксации и переноса документальных сообщений в основном используются радиосигналы, инфракрасные и световые.

2. Электрических сигналов – средств переноса компьютерной информации по проводникам с помощью упорядоченного движения заряженных частиц: характеризуется напряжением (измеряется в вольтах), силой (измеряется в амперах) и частотой пульсации (измеряется в герцах) тока.

3. Магнитных меток (магнитных доменов) – способа записи информации на машинный магнитный носитель (диск, ленту, проволоку, карту) путем создании на нем участков с различной степенью напряженности магнитного поля или противоположными направлениями магнитной ориентации.

4. Оптических меток – пит (от англ. «pits»– «ямка). Пита представляет собой ямку, пузырек, сквозное отверстие, точечно сплавленное либо сглаженное (текстурированное) образование различных геометрических размеров, полученное с помощью луча лазера на поверхности или в объеме пластика, из которого изготовлен оптический или магнитооптический МНИ (диск или карта).

5. Штрих-кода – параллельных черно - белых графических линий одинаковой высоты, но разной ширины. Их наносят на МНИ с помощью красителя различными печатающими устройствами, например, принтерами либо специальными электронно - цифровыми маркираторами.

6. Сквозных отверстий, имеющих круглую, овальную или прямоугольную форму. С их помощью компьютерная информация записывается на перфоленту или перфокарту.

Основным реквизитом, позволяющим ЭВМ идентифицировать форму компьютерной информации, является стандарт передачи информации в канале электросвязи или формат ее записи на машинный носитель.

В связи с тем, что информация находится в машиночитаемой форме, которая непосредственно не доступна восприятию человеком (за исключением видимых форм записи), используются дополнительные идентификационные реквизиты. Они позволяют определить вид документа на машинном носителе и конкретное средство электронно – вычислительной техники (компьютерное устройство или программу для ЭВМ), которое необходимо использовать для перевода его содержания в человекочитаемую форму. Как правило, ими являются атрибуты файла.

Файл – это поименованная область записей на МНИ, где в закодированном виде хранится строго определенная информация с реквизитами, позволяющими ее идентифицировать. Как в библиотеке, архиве или папке упорядочивают местоположение книги или документа, так и на МНИ упорядочивают файлы. Для этого ему присваивается определенное имя, которое, во-первых, позволяет отличить его от множества других файлов, и, во-вторых, дает некоторое представление о категории сведений, содержащихся в нем, или о лице, его создавшем. Однако, это не является обязательным: файлу может быть дано любое условное наименование, не связанное с его содержанием. К имени файла может быть добавлено так называемое «расширение», то есть примечание, содержащее не более трех символов. Расширение отражает специфику формата файла и особенности его использования. По расширению, как правило, можно установить название или вид программы для ЭВМ, с помощью которой файл был создан и может быть переведен в человекочитаемую форму.

При создании файла или изменении его содержания компьютерной системой либо программой для ЭВМ автоматически регистрируется дата и время, когда эти действия были совершены. Они берутся ЭВМ из внутрисистемных показаний встроенного календаря и таймера (часов) и могут быть откорректированы пользователем «вручную». Имя, тип, дата и время являются атрибутами файла, которые фиксируются в каталоге.

Каталог файлов – директорий («папка») является еще одним идентификационным реквизитом. Он содержит информацию о группе файлов, хранимых совместно на одном машинном носителе. Директорий имеет имя (название) и, в свою очередь, может быть зарегистрирован в другом директории (одна «папка» может быть вложена в другую). В этом случае он становится подчиненным или «под – директорием». Так образуется иерархическая файловая система: на каждом машинном носителе всегда имеется корневой директорий – тот, в котором начинают регистрироваться обычные файлы («главная папка») и под-директории 1-го уровня («папки», вложенные в нее); в них, в свою очередь, могут регистрироваться файлы и под-директории 2-го уровня («папки» вложенные в «папки» 1-го уровня) и т.д.

Реквизиты, идентифицирующие содержание документа на машинном носителе, определяются после его перевода в человекочитаемую форму либо из сопроводительной документации на него, представленной на обычных бумажных носителях. Эти реквизиты устанавливаются для каждого отдельного вида документа рассматриваемой категории и определяются соответствующими стандартами и иными нормативными актами. С правовой точки зрения представляется возможным выделить следующие виды таких документов.

1. Электронный документ – документ, в котором информация представлена в электронно-цифровой форме. К этой категории относятся документы, все реквизиты которых находятся в сложных форматах – в виде компьютерной информации, например: электронно-цифровое документальное сообщение, переданное по каналам электросвязи; электронная страница глобальной сети ЭВМ «Интернет»; сайт; бездокументарная ценная бумага; цифровой фотоснимок, видео- и аудиозапись; файл с данными, позволяющими их идентифицировать; электронный журнал автоматического регистрирующего устройства; электронная записная книжка сотового радиотелефона; программа для ЭВМ; база данных.

Программа для ЭВМ – это объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата, а также подготовленные и зафиксированные на физическом носителе материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения.

База данных – объективная форма представления и организации совокупности данных (например: статей, расчетов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

2. Пластиковая карта – документ, выполненный на основе металла, бумаги или полимерного (синтетического) материала – пластика стандартной прямоугольной формы, хотя бы один из реквизитов которого находится в форме, доступной восприятию средствами электронно-вычислительной техники и электросвязи. В соответствии с российским стандартом ГОСТ Р 50809 «Нумерация и метрологическое обеспечение идентификационных карт для финансовых расчетов» эти документы должны иметь следующие геометрические параметры: 85,595×53,975×0,76×3,18 мм (ширина×высота×толщина×радиус окружности в углах).

Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью (ЭЦП)9 – аналогом собственноручной подписи. Юридическая сила документа – это свойство официального документа, сообщаемое ему действующим законодательством, компетенцией издавшего его органа и установленным порядком оформления. Как правило, в качестве аналога собственноручной подписи используется электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП (ПИН-кода – В.В.) и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе. При этом, её юридическая сила признается при одновременном соблюдении следующих условий:

1. Сертификат ключа ЭЦП не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент его подписания;

2. Подтверждена подлинность ЭЦП в электронном документе;

3. ЭЦП используется в соответствии со сведениями, указанными в сертификате ее ключа.

Право удостоверять идентичность ЭЦП осуществляется на основании лицензии, порядок выдачи которой определяется Законом Российской Федерации от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи». Его действие распространяется на отношения, возникающие при совершении гражданско-правовых сделок, а также в других предусмотренных законодательством России случаях, когда ЭЦП с юридической точки зрения признается равнозначной собственноручной подписи в обычных – бумажных документах. Так, например, Гражданский кодекс разрешает применять для удостоверения прав распоряжения денежными суммами, находящимися на счете, электронные средства платежа и другие документы с использованием в них аналогов собственноручной подписи, кодов, паролей и иных средств, подтверждающих, что распоряжение дано уполномоченным на это лицом (ч. 2 ст. 160; ч. 3 ст. 434; ч. 3 ст. 847).

**Тактика осмотра документа на машинном носителе**

При раскрытии и расследовании преступлений в сфере экономики и компьютерной информации очень часто возникает необходимость проведения осмотра специфического вещественного доказательства – документа на машинном носителе. Данное следственное действие производят с участием специалиста или группы специалистов в зависимости от вида и назначения этого документа, а также формата записи компьютерной информации.

Документ на машинном носителе – это документ, созданный с использованием носителей и способов записи, обеспечивающих обработку его информации ЭВМ. С криминалистической точки зрения выделяют два вида таких документов:

1. Электронный документ – документ, в котором информация представлена в электронно-цифровой форме. К этой категории относятся документы, все реквизиты которых находятся в сложных форматах – в виде компьютерной информации (электронно-цифровое документальное сообщение, переданное по каналам электросвязи; электронная страница глобальной сети ЭВМ «Интернет»; файл с данными, позволяющими их идентифицировать; электронный журнал автоматического регистрирующего устройства; электронная записная книжка сотового радиотелефона; программа для ЭВМ; база данных и др.).

2. Пластиковая карта – документ, выполненный на основе металла, бумаги или полимерного (синтетического) материала – пластика стандартной прямоугольной формы, хотя бы один из реквизитов которого находится в форме, доступной восприятию средствами электронно-вычислительной техники и электросвязи. В соответствии с российским стандартом ГОСТ Р 50809 «Нумерация и метрологическое обеспечение идентификационных карт для финансовых расчетов» все карты должны иметь следующие геометрические параметры:85,595×53,975×0,76×3,18 мм (ширина×высота×толщина×радиус окружности в углах).

Цели осмотра – выявление и анализ внешних признаков и реквизитов документа, анализ его содержания, обнаружение возможных признаков его подделки (фальсификации).

При подготовке к проведению данного следственного действия следователю (дознавателю) необходимо ознакомиться с требованиями ГОСТ 6.10.4-84 от 01.07.87 г. «Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения». Этим нормативным актом определяются требования, предъявляемые к составу и содержанию реквизитов, придающих юридическую силу данным документам3; порядок внесения в них изменений; условия их транспортирования (передачи, пересылки и т. д.) и записи на машинный носитель информации; система приема документов по каналам электросвязи; порядок воспроизведения электронного документа на машинограмму, создания копий и дубликатов машинных документов.

С тактической точки зрения, следует разделить производство рассматриваемого следственного действия на два этапа:

1. Осмотр машинного носителя информации (подложки электронного документа);

2. Осмотр формата и содержания электронного документа или отдельных электронных реквизитов.

Осмотр машинного носителя информации (МНИ) начинается с определения его типа, вида, назначения и технических параметров, а заканчивается ознакомлением с содержанием сопроводительной документации.

В протоколе осмотра должны быть зафиксированы следующие фактические данные:

1. Тип, вид, марка, назначение, цвет, заводской или учетный номер носителя.

2. Наличие, индивидуальные признаки и техническое состояние футляра (коробки, упаковки, внешней оболочки МНИ) – тип, размеры, цвет, материал, физические повреждения, надписи, принцип функционирования, информационная емкость и другие.

3. Техническое состояние – размеры , внешний вид и материал каркаса, его целостность и индивидуальные признаки; материал основного информационно-несущего слоя и его признаки (наличие или отсутствие механических повреждений – царапин, деформаций, нарушений несущего слоя и т. д.); наличие и положение (сохранность) приспособлений от несанкционированного уничтожения (перезаписи) информации (ключей, пломб, заглушек, маркеров); наличие и техническое состояние механизмов защиты информационно-несущего материала (отверстий – «окон» для считывания и записи информации).

4. Наличие, количество, размеры, цвет, марка и техническое состояние разъемов для подключения к считывающему устройству.

5. Наличие внешней спецификации, ее цвет и размеры (заводские или пользовательские наклейки либо печатные изображения с текстом, рисунком или специальными метками).

6. Наличие и индивидуальные признаки защиты МНИ от подделки или несанкционированного копирования (голограмма, штрих-код, эмбоссинг, идент-печать, флуоресценция, перфорация, ламинат и другие).

7. Признаки материальной подделки МНИ и их защиты4.

8. Индивидуальные признаки компьютерного устройства и его программного обеспечения, используемых в процессе осмотра внутреннего состояния МНИ – их тип, вид, марка, название, серийный или регистрационный (учетный) номер, версия, год выпуска и т. п.

9. Ссылка на то, что используемые в процессе осмотра средства электронно–вычислительной техники перед началом следственного действия были тестированы специалистом в присутствии понятых на предмет отсутствия в них вредоносных программных и аппаратных средств: указываются реквизиты (паспортные данные) средств тестирования, например, название программы для ЭВМ, номер ее версии, изготовитель (автор), год выпуска, а также результат тестирования.

10. Результат проверки тестирующей программой для ЭВМ данных, записанных на осматриваемом машинном носителе.

11. Работоспособность и внутренняя спецификация – серийный номер и (или) метка тома либо код доступа к информации; общий объем носителя (для дисков – по объему записи информации, для лент и проволоки – по продолжительности записи); формат разметки; объем области носителя, свободной от записи и занятой под информацию; количество и номера сбойных зон, секторов, участков, кластеров, цилиндров; количество записанных файлов5, программ, каталогов-подкаталогов, их название, логическая структура размещения на носителе.

12. Результат поиска скрытых, закодированных или ранее стертых файлов (программ).

После выполнения вышеуказанных действий переходят ко второму этапу следственного действия - осмотру формата и содержания электронного документа или отдельных электронных реквизитов, обнаруженных на МНИ, в том числе скрытых, закодированных или стертых. Его производят по следующему алгоритму.

1. Определяют формат записи компьютерной информации на машинном носителе, стандарт (вид) кодирования данных.

2. Фиксируют название и другие реквизиты программы для ЭВМ, с помощью которой был определен формат записи данных.

3. Устанавливают атрибуты файла: вид программы для ЭВМ, с помощью которой файл был создан; название (имя и расширение), размер (объем), дату и время создания (последнего изменения или стирания), наличие специальной метки или флага (системный, архивный, скрытый, только для чтения или записи и т. д.).

4. Сравнивают установленные атрибуты с отраженными в сопроводительной документации к МНИ и других документах.

5. Определяют и подыскивают программу для ЭВМ, позволяющую осмотреть содержание файла; фиксируют ее название и другие реквизиты6.

6. Получают видеограмму документа – изображение документа на экране (мониторе, дисплее) электронного терминала. Если по различным причинам, например, в случае наличия неизвестного пароля, видеограмму документа получить не удается, в дальнейшем это следует сделать путем назначения судебной компьютерно–технической экспертизы.

7. Определяют обязательные реквизиты документа:

1) наименование физического или юридического лица – создателя документа;

2) местонахождение создателя документа, его почтовый или электронный адрес;

3) наименование документа;

4) дату изготовления документа или записи на машинный носитель;

5) размер документа (количество символов, общий объем символов в байтах (битах), количество страниц или дорожек записи информации);

6) на чье имя выдан документ или кому предназначается (реквизиты адресата – получателя);

7) код лица или СВТ, ответственного за правильность изготовления документа или его записи на МНИ (код, позывной, идентификационный номер терминала в сети ЭВМ или электросвязи – номер факса, телефона, IMEI и др.);

8) код лица, утвердившего документ (ПИН-код, номер ЭЦП или закодированный биометрический параметр – отпечаток пальца руки, рисунок радужной оболочки глаза, фоноскопический реквизит, размер ладони, фотография лица и др.).

8. Фиксируют дополнительные реквизиты документа: порядковый номер документа в пакете (системе, базе данных) документов; номер телефона, телетайпа; индивидуальный номер налогоплательщика (ИНН); гриф ограничения доступа и другие.

9. Сравнивают обнаруженные реквизиты с отраженными в сопроводительной документации к МНИ и других документах.

10. Изучают признаки оформления и содержание электронного документа: параметры страницы; стиль текста и его расположение на странице; вид, название и размер шрифта; наличие нумерации или маркеров страниц, выделений отдельных реквизитов, символов; содержание реквизитов (текста), имеющее значение для уголовного дела. При этом, следует принимать во внимание такие важные положения вышеуказанного ГОСТ 6.10.4-84, как:

1) Запись документа на машинный носитель и создание машинограммы всегда должны производиться на основе данных, зафиксированных в исходных (первичных) документах, полученных по каналам электросвязи от автоматических регистрирующих устройств или в процессе автоматизированного решения задач (п. 1.6).

2) По требованию пользователя для визуального контроля документа на машинном носителе, он должен быть преобразован в человекочитаемую форму с помощью различных технических средств отображения данных (п. 1.7).

3) Подлинники, дубликаты и копии документа на машинном носителе и машинограммы, полученные стандартными программными средствами, имеют одинаковую юридическую силу, если оформлены в соответствии с требованиями настоящего стандарта (п. 3.1).

4) Подлинником документа на машинном носителе является первая во времени запись документа на машинном носителе, содержащая указание, что этот документ является подлинником (п. 3.2).

5) Дубликаты документа на машинном носителе – это все более поздние по времени, аутентичные по содержанию записи документа на машинном носителе и содержащие указание, что эти документы являются дубликатами (п. 3.3).

6) Копиями документа на машинном носителе считаются документы, переписанные с подлинника или дубликата документа на машинном носителе на другой носитель информации, аутентичные по содержанию и содержащие указание, что эти документы являются копиями (п. 3.4).

7) В дубликатах и копиях должны быть сохранены все обязательные реквизиты, содержащиеся в подлиннике документа на машинном носителе.

11. Производят поиск следов интеллектуального подлога и материальной подделки документа и его носителя.

12. Распечатывают документ в человекочитаемой форме на бумаге и прикладывают к протоколу следственного действия.

13. В случае, если машинным носителем информации является оперативное запоминающее устройство либо нет возможности изъять МНИ с осмотренным документом, принимаются меры к копированию электронного документа на другой МНИ или получается его машинограмма7.

14. Полученные в ходе осмотра документы и предметы оформляются и изымаются соответствующим процессуальным порядком.

При осмотре документа следует иметь в виду тот факт, что в соответствии со статьей 160 Гражданского кодекса Российской Федерации допускается использование для удостоверения подлинности юридических документов факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронно-цифровой подписи (ЭЦП) либо иного аналога собственноручной подписи физического лица, например электронного факсимиле.

В частности, порядок использование ЭЦП определяется следующими нормативными документами:

1. Законом Российской Федерации от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи»;

2. Государственным стандартом ГОСТ Р 34.10-94 «Информационная технология. Криптографическая защита информации. Система электронной цифровой подписи на базе асимметричного криптографического алгоритма»;

3. Государственным стандартом ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования»;

4. Частями 3 и 4 статьи 5 Закона Российской Федерации от 20.02.95 г. № 24-ФЗ «Об информации, информатизации и защите информации».

Знание следователем основных положений вышеперечисленных документов является залогом успешного производства осмотра документа на машинном носителе. Из них наиболее важны следующие определения.

Электронная цифровая подпись – это реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Средства электронной цифровой подписи – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи в электронном документе с использованием закрытого ключа ЭЦП; подтверждение с использованием открытого ключа ЭЦП подлинности электронной цифровой подписи в электронном документе; создание закрытых и открытых ключей электронных цифровых подписей.

Сертификат средств электронной цифровой подписи – документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.

Закрытый ключ электронной цифровой подписи – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием ее средств (персональный идентификационный номер, состоящий из 4 – 8 знаков, называемый ПИН-кодом).

Открытый ключ электронной цифровой подписи – уникальная последовательность символов, соответствующая закрытому ключу ЭЦП, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств ЭЦП ее подлинности в электронном документе (группа цифр, записываемая в форме компьютерной информации на МНИ – электронный реквизит документа).

Сертификат ключа подписи – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ ЭЦП и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности ЭЦП и идентификации владельца сертификата ключа подписи.

Подтверждение подлинности электронной цифровой подписи в электронном документе – положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи ее принадлежности в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной подписью электронном документе.

Пользователь сертификата ключа подписи – физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности ЭЦП владельцу сертификата ключа подписи.

Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

1. Сертификат ключа ЭЦП не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

2. Подтверждена подлинность ЭЦП в электронном документе;

3. ЭЦП используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Осмотр документа на машинном носителе, как правило, приводит к необходимости следственной и оперативной проверки по существу данных и операций, которые отражает данный документ.