**В. В. Арефьев** Ульяновский государственный университет

**ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ, ПОЛУЧЕННОЙ ПРИ ФИКСАЦИИ ПРАВОНАРУШЕНИЙ С ИСПОЛЬЗОВАНИЕМ ТЕХНИЧЕСКИХ СРЕДСТВ**

*Аннотация*. В статье поднимаются проблемы действующего законодательства регулирующего вопросы применения технических средств для фиксации следов преступлений и правонарушений и необходимость правового регулирования обеспечения конфиденциальности такой информации. Рассматриваются правовые основы использования технических средств для фиксации такой информации в разрезе обеспечения конфиденциальности информации

*Ключевые слова:* Конфиденциальная информация, правоохранительные органы, технические средства, защита информации, разглашение информации, правила защиты информации.

**THEORETICAL JUSTIFICATION FOR ENSURING THE CONFIDENTIALITY OF INFORMATION OBTAINED WHEN FIXING OFFENSES USING TECHNICAL MEANS**

*Annotation.* The article raises the problems of the current legislation regulating the use of technical means to record traces of crimes and offenses and the need for legal regulation to ensure the confidentiality of such information. The legal basis for the use of technical means for recording such information in the context of ensuring the confidentiality of information is considered

*Keywords*: Confidential information, law enforcement agencies, technical means, information protection, disclosure of information, rules for information protection.

Понятие «конфиденциальная информация» все более и более увеличивает свое значения в современной юриспруденции. Сейчас, практически ни один нормативный акт Российской Федерации не может на 100% обойти данное понятие. Становится нормой для каждого мало-мальски серьезного договора, включение в него раздела о конфиденциальности, а в случаях отсутствия такого раздела, заключение дополнительного соглашения к уже имеющемуся договору. Повсеместно в трудовые договора включаются понятия о запрете разглашения конфиденциальной информации, а нарушение такого запрета является безусловным основанием для расторжения трудового договора. Все более и более законодатель ужесточает порядок защиты персональных данных, тайны переписки, семейной тайны, не говоря уже о такой информации как государственная или служебная тайна.

Вместе с тем, несмотря на столь широкое распространение данного словосочетания, в настоящее временя законодательство Российской Федерации, так и не содержит в себе однозначного понятия «конфиденциальная информация». Ранее, до вступления в силу Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ, конфиденциальная информация определялась как, документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации. 149 ФЗ, в свою очередь, как такового определения понятия «конфиденциальная информация» в себе не содержит. Отсутствует такое определение и в иных нормативных актах Российской Федерации. Однако, определение конфиденциальной информации, может быть сформировано, путем изучения данного федерального закона.

Так, в соответствии с частью 1 статьи 2 названного закона информация – это сведения (сообщения, данные) независимо от формы их представления. Одновременно, в части 7 той же статьи указано, что конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Из изложенных норм права, в их системной взаимосвязи, возможно определить конфиденциальную информацию как сведения, независимо от формы их предоставления, которые не могут быть переданы лицом, получившим доступ к данным сведениям, третьим лицам без согласия их обладателя.

Перечень сведений, которые относятся к конфиденциальной информации, представлен в Указе Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера». Согласно данному указу к сведениям конфиденциального характера относятся:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2. Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых в соответствии с федеральными законами от 20 апреля 1995 г. № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» и от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства», другими нормативными правовыми актами Российской Федерации принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством Российской Федерации такие сведения не отнесены к сведениям, составляющим государственную тайну.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

7. Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с Федеральным законом от 2 октября 2007 г. № 229-ФЗ «Об исполнительном производстве».

Особое внимание, следует обратить на то, что данный перечень, не является исчерпывающим, как в соответствии с законодательством, так и исходя из здравого смысла. Действующий 149-ФЗ не устанавливает требований о принятии нормативных актов Президента или правительства для отнесения информации к конфиденциальной. Более того, действующее законодательство относит право отнесения информации к конфиденциальной, к исключительной компетенции обладателя информации.

Указанное обстоятельство, имеет чрезвычайно важное значение для магистерской работы, поскольку право самостоятельного определения статуса конфиденциальной информации позволяет ее обладателю самостоятельно определять способы защиты такой информации, использования и распространения, а также предусматривать меры гражданско-правовой ответственности в случае совершения указанных действий.

В настоящее время единой классификации видов конфиденциальной информации, хотя действующими нормативными актами установлено свыше 30 ее разновидностей. Попытки классифицировать конфиденциальную информацию, осуществляют современные ученые, так например, А. И. Алексенцев, в своей работе «О классификации конфиденциальной информации по видам тайны»[[1]](#footnote-1), предлагает следующие основания разделения информации по видам тайны:

собственники информации (по отдельным видам они могут частично совпадать);

области (сферы) деятельности, в которых может быть информация, составляющая данный вид тайны;

на кого возложена защита данного вида тайны (по некоторым видам тайны здесь также возможно совпадение).

А, вот А.А.Фатьянов дает классификацию конфиденциальной информации, по трем признакам: по принадлежности, по степени конфиденциальности (степени ограничения доступа) и по содержанию.

По принадлежности владельцами защищаемой информации могут быть органы государственной власти и образуемые ими структуры (государственная тайна, служебная тайна, в определенных случаях коммерческая и банковская тайны); юридические лица (коммерческая, банковская служебная, адвокатская, врачебная, аудиторская тайны и т. п.); граждане (физические лица) - в отношении личной и семейной тайны, нотариальной, адвокатской, врачебной. Следует отметить, что использование понятий «владелец», «собственник» в отношении информации содержится в ФЗ «Об информации…», Законе РФ «О государственной тайне» и ряде других нормативных актов. Это использование, равно как и признание информации в качестве объекта вещных прав и, в том числе права собственности, установленное вышеназванными актами, вызывает большую критику среди ученых и в определенной мере противоречит Гражданскому кодексу Российской Федерации, так как согласно статье 128 Гражданского кодекса Российской Федерации, информация не относится к вещам. Эта проблема уже освещалась автором, и необходимо признать, что целесообразнее все - таки отказаться от использования вещных прав в отношении информации, а поэтому правильнее говорить об обладателе, как это указано в статье 139 Гражданского кодекса Российской Федерации, а не владельце, пользователе или собственнике информации. В дальнейшем понятия «владелец», «пользователь» или «собственник» будут применятся только в случае цитирования закона или мнения какого - либо исследователя.

По степени конфиденциальности (степени ограничения доступа) в настоящее время можно классифицировать только информацию, составляющую государственную тайну. Согласно статье 8 Закона РФ «О государственной тайне», устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «особой важности», «совершенно секретно» и “секретно». Интересно, что в США и ряде стран НАТО грифы секретности схожи с установленными отечественным законодательством – «конфиденциально (confidential)», «секретно (secret)», «совершенно секретно (top secret)». Для остальных видов тайн данное основание классификации пока не разработано, при этом согласно ст. 8 Закона РФ «О государственной тайне», использование названных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

По содержанию защищаемая информация может быть разделена на политическую, экономическую, военную, научную, технологическую, личную, коммерческую и т.п. [[2]](#footnote-2)

Необходимо обратить внимание, указанные классификации не являются исчерпывающими, да и более того, являются только доктринальными, а не нормативными. Современному российскому законодательству еще только предстоит установить классификацию конфиденциальной информации в нормативных актах.

Отсутствие законодательной классификации конфиденциальной информации, отсутствие единого порядка обращения с каждым видом конфиденциальной информации, ряд проблем действующего законодательства, выражающееся в противоречии нормативных актов, не однозначной их трактовке и как следствие неисполнению на всех уровнях.

К примеру, в силу положений статьи 2 Закона РФ «О государственной тайне», государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Алексенцев А. И., отмечает, что термин «распространение» в данном случае, является слишком неопределенным [[3]](#footnote-3).

Таким образом, в настоящее время, видами конфиденциальной информации принято считать, государственную, коммерческую, личную и семейную, служебную и профессиональную тайну, которые, так же имеют ряд разновидностей. При этом правовой режим подавляющего большинства из данных тайн, должным образом не урегулирован, а урегулированные правоотношения противоречат один другому.

В результате, образуется целый ряд нарушений конфиденциальности различного вида тайны, при деятельности правоохранительных органов. Отсутствие как в административно-процессуальном кодексе, так и в уголовно-процессуальном кодексе должного регулирования соблюдения конфиденциальности получаемой в качестве доказательств информации, ведет к частым уклонениям со стороны правоохранительных органов, от выполнения законодательства в части, касающейся различного вида тайн.

Кроме того, в открыто опубликованных законодательных и иных нормативных актах, отсутствует единый или более менее систематизированный перечень сведений, конфиденциального характера, что по сути своей, объективно создает возможности, к непреднамеренному нарушения конфиденциальности такой информации, так как сотрудники правоохранительных органов зачастую объективно могут не знать о конфиденциальности той или иной информации.

Более того, относительного столь серьезных сведений как государственная тайна, ситуация точно такая же как и в отношении иных сведений конфиденциального характера. Каждое ведомство, каждое предприятие в той или иной степени связанное с разработкой документов или изделий составляющих государственную тайну, имеет свой перечень сведений, подлежащих засекречиванию. Эти перечни в 90 % случаев имеют ограничительные пометки, а зачастую и вовсе засекречены, как следствие не публикуются открыто. Указанное обстоятельство приводит к невозможности достоверно определять наличие сведений, составляющих государственную тайну в соответствующих носителях, без нанесенного на эти носители грифа секретности, что как следствие, объективно создает угрозу разглашения таких сведений.

Это далеко не исчерпывающий перечень пробелов действующего законодательства Российской Федерации в области обеспечения конфиденциальности информации. Российскому законодательству, предстоит решить еще огромный перечень пробелов, что был урегулировать вопросы обеспечения конфиденциальности информации, в особенности, в части касающейся реализации прав сотрудников правоохранительных органов на фиксацию следов преступлений и правонарушений, содержащих конфиденциальную информацию, с использованием технических средств.

1. **Права сотрудников правоохранительных органов по фиксации правонарушений с использованием технических средств.**

Общеизвестный факт, что в настоящее время, сотрудникам правоохранительных и силовых структур, предоставлено право, на использование в своей работе достижений современной науки, а именно использование фото и видео записывающих устройств, для фиксации следов преступлений и правонарушений. В Российской Федерации приняты и действуют законодательные акты, которые содержат нормы, допускающие использование технических средств и соответствующих приемов и действий в процессе осуществления правоохранительной деятельности.

Согласно статьи 11 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции» полиция в своей деятельности обязана использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру.

На основании данного закона, а именно части 3 вышеназванной статьи, сотрудники полиции активно используют технические средства, такие как средства аудио-, фото- и видеофиксации, при фиксации доказательств и обстоятельств совершения преступлений, административных правонарушений, обстоятельств происшествий. В большинстве случаев, конечно, же это происходит в общественных местах, но может происходить и вне таких мест. В соответствии с частью 4 статьи 11 того же закона Федеральный орган исполнительной власти в сфере внутренних дел обеспечивает полиции возможность использования информационно-телекоммуникационной сети Интернет, автоматизированных информационных систем, интегрированных банков данных. Что по своему смыслу, предоставляет сотрудникам полиции хранить и передавать информацию, в том числе и конфиденциальную, с использованием информационно-телекоммуникационной сети «Интернет», не указывая при этом, на необходимость обеспечения конфиденциальности такой информации.

В силу положений части 19 статьи 13 ФЗ «О полиции», полиция, помимо прочего, имеет право производить регистрацию, фотографирование, аудио-, кино- и видеосъемку, дактилоскопирование лиц, задержанных по подозрению в совершении преступления, заключенных под стражу, обвиняемых в совершении преступления, подвергнутых административному наказанию в виде административного ареста, иных задержанных лиц, если в течение установленного срока задержания достоверно установить их личность не представилось возможным, а также других лиц в соответствии с федеральным законом. В данном случае, использование технических средств для фотографирования или видеозаписи, возможно только в отношении задержанных лиц или же лиц, личность которых установить в установленный законом срок представилось не возможным.

Частью 33 статьи 13 ФЗ «О полиции», предусмотрено право полиции использовать в своей деятельности:

информационные системы, видео- и аудиотехнику, кино- и фотоаппаратуру, а также другие технические и специальные средства, не причиняющие вреда жизни и здоровью граждан, а также окружающей среде;

вести видеобанки и видеотеки лиц, проходивших (проходящих) по делам и материалам проверок полиции;

формировать, вести и использовать банки данных оперативно-справочной, криминалистической, экспертно-криминалистической, розыскной и иной информации о лицах, предметах и фактах;

использовать банки данных других государственных органов и организаций, в том числе персональные данные граждан, если федеральным законом не установлено иное.

Данные положения установлены довольно обобщенно и представляется, что не устанавливают порядок реализации таких прав сотрудниками полиции.

Кроме того, одной из функций полиции является осуществление оперативно-розыскной деятельности, которая осуществляется на основании Федерального закона от 12 августа 1995 г. «Об оперативно-розыскной деятельности». Данный закон, является основным актом, регламентирующим применение специальных технических средств для негласного получения информации. Данным ФЗ «Об ОРД» предусмотрено право сотрудников непосредственно осуществляющих оперативно-розыскную деятельность, применять в ходе проведения оперативно-розыскных мероприятий информационные системы, видео- и аудиозапись, кино- и фотосъемку, а также другие технические и иные средства, не наносящие ущерба жизни и здоровью людей и вреда окружающей среде. Однако, данный закон, как и иные ранее рассмотренные не указывают на необходимость соблюдения какого-либо законодательства о защите информации, обеспечение ее конфиденциальности.

Статьей 6 Федерального закона «Об оперативно-розыскной деятельности» определено, что оперативные сотрудники, вправе использовать для решения задач оперативно-розыскной деятельности помощь специалистов, обладающих научными, техническими и иными специальными знаниями, а также отдельных граждан с их согласия на гласной и негласной основе. По сути своей, данное положение закона, закрепляет за оперативными сотрудниками право передавать часть полученных в результате оперативно-розыскных мероприятий сведений и данных иным лица, которые привлекаются к оказанию помощи при проведении оперативно-розыскной деятельности. Перечень случаев в которых сотрудники осуществляющие оперативно-розыскную деятельность, при которых допускает привлечение иных лиц для оказания помощи закон не устанавливает, равно как и не устанавливает случаи, при которых допускается такая передача информации. Такое законодательное регулирование, предоставляет довольно широкие полномочия сотрудникам осуществляющим оперативно-розыскную деятельность. По смыслу данного законоположения, органам осуществляющим оперативно-розыскную деятельность предоставлены неограниченные полномочия по привлечению иных лиц, к работе с результатами оперативно розыскной деятельности, при условии, оформления данной деятельности как помощь соответствующему органу, что в свою очередь создает условия к не контролируемому распространению информации, в том числе конфиденциальной. А ограничения такого распространения представляется должен устанавливать орган, непосредственно осуществляющий оперативно-розыскную деятельность.

# Федеральный закон от 4 мая 2011 года № 99-ФЗ «О лицензировании отдельных видов деятельности», к лицензируемому виду деятельности относит деятельность по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации. В развитие данного закона, Постановлением Правительства РФ от 12 апреля 2012 года № 287 утверждено Положение о лицензировании деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации. Данные нормативные акты устанавливают соответствующие требования к специальным техническим средствам, используемым для негласного получения информации. То есть, учитывая, вышеизложенные положения законодательства об оперативно-розыскной деятельности и данные нормативные акты, усматривается вывод, что в своей деятельности при получении информации, без разрешения обладателя информации, сотрудники осуществляющие оперативно-розыскную деятельность, могут использовать только специальные технические средства, лицензированные и прошедшие сертификацию в установленном законом порядке. Использование же иных средств, в том числе и личных, допускается только в случае согласия обладателя информации, на фиксацию принадлежащей ему информации, с использованием конкретного технического средства. Иное, представляется противоречащим действующему законодательству, регулирующему как оперативно-розыскную деятельность, так и вопросы обращения с информацией.

Указ Президента РФ от 01 сентября 1995 года № 891 «Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств» разграничивает полномочия Федеральной службы безопасности Российской Федерации и Министерства внутренних дел Российской Федерации по использованию технических средств, при проведении оперативно-розыскных мероприятий. Так, данным Указом, установлено, что контроль почтовых отправлений, телеграфных и иных сообщений в интересах органов, осуществляющих оперативно-розыскную деятельность, возлагается на органы федеральной службы безопасности. То есть, по смыслу данного нормативного акта, иные органы, осуществляющие оперативно-розыскную деятельность, не вправе использовать технические средства предназначенные для контроля почтовых, телеграфных и иных сообщений. Однако, данное положение Указа, не является однозначно запрещающим иным органам, осуществлять контроль таких отправлений.

Тем же Указом, определено, что оперативно-розыскные мероприятия, связанные с подключением к станционной аппаратуре операторов связи, в интересах органов, осуществляющих оперативно-розыскную деятельность, проводятся с использованием оперативно-технических средств органов федеральной службы безопасности. При отсутствии у органов федеральной службы безопасности на объектах связи необходимых оперативно-технических возможностей указанные мероприятия проводятся органами внутренних дел Российской Федерации, в том числе в интересах других органов, осуществляющих оперативно-розыскную деятельность.

Такие положения, по сути своей, предоставляют органам внутренних дел, осуществлять деятельность, которую имеет право осуществлять исключительно федеральная служба безопасности, что так же ведет к расширению возможностей, по нарушению конфиденциальности информации, в частности тайны переписки. Кроме того, указанные положения закона, не обеспечивают возможности обладателя информации, на контроль за тем, что бы принадлежащая ему конфиденциальная информация была защищена.

Статьей 34 Федерального закона от 21 июля 1995 № 103-ФЗ «О содержании под стражей подозреваемых и обвиняемых в совершении преступлений» установлено, что в целях осуществления надзора за подозреваемыми и обвиняемыми может использоваться аудио - и видеотехника. Данное законоположение устанавливает права на использование технических средств исключительно в местах содержания заключенных и обвиняемых. Кроме того, данное законоположение распространяет свое действие на фиксацию действий лиц, указанных в нем. Ограничение прав таких лиц, представляется вполне оправданным, однако, на законодательном уроне не урегулирован вопрос о порядке хранения такой информации, определения порядка допуска лиц к такой информации и правах на ее распространение.

Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 года № 174-ФЗ содержит в себе ряд положений, в которых которые прямо указывают на возможность и допустимость использования технических средств для фиксации доказательств о преступлениях, а также использования полученных с их помощью результатов в уголовном судопроизводстве (досудебном и судебном разбирательстве по уголовному делу).

Возможность использования технических средств при производстве следственных действий, а так же в рамках доследственной проверки или при производстве предварительного расследования, безусловно является необходимостью. Существенно облегчает возможности оперативного получения объективных достоверных обоснованных доказательств по делу. Уголовно-процессуальный кодекс, предусматривает необходимость указания в протоколе следственного действия, сведений об использовании технических средств, порядок и условия использования, объекты, к которым эти средства были применены, и полученные результаты. Обязательным условием (с отражением в протоколе) является предупреждение лиц, участвующих в следственном действии, о применении технических средств. Вместе с тем, следует отметить, что указание в протоколе следственного действия на технические средства использованные при его проведении, не устанавливает каких либо конкретных требований к такому техническому средству. Кроме того, отсутствует указание на необходимость обеспечения конфиденциальность информации, в случае фиксации конфиденциальной информации в рамках следственного действия, в особенности, в случае, когда обладателем информации является не подследственный и право на ограничение доступа к информации предоставлено не ему лично.

Уголовно-процессуальный кодекс Российской Федерации определяет кроме того, необходимость участи специалиста в области защиты информации, который, используя свои специальные познания, обязан оказывать помощь в обнаружении, закреплении и изъятии доказательств с помощью технических средств, однако и эта норма, не указывает на необходимость обеспечения конфиденциальности получаемой информации, равно как и не устанавливает какие либо законодательные нормы, указывающие на требования к техническим средствам, применяемым для фиксации следов преступлений. Кроме того, уголовно-процессуальный не устанавливает конкретных требований к лицу, привлекаемому в качестве специалиста, что наделяет лицо, осуществляющего следствие или доследственную проверку неограниченным правом самостоятельно определять лиц, привлекаемых в качестве специалистов, что само по себе, ведет к возможному нарушению конфиденциальности получаемой информации. Кроме того, следует отметить, что уголовно-процессуальный закон, не содержит в себе указания на необходимость получения обязательства от специалиста, о неразглашении полученной информации, что существенно затрудняет возможность привлечения такого лица к установленной законом ответственности в случае разглашения им информации, полученной в ходе следственного действия.

Статьи 25.8 и 25.9 Кодекса об административных правонарушениях Российской Федерации, установлена возможность участия в производстве по делу об административном правонарушении, так же как и в уголовном судопроизводстве, специалиста и эксперта, обладающих необходимыми познаниями в технике и применении технических средств, однако, как и в уголовном судопроизводстве, указаний о требованиях к данному лицу, с учетом наличия в материалах дела конфиденциальной информации не установлено, что объективно создает угрозу разглашения конфиденциальной информации при ее наличии.

Статьей 26.2 Кодекса об административных правонарушениях Российской Федерации, определено, что к доказательством по делу об административном правонарушении могут быть в том числе, показания специальных технических средств, а статья 26.7 того же кодекса, относит к документам, признанным в качестве доказательств, по делу материалы фото- и киносъемки, звуко- и видеозаписи, информационных баз и банков данных и иные носители информации, но и в этих статьях нет какого либо указания, на требования предъявляемые к техническим средствам с помощью которых зафиксированы доказательства. Права сотрудников правоохранительных органов в такой ситуации, представляются неограниченными, так как прямого указания в законе на какие либо ограничения не установлено, то есть фактически сотрудник, осуществляющий правоохранительную деятельность, не ограничен в своих возможностях по фиксации следов или фактов правонарушений с помощью технических средств. На практике это приводит к использованию личных технических средств в целях фиксации следов правонарушений, не взирая на то, что таким образом может быть зафиксирована и в последствии разглашена, пусть даже и непреднамеренно конфиденциальная информация.

Использование технических средств для фиксации следов преступлений и правонарушений, безусловно представляет собой процесс поиска, сбора, хранения, обработки, предоставления информации, то есть является информационной технологией. Правоотношения, возникающие при применении информационных технологий, регулируются Федеральным законом от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Как следствие, все вышеописанные права сотрудников правоохранительных органов, должны быть использованы ими, с учетом требований 149-ФЗ. Как следствие представляется, что к этому же должны принципу должны быть приведены ведомственные нормативные акты правоохранительных органов, а так же правоприменительная практика.

К сожалению, в открытом доступе нет информации, которая прямо указывала бы на наличие ведомственных правовых актов правоохранительных органов, в котором имелось бы указание на реализацию полномочий правоохранительных органов, с учетом требований обеспечения конфиденциальности информации. Представляется, что такие нормативные акты ведомств, сами по себе содержат конфиденциальную информацию и не публикуются открыто, хотя и затрагивают интересы неопределенного круга граждан.

Современная судебная практика, по данному направлению, чрезвычайно скудна. Ввиду отсутствия должного правового регулирования, правоприменители скорее всего не задумываются на вопросами обеспечения конфиденциальности информации при реализации прав сотрудниками правоохранительных органов, на фиксацию следов преступлений и правонарушений. Долгое время, в вопросах требований предъявляемых к технических средствам, использующихся для фиксации правонарушений, суды были полностью на стороне правоохранителей. Так, например, Верховный Суд РФ в своем решение от 18 сентября 2013 г. № АКПИ13-679[[4]](#footnote-4) указывает, что по смыслу закона, для фиксации правонарушения могут быть использованы любые технические средства фото- видео записи, при этом, это не обязательно должны быть технические средства принадлежащие МВД РФ. Выдержка из решения: «….из приведенных законоположений видно, что возможность использования специальных технических средств, включая работающие в автоматическом режиме и имеющие функции фото- и киносъемки, звуко- и видеозаписи, не связывается с их нахождением на балансе соответствующих органов. Федеральным законодателем лишь установлено, что измерительные приборы, которые используются в качестве специальных технических средств, должны быть утверждены в установленном порядке в качестве средств измерения, иметь соответствующие сертификаты и пройти метрологическую поверку….».

То есть, по сути своей таким решением суд фактически указывает, что для фиксации правонарушений и преступлений могут быть использованы любые технические средства, без указания на то, каким образом должна быть обеспечена конфиденциальность информации. Особенно в тех условия когда фиксация производилась с использованием технических средств постороннего человека, который и к правоохранительным органам то не имеет отношения.

Однако, в настоящее время, судебная практика несколько изменилась благодаря Конституционному суду Российской Федерации. И все произошло благодаря тому, что сотрудники правоохранительных органов, сами не забывают о необходимости соблюдения конфиденциальности информации полученной ими при осуществлении следственных действий и активно требуют соблюдения конфиденциальности от адвокатов. Так, сотрудниками правоохранительных органов, были ограничены права адвоката, на производство копий материалов уголовного дела с использованием личного смартфона, запрещен его пронос в задние Министерства внутренних дел. Адвокат не согласился с таким положением дел и обжаловал решения должностных лиц Министерства внутренних дел в суд. Дело дошло до Конституционного суда Российской Федерации, который, в своем постановлении № 21П от 26 мая 2022 года «По делу о проверке конституционности пункта 25 части 1 статьи 13 Федерального закона «О полиции» в связи с жалобой гражданина И.Н.Фролова» [[5]](#footnote-5) указал:

«…Признать пункт 25 части 1 статьи 13 Федерального закона «О полиции» не противоречащим Конституции Российской Федерации, поскольку по своему конституционно-правовому смыслу в системе действующего правового регулирования он не может служить основанием для запрета должностными лицами полиции прохода адвокатов в связи с оказанием в установленном федеральным законом порядке юридической помощи в уголовном судопроизводстве в административные здания органов внутренних дел с мобильным телефоном, имеющим функции аудио- и видеофиксации, а также выхода в информационно-телекоммуникационную сеть «Интернет», что не препятствует должностным лицам, осуществляющим уголовное преследование, в соответствии с уголовно-процессуальным законодательством определять возможность использования соответствующих функций телефона при производстве предварительного расследования…». То есть, Конституционный суд Российской Федерации фактически признает право обладателя информации, в уголовном процессе, определять правила обращения с принадлежащей ему информацией, а именно при наличии в материалах уголовного дела конфиденциальной информации, лицо осуществляющее уголовное преследование вправе ограничить право адвоката на фиксацию такой информации с использованием личного технического средства. И это при том, что право на копирование документов, содержащихся в уголовном деле, в том числе с использованием личного мобильного телефона, это право которое предоставлено адвокату федеральным законом. В общем и целом, представляется, что Конституционный суд Российской Федерации фактически признал чрезвычайную важность обеспечения конфиденциальности информации, в том числе в уголовном и административном судопроизводстве.

С учетом такого мнения Конституционного суда Российской Федерации, представляется, что подобная позиция должна распространяться и на сотрудников правоохранительных органов, как в уголовном и административном процессах, так и в рамках осуществления оперативно-розыскной деятельности. Вместе с тем, в настоящее время на законодательном уровне отсутствуют указания на порядок установления конфиденциальности и порядок требования обеспечения конфиденциальности таких сведений как например персональные данные человека. Вследствие чего, возникает правовая неопределенность, с возможностью использования сотрудниками правоохранительных органов личных технических средств для фиксации следов преступления и правонарушений, а так же в рамках оперативно-розыскной деятельности. Однако, в таком регулировании так же есть сложности, ввиду отсутствия возможностей однозначного определения на законодательном уровне порядка отнесения информации к конфиденциальной. Очевидные трудности возникают и в реализации критериев, по котором информация должна отнестись к конфиденциальной, но самое проблематичное, это информирование о наличии конфиденциальной информации сотрудников правоохранительных структур.

Действующее законодательное регулирование, по формальным признакам, не ограничивает сотрудников правоохранительных органов в использовании конкретных технических средств для фиксации правонарушений, не устанавливает требования к носителям информации которые в них применяются. Указанное положение дел, в свою очередь приводит к многочисленным случаям нарушения конфиденциальности информации, созданию угрозы разглашения конфиденциальной информации, а зачастую и прямому разглашения сведений конфиденциального характера, сотрудниками правоохранительных органов, как реализующих свои полномочия в рамках административного и уголовного процессов, так и в рамках осуществления оперативно-розыскной деятельности.

**СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ**

**Нормативно-правовые акты Российской Федерации**

1. Федеральный закон от 26.07.2017 года и № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>, 26.07.2017.
2. Федеральный закон от 27.07.2006 года № 152-ФЗ «О персональных данных» (в ред. от 02.07.2021) //Российская газета от 29 июля 2006 г. - № 165, Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>, 02.07.2021.
3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (в ред. от 02.07.2021) // Российская газета от 29 июля 2006 г. - № 165, Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>, 02.07.2021.
4. Федеральный закон от 29.07.2004 года № 98-ФЗ «О коммерческой тайне» (в ред. от 09.03.2021) // Собрание законодательства Российской Федерации от 9 августа 2004 г. - № 32 - ст. 3283, Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>, 09.03.2021.
5. Закон РФ от 21 июля 1993 года № 5485-1 «О государственной тайне» (в ред. от 11.06.2021) // Российская газета от 21 сентября 1993 г. - № 182, Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>, 11.06.2021.
6. Указ Президента Российской Федерации от 2 июля 2021 года № 400 «Об утверждении стратегии национальной безопасности» // Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>, 03.07.2021.
7. Указ Президента РФ от 22.12.2017 года № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>, 22.12.2017.
8. Указ Президента Российской Федерации от 9 мая 2017 года № 203 «Об утверждении Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>, 10.05.2017.
9. Указ Президента Российской Федерации  
   от 5 декабря 2016 г № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации <http://www.pravo.gov.ru> 06.12.2016.
10. Постановление Правительства Российской Федерации от 3 ноября 1994 года № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» (в ред. от 19.08.2020) // Собрание законодательства Российской Федерации от 25 июля 2005 г. - № 30 - ст. 3165, официальный интернет-портал правовой информации <http://www.pravo.gov.ru>, 11.08.2020.

**Проекты, концепции и другие документы программного**

**характера**

1. Национальный стандарт РФ ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» (утв. [приказом](garantF1://6628050.0) Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 532-ст) / Стандартинформ, Москва, 2009 г. // СПС Гарант.
2. Национальный стандарт РФ ГОСТ Р 53110-2008  
   «Система обеспечения информационной безопасности сети связи общего пользования. Общие положения» (утв. [приказом](garantF1://6632082.0) Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 528-ст) Стандартинформ, Москва, 2009 г. // СПС Гарант.

**Книги (учебники, учебные пособия, монографии, сборники)**

1. Гафнер, В. В. Информационная безопасность: Учебное пособие / В. В. Гафнер. - Москва: Феникс, 2010. - 324 c.
2. Гришина, Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - Москва: Форум, 2017. - 159 c.
3. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие для вузов. / А.А. Малюк. - Москва: Горячая линия - Телеком, 2004. - 280 c.
4. Семененко, В.А. Информационная безопасность / В.А. Семененко. - Москва: МГИУ, 2011. - 277 c.
5. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. – Москва: Академический проспект, 2008. - 544 c.

**Ресурсы информационно – телекоммуникационной сети Интернет**

1. Справочник законодательства РФ в области информационной безопасности (версия от 10.11.2021) – текст электронный // [сайт] 2023 - URL <https://habr.com/ru/post/432466> (дата обращения 04.02.2023).
2. Информационный портал Совета безопасности Российской Федерации – текст электронный // [сайт] 2021 - URL <http://www.scrf.gov.ru/security/docs/> (дата обращения 03.02.2023).
3. Публикация «На каких серверах держится Рунет Деловая газета «Взгляд» 12 февраля 2020» – текст электронный // [сайт] 2023 - URL <https://news.rambler.ru/other/43670761-na-kakih-serverah-derzhitsya-runet/> (дата обращения 02.02.2023).

**REFERENSES**

**Regulatory legal acts of the Russian Federation**

1. Federal Law of 26.07.2017 and No. 187-FZ "On the security of the critical information infrastructure of the Russian Federation" // Official Internet Portal of Legal Information http://www.pravo.gov.ru , 26.07.2017.

2. Federal Law No. 152-FZ of 27.07.2006 "On Personal Data" (as amended. from 02.07.2021) //Rossiyskaya Gazeta of July 29, 2006 - No. 165, Official Internet portal of legal Information http://www.pravo.gov.ru , 02.07.2021.

3. Federal Law "On Information, Information Technologies and Information Protection" dated 27.07.2006 No. 149-FZ (as amended. dated 02.07.2021) // Rossiyskaya Gazeta dated July 29, 2006 - No. 165, Official Internet portal of Legal Information http://www.pravo.gov.ru , 02.07.2021.

4. Federal Law No. 98-FZ of 29.07.2004 "On Commercial Secrets" (as amended. dated 09.03.2021) // Collection of Legislation of the Russian Federation dated August 9, 2004 - No. 32 - Article 3283, Official Internet portal of legal information http://www.pravo.gov.ru , 09.03.2021.

5. The Law of the Russian Federation of July 21, 1993 No. 5485-1 "On State secrets" (ed. dated 11.06.2021) // Rossiyskaya Gazeta dated September 21, 1993 - No. 182, Official Internet portal of Legal Information http://www.pravo.gov.ru , 11.06.2021.

6. Decree of the President of the Russian Federation No. 400 dated July 2, 2021 "On approval of the National Security Strategy" // Official Internet Portal of Legal Information http://www.pravo.gov.ru , 03.07.2021.

7. Decree of the President of the Russian Federation No. 620 dated 22.12.2017 "On improving the state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation" // Official Internet Portal of Legal Information http://www.pravo.gov.ru , 22.12.2017.

8. Decree of the President of the Russian Federation No. 203 of May 9, 2017 "On approval of the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030" // Official Internet Portal of Legal Information http://www.pravo.gov.ru , 10.05.2017.

9. Decree of the President of the Russian Federation No. 646 of December 5, 2016 "On the approval of the Information Security Doctrine of the Russian Federation" // Official Internet Portal of Legal Information http://www.pravo.gov.ru 06.12.2016.

10. The Decree of the Government of the Russian Federation dated November 3, 1994 No. 1233 "On Approval of the Regulations on the Procedure for Handling Official Information of Limited Distribution in Federal Executive Authorities, the Authorized Body for Managing the Use of Atomic Energy and the Authorized Body for Space Activities" (as amended. dated 19.08.2020) // Collection of Legislation of the Russian Federation dated July 25, 2005 - No. 30 - Article 3165, official Internet portal of legal information http://www.pravo.gov.ru , 11.08.2020.

**Projects, concepts and other documents of a programmatic nature**

11. The national standard of the Russian Federation GOST R 53114-2008 "Information protection. Ensuring information security in the organization. Basic Terms and Definitions" (approved by Order No. 532-st of the Federal Agency for Technical Regulation and Metrology dated December 18, 2008) / Standartinform, Moscow, 2009 // SPS Garant.

12. National standard of the Russian Federation GOST R 53110-2008 "The information security system of the public communication network. General Provisions" (approved by Order No. 528-st of the Federal Agency for Technical Regulation and Metrology dated December 18, 2008) Standartinform, Moscow, 2009 // SPS Garant.

**Books (textbooks, manuals, monographs, collections)**

13. Gafner, V. V. Information security: A textbook / V. V. Gafner. - Moscow: Phoenix, 2010. - 324 p.

14. Grishina, N.V. Information security of the enterprise: A textbook / N.V. Grishina. - Moscow: Forum, 2017. - 159 p.

15. Malyuk, A.A. Information security: conceptual and methodological foundations of information protection: A textbook for universities. / A.A. Malyuk. - Moscow: Hotline - Telecom, 2004. - 280 p.

16. Semenenko, V.A. Information security / V.A. Semenenko. - Moscow: MGIU, 2011. - 277 p.

17. Yarochkin, V.I. Information security: Textbook for universities / V.I. Yarochkin. – Moscow: Akademicheskiy prospekt, 2008. - 544 p.

**Internet information and telecommunication network resources**

18. Handbook of the legislation of the Russian Federation in the field of information security (version from 10.11.2021) – electronic text // [website] 2023 - URL https://habr.com/ru/post/432466 (accessed 04.02.2023).

19. Information portal of the Security Council of the Russian Federation – electronic text // [website] 2021 - URL http://www.scrf.gov.ru/security/docs / (accessed 03.02.2023).

20. Publication "On which servers the Runet Business newspaper "Vzglyad" is kept on February 12, 2020" – electronic text // [website] 2023 - URL https://news.rambler.ru/other/43670761-na-kakih-serverah-derzhitsya-runet / (accessed 02.02.2023).

**ИНФОРМАЦИЯ ОБ АВТОРАХ**

*Арефьев Владимир Викторович —* Ульяновский государственный университет, 432071, г. Ульяновск, ул. Гончарова 40/9, Российская Федерация, e-mail: shiphr008@gmail.com.

**AUTHORS**

*Arefyev Vladimir Viktorovich —* Ulyanovsk State University, 40/9 Goncharova str., Ulyanovsk, 432071, Russian Federation, e-mail: shiphr008@gmail.com .

1. Алексенцев А.И. О классификации конфиденциальной информации по видам тайны // Безопасность информационных технологий. 1999. № 3. С. 65. [↑](#footnote-ref-1)
2. Фатьянов А.А. Концептуальные основы обеспечения безопасности на современном этапе // Безопасность информационных технологий. 1999. № 1. С. 27. [↑](#footnote-ref-2)
3. Алексенцев А.И. О классификации конфиденциальной информации по видам тайны // Безопасность информационных технологий. 1999. № 3. С. 96. [↑](#footnote-ref-3)
4. Решение Верховного Суда РФ от 18 сентября 2013 г. N АКПИ13-679// СПС «Гарант», 2013. [↑](#footnote-ref-4)
5. Постановление Конституционного суда по делу «О проверке конституционности пункта 25 части 1 статьи 13 Федерального закона «О полиции» в связи с жалобой гражданина И.Н.Фролова» № 21П от 26 мая 2022 года // СПС «Гарант», 2022. [↑](#footnote-ref-5)