Уголовно-процессуальная деятельность начальника подразделения дознания в виде процессуального руководства деятельностью подчиненных ему дознавателей является одной из гарантий законности в деятельности дознавателей как должностных лиц государства и участников уголовного судопроизводства.

С.А. Сумин*

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ УЧАСТНИКОВ УГОЛОВНОГО СУДОПРОИЗВОДСТВА С ИСПОЛЬЗОВАНИЕМ ИННОВАЦИОННЫХ ТЕХНИЧЕСКИХ СРЕДСТВ ФИКСАЦИИ И ЗАЩИТЫ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ

Ключевые слова: *технические средства, правоохранительные органы, уголовное судопроизводство, биометрическая идентификация, GPS-позиционирование, Электронно-цифровая подпись (ЭЦП).*

S.A. Sumin. Assuring of Security for Participants of Criminal Process Applying Innovative Technical Means for Fixation and Further Defence of Proving Information

In the present article it tells upon the problem of assuring of proper implementation legal base during investigation process, using different innovative technical means. The innovative development in judicature and police forces in all levels and dimensions has been considerably fastening in recent time. The legislature can scarcely follow in this direction with the same capacity of adaptation. That is why, using innovative technology is relatively hindered in helping fight criminalty. Inapting, controversial diversity and even lack of legal base in this field of criminal justice lead to far-going legal and processional problems, mostly influencing the quality of inquiry measures, processional trial measures, and finally damaging human and civil rights of citizens.

One of essential hindernis for using of results of implementation of technical innovations in criminal justice is controversy of form and meaning of existing legal base for proving, as in regard to Criminal Process Law of the Russian Federation.

На протяжении всего XX в. применение технических средств в сфере уголовного судопроизводства происходило нарастающими темпами. В последние годы внедрение значительного количества технических средств самого разного назначения в обыденную практику правоохранительных органов ускорилось настолько, что действующее законодательство не успевает

* Старший следователь по особо важным делам организационно-зонального отдела Главного следственного управления, майор юстиции. [shtorm69@yandex.ru]

адаптироваться к постоянно меняющимся условиям, что затрудняет использование инновационных разработок в борьбе с преступностью. Недостаточность, двойственность, а иногда и отсутствие правовой базы использования технических средств в сфере уголовного судопроизводства приводят к возникновению правовых и процессуальных проблем, наличие которых существенно влияет на качество производства следственных действий, рассмотрение уголовных дел в суде, а также приводит к нарушению прав и свобод граждан.

В связи с этим на практике возникают вопросы относительно того, как должно регламентироваться законом применение в уголовном процессе новых технических средств, появляющихся в результате развития науки и техники, а также возможно ли в законе дать их исчерпывающий перечень?

В современной литературе преобладает такая точка зрения: право не должно регулировать применение каждого технического средства. В законе устанавливаются общие принципы, которым должны отвечать используемые на практике технические средства. Разделяя данную позицию, отметим, что УПК РФ содержит перечень основных групп технических средств, применяемых в уголовном процессе. Здесь необходимо согласиться с мнением А.В. Ткачева, который считает, что в отношении компьютерных средств надо дополнительно учитывать коренные изменения, которые они вызвали в технологии обработки информации [1]. Поэтому необходимо сформулировать основные условия, при соблюдении которых возможно использование инновационных технических средств.

Несмотря на то, что в федеральном законодательстве содержится значительное количество правовых норм, призванных обеспечить гарантии прав и свобод граждан от необоснованного их ограничения при осуществлении государственными органами правоохранительной деятельности, некоторые из ныне действующих нормативных правовых актов не только не учитывают современный уровень развития технических средств, но и не соответствуют положениям Конституции РФ, выступающей гарантом прав и свобод человека и гражданина.

Существующие проблемы обеспечения законности при раскрытии и расследовании преступлений с использованием технических средств, предназначенных для негласного получения информации являются наиболее актуальными. Это обусловлено тем, что указанные технические средства на законных основаниях используются для раскрытия и расследования преступлений исключительно органами, уполномоченными законом на ведение

[1] См.: *Ткачев А.* Правовые и криминалистические аспекты использования компьютерной техники при расследовании серийных убийств // Следственная практика. Вып. 4 (161). М., 2003. С. 235—243.

оперативно-розыскной деятельности, в ходе которой, возможно, ограничены права и свободы граждан, закрепленные в ст. 23, 24 и 25 Конституции РФ. Поэтому на законодателей, разрабатывающих нормативно-правовое обеспечение деятельности правоохранительных органов, возлагается обязанность создания условий, не допускающих деформации границы, отделяющей необходимые для общества ограничения прав и свобод отдельных граждан от их ущемления и нарушения. Также применение технических средств в оперативно-розыскной деятельности является неотъемлемой частью процесса раскрытия и расследования преступлений и, соответственно, допустимо только при осуществлении его в строгом соответствии с законом.

Рассмотрим допустимость применения технологий биометрической идентификации, GPS-позиционирования и ЭЦП в уголовном судопроизводстве.

Несмотря на столь явные преимущества использования биометрических паспортов и методов биометрической идентификации, уже сейчас можно услышать протесты против подобных нововведений. Активнее всех протестуют против введения биометрических технологий защитники прав человека, так как использование биометрии означает создание баз данных не только с информацией о биопараметрах всех граждан страны, но и практическую возможность неограниченного отслеживания перемещений отдельно взятого лица, которое фактически означает установление системы тотального контроля. Данная система ограничивает основные права человека — на конфиденциальность, свободу перемещения, тайну личной жизни. Кроме того, возникает и ряд других проблем, среди которых главной является обеспечение сохранности конфиденциальности информации о персональных и биометрических данных граждан, содержащейся в таких базах данных, гарантированное исключение ее несанкционированного использования [1].

[1] В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» все информационные системы, содержащие персональные данные, должны быть приведены в соответствие с требованиями настоящего Федерального закона не позднее 1 января 2010 г. Одним из основных положений данного закона является требование принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства для защиты персональных данных. При проведении мероприятий по обеспечению безопасности информационных систем персональных данных необходимо опираться на постановление Правительства РФ от 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации», а так же на следующие руководящие документы Федеральной службы по техническому и экспортному контролю (ФСТЭК России): Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные заместителем директора ФСТЭК России 15 февраля 2008 г.; Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 14 февраля 2008 г.; Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, утвержденные за-

Следует отметить, что указанные системы государственной регистрации граждан создаются с ориентацией не только и не столько для борьбы с преступностью, сколько для решения множества иных социальных проблем (здравоохранения, образования, пенсионного обеспечения, страхования, обороны и т.п.). Не случайно в США, отмечает В. Шмаков, такая система называется «Social Security» — социальной защиты. Хотя, по оценкам самих американцев, отмечает указанный автор, «ни в одном самом тоталитарном государстве нет такой системы контроля за деятельностью и перемещением населения, как в США, но они к ней привыкли и считают безусловно нужной»[2]. Мы согласны с мнением М.М. Эндреева, который считает, что это один из наглядных примеров адекватного восприятия обществом угроз преступности и мер по борьбе с ней, а вместе с тем доверия, но не к власти, а к определенным законом формам контроля за ее деятельностью, исключающим злоупотребление властью [2].

В этой связи нам хотелось бы обратить внимание на то, что аналогичные проблемы «тоталитарного контроля» поднимались правозащитниками при повсеместном внедрении национальными банками зарплатных пластиковых карт. Вместе с тем достаточно длительный интервал времени использования населением такого «электронного» платежного средства показал, что нарушения в этой сфере несомненно имеются, однако практичность и удобство пластиковых карт, по сравнению с наличными деньгами, одержали верх в спорах с правозащитниками.

Несмотря на протесты защитников прав человека свыше 100 стран, большинство из которых являются демократическими, вводят биометрические паспорта или «ID cards» (биометрические документы) в разных вариантах. В перспективе наличие компьютерного чипа в единственном биометрическом документе дает возможность использовать «ID cards» как паспорт, удостоверение водителя, платежное средство, карту системы национального здравоохранения и др.[3]. Информация, содержащаяся в таком доку-

---

местителем директора ФСТЭК России 15 февраля 2008 г.; Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 15 февраля 2008 г.; Специальные требования и рекомендации по технической защите конфиденциальной информации, утвержденные приказом Гостехкомиссии России от 30 августа 2002 г. № 282 и др. (см. подробнее: Автоматизированная система органов предварительного следствия как информационная система обработки персональных данных // Информационный бюллетень Следственного комитета при МВД России. 2009. № 4 (142). С. 132—138 (для служебного пользования)).

[1] *Шмаков В.* Беседы о криминалистике. Челябинск, 1997. С. 44.

[2] См.: *Эндреев М.М.* Значение информационно-поисковых систем в раскрытии и расследовании преступлений // Проблемы нераскрытых преступлений прошлых лет: сб. матер. межвуз. науч. семинара. М., 2008. С. 293—297.

[3] См.: *Билоус Е.Н., Захаров В.П., Харченко С.В.* Использование возможностей биометрии человека в установлении личности // Проблемы нераскрытых преступлений прошлых лет: сб. матер. межвуз. науч. семинара. М., 2008. С. 257—261.

менте, может стать эквивалентом портативного персонального файла владельца [1]. Рассмотренные нами удостоверения личности, (которые, как было показано нами выше, целесообразно снабдить еще и технологией ЭЦП) превращают их в надежный «ключ» для входа в информационную базу данных для идентификации и последующей проверки владельцев удостоверений на благонадежность с точки зрения властных структур.

Данное высказывание не является футуристическим, поскольку методы биометрической идентификации в настоящее время уже широко применяются в практической деятельности правоохранительных органов. Так в целях проведения идентификации личности в настоящее время в системе МВД РФ широко применяются возможности дактилоскопической системы «Папилон»[2], подключенной к ведомственной базе данных, с помощью которой можно установить личность лица, а также проверить его на причастность к совершению других преступлений [3]. Помимо названной идентификационной системы, с 90-х гг. прошлого века началась мировая практика внедрения автоматизированных систем идентификации по внешнему облику, например, программного обеспечения «Face-it Argus» США. На территории СНГ также разрабатываются и внедряются такие системы, как: «Портрет 2005» (портрет-поиск), «FACE MANAGER», «ОБЛИК», «ЕЛЛИ 6.0», «КРИМНЕТ», АПК «СОВА» и др. В настоящее время в подразделениях ОВД РФ успешно функционирует свыше 341 аппаратно-программных комплекса «Сова»[4].

Все изложенное однозначно свидетельствует о необходимости и допустимости повсеместного криминалистического использования биометричес-

---

[1] Например, в Швеции при регистрации новорожденного ребенка в магистратуре ему присваивается цифровой код, в котором зашифрованы его установочные данные. В дальнейшем на основе такого кода формируется своеобразное «биографическое досье» с указанием важнейших в жизни человека событий и явлений, в частности касающихся учебы, профессии, трудовой деятельности, службы в армии, состояния здоровья, серьезных конфликтов с законом и т.д. (см. подробнее: *Беляков А.А., Усманов Р.А.* Состояние, проблемы и перспективы развития криминалистической регистрации в России. Красноярск, 2001).

[2] «Папилон» — автоматизированная дактилоскопическая информационная система (АДИС) в России построена на базе унифицированного программного обеспечения и представляет собой структуру трех уровней: регионального, межрегионального и федерального. В течение 2007 г. в ГИАЦ МВД России с помощью АДИС произведено 28000 отожествлений, по объектам учета, в том числе опознано 2000 трупов, региональными ИЦ отожествлено 270 тыс. объектов учета, опознано 14000 трупов (см. подробнее: Информационное письмо ГИАЦ МВД России в ГОУ ВПО БЮИ МВД России №34/2-153 от 25 апреля 2008 г.).

[3] См.: *Смагин П.Г.* Проблемы допустимости доказательств в условиях электронного документооборота при расследовании преступлений в ОВД // Международная научно-практическая конференция «Обеспечение законности и правопорядка в странах СНГ»: сб. мат. Ч. 1. Воронеж, 2009. С. 252—255.

[4] См.: *Иванов И.И.* Противодействие коррупции средствами уголовного судопроизводства: иллюзии и реальность // Проблемы нераскрытых преступлений прошлых лет: сб. матер. межвуз. науч. семинара. М., 2008. С. 215; Информационное письмо ГИАЦ МВД России в ГОУ ВПО БЮИ МВД России №34/2-153 от 25 апреля 2008 г.

ких удостоверений личности, а также баз данных, в том числе содержащих биометрические сведения.

Переходя к рассмотрению допустимости применения в процессуальной деятельности GPS-позиционирования следует отметить, что в России в настоящее время нет закона об использовании средств системы глобальной спутниковой навигации, в том числе при выполнении процессуальных действий, однако есть ряд законов и нормативных актов, регулирующих смежные вопросы. Так, в соответствии со ст. 2 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»[1] к радиоэлектронным относятся технические средства, предназначенные для передачи и (или) приема радиоволн, состоящие из одного или нескольких передающих и (или) приемных устройств либо комбинации таких устройств и включающие в себя вспомогательное оборудование. В примечании к п. 1 Положения об изготовлении, ввозе и использовании радиоэлектронных средств на территории РФ, приводится открытый перечень указанных выше средств [2]. В п. 3 этого же нормативного акта ведется речь о необходимости получения соответствующего разрешения, однако специальной системы выдачи на приемники радионавигационных сигналов (ПРС) в нем не предусмотрено, поскольку в соответствии с п. 2 рассматриваемого Положения действие данной нормы не распространяется на радиоэлектронные средства, предназначенные для индивидуального приема программ теле— и радиовещания, изделия бытовой электроники, не содержащие радиоизлучающих устройств, к которым, несомненно, следует отнести и ПРС [3], в обиходе именуемых навигаторами.

Вместе с тем деятельность современных навигаторов неразрывно связана с использованием ими данных геодезии и картографии для наглядности отображаемой информации о месте нахождения приемника, что является значимым элементом системы позиционирования. Однако геодезическая и картографическая деятельность (в том числе и системы электронной картографии) подлежат лицензированию на основании ст. 12 Федерального закона от 26 декабря 1995 г. № 209-ФЗ «О геодезии и картографии»[4] и в соответствии со ст. 17 Федерального закона от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности»[5]. При этом под геодезичес-

---

[1] Росс. газ. 2003. 10 июля.

[2] Постановление Правительства РФ от 5 июня 1994 г. № 643 «О порядке изготовления, приобретения, ввоза в Российскую Федерацию и использования на территории Российской Федерации радиоэлектронных средств (высокочастотных устройств)» // Собрание законодательства РФ. 1994. № 8. Ст. 861.

[3] См.: *Пропастин С., Шепель В.* Использование современных технологий позиционирования при производстве отдельных следственных действий // Уголовное право. 2009. № 1. С. 105—108.

[4] Росс. газ. 1996. 13 янв.

[5] Росс. газ. 2001. 10 авг.

кой и картографической деятельностью в соответствии со ст. 1 Закона «О геодезии и картографии» понимается «научная, техническая, производственная и управленческая деятельность в области геодезии и картографии». Следовательно использование навигаторов, затрагивая область геодезии и картографии, не включается в таковую, а стало быть не требует лицензирования, т.е. использование приемника сигналов любым потребителем (в том числе следователем) не требует получения лицензии либо специального разрешения [1].

По указанной причине данные навигационной системы, по нашему мнению, при необходимости их учитывания при проведении процессуального действия, могут быть легально использованы в качестве вспомогательного средства фиксации, тем более, что визуальные показания ПРС основаны на лицензированных данных электронной картографии системы ГЛОНАСС, предоставляемой российским потребителям на безвозмездной основе и без ограничений.

В основе действия навигатора лежит использование цифровых технологий, а сам приемник может быть отнесен к носителям компьютерной информации, особенно если его использование подразумевается в сочетании со смартфоном или персональным компьютером (ноутбуком). Здесь особо хотелось бы отметить, что информация приемников радионавигационных сигналов уже достаточно широко распространена в правоохранительной деятельности [2] и применяется судами в качестве доказательств по уголовным делам [3].

Переходя к допустимости использования криптографических алгоритмов в правоохранительной деятельности, хотелось бы отметить, что сам факт наличия в разных странах законов об ЭЦП, говорит сам за себя. На национальном уровне криптографические способы защиты информа-

---

[1] Здесь потребитель — лицо, использующее товары (услуги) исключительно для личных или иных нужд (как синоним — бытовых нужд), не связанных с осуществлением предпринимательской деятельности (в том числе выполнения должностных обязанностей в рамках уголовного судопроизводства) (цит. по: *Пропастин С., Шепель В.* Использование современных технологий позиционирования при производстве отдельных следственных действий // Уголовное право. 2009. № 1. С. 105—108).

[2] См.: *Куликов В.* Конвой на дому // Росс. газ. 2009. 2 апр. В статье рассказывается об использовании в системе ФСИН РФ спутниковых систем позиционирования при их применении в качестве устройств слежения за осуждёнными за незначительные преступления.

[3] См.: *Борисов Т.* Контрольный выстрел в голову // Росс. газ. 2009. 2 апр. В статье рассказывается о признании судом г. Екатеринбурга в качестве доказательства полученной с помощью цифровых технологий картографической схемы с записью маршрута движения патрульного автомобиля милиции, (оборудованного спутниковой системой позицио-нирования), сотрудники которой были признаны виновными в совершении преступления, предусмотренного ст. 105 УК РФ.

ции получили также широкое распространение и правовую регламентацию [1].

Именно цифровая подпись и отметки времени являются теми инструментами, которые позволяют создать правовые основы для электронного документооборота в сетях Интернет, заключать сделки в Сети, создавать платежные системы нового типа и электронные ценные бумаги. Технологии цифровой подписи находят применение также для документооборота в сфере юстиции и управления [2]. Так, компанией Microsoft проведены работы по внедрению электронного оборота в нескольких верховных судах штатов США и в Международном коммерческом суде в Нью-Йорке. Установленное программное обеспечение делает возможным электронную подачу документов в суд через Интернет. Подобные программы внедрялись также компаниями *Intelliquest Information Group и Precise Software Technologies* в судах штатов Юта и Канзас [3].

Сегодня без использования криптографических алгоритмов ЭЦП немыслимо решение задач по обеспечению безопасности информации, связанных с конфиденциальностью и целостностью, аутентификацией и невозможностью отказа сторон от авторства. Если до 1990 г. криптография

[1] Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (часть I). Ст. 3448; Федеральный закон Российской Федерации от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» // Собрание законодательства РФ. 2002. № 2. Ст. 1272; постановление Правительства Российской Федерации от 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации» // Собрание законодательства РФ. 2006. № 34. Ст. 3691; ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию»; ГОСТ Р 51624-2000 «Защита информации. АС в защищенном исполнении. Общие требования»; Требования к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну; в/ч 43753, 2007 г.; Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005) (утверждено приказом ФСБ России от 9 февраля 2005 года № 66); Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (утверждена приказом ФАПСИ от 13 июня 2001 г. № 152); Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) (утверждены приказом ФСТЭК (Гостехкомиссии) России от 30 августа 2002 г. № 282); Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», ФСТЭК (Гостехкомиссия) России.

См. подробнее: Автоматизированная система органов предварительного следствия как информационная система обработки персональных данных // Информационный бюллетень Следственного комитета при МВД России. 2009. № 4 (142). С. 132—138 (для служебного пользования).

[2] См.: *Агеев В.Н.* Правовое регулирование цифровой подписи и отметок времени в Германии.

[3] См.: *Ясневская А.* Правосудие — это власть юристов плюс электронизация всех судов // Юридическая практика. 1998. №16.

обеспечивала «закрытие» исключительно государственных линий связи, то в наши дни использование криптографических методов получило широкое распространение благодаря развитию компьютерных сетей и электронного обмена данными в различных областях: финансах, банковском деле, торговле и т.п. Представляется, что значение криптографических методов в указанных областях будет возрастать и далее [1].

Однако нельзя не отметить, что в настоящее время в преобладающем большинстве случаев технология ЭЦП применяется при передаче текстовых файлов и графической информации. Вместе с тем криптографические технологии ЭЦП могут применяться и при проведении конференц-связи [2]. Нам представляется, что в программно-техническом аспекте не имеет значения, что «подписывать» ЭЦП — файл, содержащий одну статическую фотографию (передаваемую по телекоммуникационным каналам) или файл, содержащий динамическую последовательность 24 фотографий, произведенных за одну секунду, что как известно будет составлять один кадр динамического видеоизображения.

Таким образом, если весь сеанс ВКС (потенциально каждый кадр выступления каждого абонента) будет подписан ЭЦП, то нам представляется, что данный видеопротокол будет полностью легитимен, т.е. выступать в качестве допустимого доказательства. Здесь следует отметить, что как таковые документы, подписанные ЭЦП (в частности, фирмы «ЛАН Крипто») признаются арбитражными судами [3]. Также хочется отметить, что современные криптоалгоритмы гарантируют значительную стойкость ЭЦП. Так для подделки цифровой подписи потребуется более 250 лет работы компьютера мощностью 100 млрд операций/с [4].

Вместе с тем быстродействие современных разрабатываемых квантовых компьютеров, нейрокомпьютеров, оптических компьютеров ставят под угрозу криптостойкость существующих алгоритмов ЭЦП. Кроме того, общепринято, что стойкость систем цифровых подписей основана на трудоемкости задачи факторизации (разложение больших чисел на множители) или на трудоемкости задачи дискретного логарифмирования. Эти две математические задачи известны достаточно давно, и до сих пор для них не найдено эффективных алгоритмов. Однако это вовсе не означает, что таких алгоритмов не существует. В последние годы (именно в связи с криптографической проблематикой) эти задачи активно изучаются математиками всего

[1] См.: *Алферов А.П., Зубов А.Ю., Кузьмин А.С, Черемушкин А.В.* Основы криптографии: учеб. пос. М., 2001. С. 3.

[2] См.: Там же. С. 401.

[3] См.: *Петраков А.В., Лагутин В.С.* Защита абонентского телетрафика. М., 2001. С. 347.

[4] См.: Там же.

мира. Если для них будут найдены эффективные алгоритмы, это будет означать крах соответствующих криптосистем [1].

Однако бурное развитие квантовой технологии и волоконно-оптических линий связи привело к появлению квантово-криптографических систем. Они являются предельным случаем защищенных волоконно-оптических линий связи (ВОЛС). Использование квантовой механики для защиты информации позволяет получать результаты, недостижимые как техническими методами защиты ВОЛС, так и традиционными методами математической криптографии. В квантово-криптографическом аппарате применим принцип неопределенности Гейзенберга, согласно которому попытка произвести измерения в квантовой системе вносит в нее нарушения, и полученная в результате такого измерения информация определяется принимаемой стороной как дезинформация. Исследования показали, что попытка перехвата информации из квантового канала связи неизбежно приводит к внесению в него помех, обнаруживаемых законными пользователями этого канала [2].

Квантовая криптография использует этот факт для получения фундаментально защищенного канала, где сообщения передаются в виде фотонов с направлениями поляризации 0°, 45°, 90° и 135°. В результате получается такой канал связи, что передаваемые по нему данные даже теоретически не могут ни читаться, ни копироваться нарушителем. Нарушитель не может извлечь никакой, даже частичной, информации об этих данных таким способом, который не поддавался бы контролю, и который не смогли бы обнаружить законные пользователи канала [3].

В настоящее время уже во многих странах мира квантовые криптосистемы на базе ВОЛС реализованы экспериментально, а в некоторых странах введены в опытную эксплуатацию. В частности, в Лосамосской национальной лаборатории завершена разработка и введена в опытную эксплуатацию в США линия связи общей длиной 48 км, в которой реализованы принципах квантовой криптографии. Последние разработки в области квантовой криптографии позволяют создавать системы, обеспечивающие практически стопроцентную защиту ключа и ключевой информации [4].

Таким образом, мы полагаем, что технологии ЭЦП с успехом могут применяться не только в настоящий период времени, но и в обозримом будущем, поскольку из изложенного видно, что использование подобных криптоалгоритмов на базе ВОЛС имеет весьма благоприятный прогноз.

---

[1] См.: *Петраков А.В., Лагутин В.С.* Защита абонентского телетрафика. М., 2001. С. 342.
[2] См.: Там же. С. 448—455.
[3] См.: *Алферов А.П., Зубов А.Ю., Кузьмин А.С, Черемушкин А.В.* Указ. соч. С. 423.
[4] См.: *Петраков А.В., Лагутин В.С.* Указ. соч. С. 455.

Можно полагать, что в обозримом будущем вся криптографическая защита информации и распределение ключей будут базироваться на квантово-криптографических системах.

На сегодняшний день представляется целесообразным решение в уголовно — процессуальном законодательстве вопроса о допустимости тех или иных научно— технических средств лишь в самом общем виде, а конкретный перечень такого рода технических средств излагать в подзаконных нормативных актах (приказах, инструкциях, положениях и т.п.). Перечни эти необходимо время от времени пересматривать и дополнять.