Прокопова А. А., научный сотрудник центра по исследованию проблем расследования преступлений НИИ, магистр юриспруденции, капитан полиции
(Карагандинская академия МВД РК им. Б. Бейсенова)

ИСПОЛЬЗОВАНИЕ СРЕДСТВ ВИДЕОКОНФЕРЕНЦ-СВЯЗИ ПРИ ПРОВЕДЕНИИ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ КАК ОДНО ИЗ НАПРАВЛЕНИЙ СОВЕРШЕНСТВОВАНИЯ ПРОЦЕССА ДОСУДЕБНОГО ПРОИЗВОДСТВА

В настоящий момент законодателем страны разрабатывается Уголовно-процессуальный кодекс Республики Казахстан, являющийся основным актом, регулирующим уголовное судопроизводство. В новом кодифицированном акте должны гармонично сочетаться лучшие стороны отечественной системы, современные процедуры, а также адаптированные имплементации из мирового опыта.

В связи с этим особую важность приобретает один их продуктивных способов совершенствования процесса расследования, не требующий значительных изменений его формы, — использование научно-технических достижений в выявлении, закреплении и исследовании объективной доказательственной информации. Кроме того, постоянно расширяющиеся возможности использования достижений науки и техники в следственной практике позволяют по-новому решать конкретные вопросы раскрытия и расследования правонарушений. Научно-технический прогресс вносит много нового в теорию и практику борьбы с правонарушениями, изменяет методы доказывания и содержание профессионального уровня деятельности правоохранительных органов, ставит важные проблемы дальнейшего совершенствования процессуальной деятельности на научной основе.

В мировом опыте уголовного судопроизводства в настоящее время все активнее применяются средства видеоконференц-связи в процессе расследования.

Видеоконференц-связь (далее — ВКС) — это телекоммуникационная технология интерактивного взаимодействия двух и более удаленных абонентов, при которой между ними возможен обмен аудио- и видеоинформацией в реальном масштабе времени с учётом передачи управляющих данных[1].

Видеоконференция во всем мире применяется как средство оперативного принятия решения в той или иной ситуации; при чрезвычайных ситуациях; для сокращения командировочных расходов в территориально распределенных организациях, а также как один из элементов технологий телемедицины и дистанционного обучения.

Во многих государственных и коммерческих организациях видеоконференции приносят большие результаты и максимальную эффективность, а именно:

- снижают время на переезды и связанные с ними расходы;
- ускоряют процессы принятия решений в чрезвычайных ситуациях (совещания различных ведомств);
- увеличивают производительность труда;
- дают возможность принимать более обоснованные решения за счет привлечения при необходимости дополнительных экспертови т. д.

В 2011 г. Российской Федерацией на законодательном уровне закреплена возможность проведения судом допроса свидетеля и потерпевшего с помощью систем видеоконференц-связи. Только за первое полугодие специализированным отделом по обеспечению установленного порядка деятельности арбитражных и военных судов УФССП России по Москве на базе Московского окружного военного суда организовано получение показаний от 55 свидетелей и потерпевших путем использования систем видеоконференц-связи и программы

«Skype». Благодаря подобной практике в первом полугодии сэкономлено порядка **1,3** млн. рублей[2]**.**

Рассмотрим более подробно процесс видеоконференции. Для общения в режиме видеоконференции абонент должен иметь терминальное устройство (кодек) видеоконференц-связи, видеотелефон или иное средство вычислительной техники. Как правило, в комплекс устройств для видеоконференц-связи входит:

- центральное устройство — кодек с видеокамерой и микрофоном, обеспечивающий кодирование/декодирование аудио-и видеоинформации, захват и отображение контента;
- устройство отображения информации и воспроизведения звука.

В качестве кодека может использоваться персональный компьютер с программным обеспечением для видеоконференций.

Большую роль в видеоконференции играют каналы связи, т. е. транспортная сеть передачи данных. Для подключения к каналам связи используются сетевые протоколы **IP**[3] или **ISDN**[4]**.**

Существуют два режима работы ВКС, которые позволяют проводить двусторонние (режим «точка-точка») и многосторонние (режим «много-точка») видеоконференции.

Основную роль в видеоконференции играют каналы связи между абонентами. Самый простой и дешёвый метод организации ВКС — через Интернет. Однако качество сеанса связи в данном случае может быть низким, так как интернет не является гарантированным каналом передачи аудио- и видеоданных. К этому добавляется проблема безопасности видеоконференции, поскольку она может быть предана огласке в случае несанкционированного взлома системы. Для организации видеоконференц-связи через Интернет требуется иметь статические **IP**-адреса и каналы связи с пропускной способностью не менее **384** кБит/св обе стороны (для исходящего и входящего трафика).

Немного сложнее настраивается связь по протоколу инкапсуляции[5] видовой маршрутизации **GRE** (англ. **GenericRoutingEncapsulation).** Протокол принадлежит к сетевому уровню. Он может инкапсулировать другие протоколы, а затем осуществлять маршрутизацию всего набора до места назначения. В данном случае обеспечивается минимальная защита видеотрафика в сети Интернет, что позволяет предотвратить основное число «неопытных» вторжений в информационное облако видеоконференц-связи. Тот же принцип, хоть и намного более высокого уровня безопасности, заложен и в протоколе **IPsec**[6]**.**

Вопрос конфиденциальности информации стоит очень остро, поскольку применение данных технологий в ходе расследования чревато разглашением информации. Однако некоторые ученые считают, что проведение подобных видеоконференций и защита поступившей информации не представляют особой технической сложности, а использование каналов сети Интернет обходится значительно дешевле стоимости использования обычных телевизионных каналов и несравнимо с финансовыми затратами на заграничные командировки следователей[7]**.** Кроме того, существуют различные виды систем, которые способны на очень высоком уровне защищать поток проходимой по ним информации. К таким системам относится **VPN** (англ. **VirtualPrivateNetwork** — виртуальная частная сеть)[8] — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет), имеющих более надежную степень защиты благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений, передаваемых по логической сети сообщений)[9]**.**

Реализация **VPN**-сети осуществляется при помощи специального комплекса программно-аппаратных средств. Такая реализация обеспечивает высокую производительность и, как правило, высокую степень защищённости, примером защищенных **VPN** являются **IPSec**[10]**, OpenVPN**[11] и **PPTP**[12]**.**

Интернет предполагает возможность проведения видеоконференции в режиме реального времени с передачей изображения и звука. Поскольку при производстве следственных действий, как правило, не возникает необходимости в проецировании изображения на большой экран, для проведения так называемых «локальных видеоконференций» может быть использован обычный (подключенный к сети Интернет) компьютер со стандартным монитором и миниатюрной видеокамерой[13]. Так, с помощью программ **«Skype»,**[14] **«Speakfree»** и других возможно проведение следственного действия со свидетелем, находящимся в любой точке мира, где есть подключение к сети Интернет. На экран монитора будет транслироваться видеоизображение свидетеля, а динамики довольно качественно передадут звук голоса. Следственное действие (и звук, и видеоизображение) может записываться и воспроизводиться при необходимости. Запись следственного действия в обязательном порядке производится

стороной-инициатором (запрашивающей стороной), причем если такой «видеопротокол» осуществляется посредством Интернет-видеокон-ференций, то он может содержать достоверные данные **GPS**-позиционирования о месте (дате, времени) нахождения любого участвующего в ВКС лица и, кроме того, может быть подписан электронно-цифровой подписью его идентифицированных биометрическими методами участников[15].

Анализ мирового опыта, а также практики применения видеоконференц-связи в уголовном судопроизводстве Российской Федерации, позволил разрабрать алгоритм проведения следственного действия с использованием ВКС посредством сети Интернет, на примере допроса свидетеля.

Алгоритм допроса.

Подготовительный этап:

1) *анализ информации по делу (установленные обстоятельства по делу, подлежащие установлению, подготовка плана допроса);*

2) определение состава участников следственного действия;

3) выяснение возможности участия свидетеля при проведении следственного действия;

Следователь удостоверяется в том, что возможность личного присутствия допрашиваемого лица при проведении следственного действия отсутствуют. Установив уважительную причину (состояние здоровья, нахождение в другом городе, области, за пределами РК), следователь, принимает решение о проведении следственного действия с использованием видеоконференц-связи;

4) определение места и времени допроса, а также технических возможностей проведения следственного действия.

После установления местонахождения допрашиваемого следователь связывается с территориальным отделом полиции по месту нахождении свидетеля для определения возможности проведения следственного действия[16].

Для этого сотрудникам территориального подразделения ОВД по месту пребывания свидетеля может быть дано отдельное поручение об организации проведения следственного действия.

Отдельное поручение должно содержать в себе поручение о проведении следственного действия, сведения о допрашиваемом лице, дату и время допроса, технические характеристики компьютера и программы связи, а также логин, под которым зарегистрирован следователь в программе, посредством которой будет осуществляться соединение между компьютерами. Кроме того, в отдельном поручении отражается порядок направления результатов следственного действия. Для экономии времени отдельное поручение может быть передано электронной почтой МВД.

Сотрудники подразделения ОВД, получившего отдельное поручение, принимают меры к обеспечению следственного действия (техническая подготовка, вызов допрашиваемого в указанное время для проведения следственного действия и т. д.);

5) проверка соединения между подразделениями.

Перед проведением следственного действия должно быть проведено пробное соединение между компьютерами, находящимися в территориальных подразделениях ОВД, для проверки технических возможностей и устранения неполадок.

После проведения всех подготовительных мероприятий в установленное время следователь приступает к проведению следственного действия.

Рабочий этап:

1) Установление связи между подразделениями.

При установлении соединения с вызываемым абонентом программы связи следователь проверяет качество изображения и звука. Убедившись в качестве соединения, следователь приступает к проведению следственного действия, включает режим видеозаписи для дальнейшего приобщения видеозаписи следственного действия к материалам уголовного дела;

2) проведение допроса.

В начале следователь удостоверяет личность свидетеля (при необходимости можно запросить снимок документов, удостоверяющих личность, сделанный при помощи **Web**-камеры, установленной на компьютере в месте нахождения свидетеля).

Удостоверившись в личности допрашиваемого, следователь объявляет цель и порядок проведения следственного действия, представляем участников, разъясняет их права и обязанности.

Изложение и фиксация показания осуществляются по общим правилам ст. **214** УПК РК. Показания свидетеля фиксируются в протоколе допроса следователем, ведущим допрос.

В протоколе должны быть отражены все действия, осуществляемые следователем и участниками следственного действия, применяемая техника, используемое программное обеспечение, качество изображения и звука и т. д.

Заключительный этап:

1) оформление результатов.

После внесения всех показаний в протокол документ в электронном варианте направляется по месту нахождения свидетеля.

Получив документ по средствам программы связи, сотрудник, находящийся с допрашиваемым, распечатывает протокол и ознакамливает с ним свидетеля. Свидетель, ознакомившись с протоколом, подписывает его, в документе также расписывается сотрудник, удостоверяющий факт проведения следственного действия;

2) направление результатов следственного действия.

Протокол допроса направляется почтой либо его электронная копия, полученная посредствам сканирования бумажного носителя, пересылается по техническим каналам связи **(fax, e-mail**)в территориальное подразделение, инициировавшее проведение следственного действия. Полученный документ приобщается к материалам уголовного дела вместе с видеозаписью допроса на электронном носителе.

Приведенный выше алгоритм может изменяться в соответствии с действующим законодательством и совершенствованием научно-технических средств, используемых в ОВД (например, применение электронно-цифровых подписей сотрудниками ОВД ускорит алгоритм и процесс удостоверения и подписи документа. Достаточно будет внесения в электронный файл допроса электронной подписи следователя, удостоверяющего ход допроса).

Проведение допросов при помощи видеоконференц-связи позволит сократить время проведения ряда следственных действий, вызывающих в настоящий момент много сложностей в ходе расследования уголовного дела. В данном случае отпадет необходимость вызова на допрос (допрос в больницах); ожидания допрашиваемого лица из командировок (вахт), отпусков; выезда сотрудников следственных и оперативных подразделений в служебные командировки для проведения следственных действий по месту пребывания свидетеля и. т. д.

Резюмируя, отметим, что юридическое закрепление в Уголовно-процессуальном кодексе Республики Казахстан процедуры применения видеоконференц-связи для проведения следственных действий, позволит значительно упростить ход расследования путем сокращения времении материальных расходов, необходимых для проведения ряда процессуальных процедур.

1 Елисеев И. ВКС от семи бед// Сети. **— 2007. № 9.**

2 Московские приставы за счет введения допроса свидетелей через Интернет сэкономили **1,3** млн на доставке свидетелей из других регионов **//www.tasstelecom.ru/news/one**

3 **InternetProtocol (IP,** досл. «межсетевой протокол») — маршрутизируемый протокол сетевого уровня стека **TCP/IP.** Именно **IP** стал тем протоколом, который объединил отдельные компьютерные сети во всемирную сеть Интернет. Неотъемлемой частью протокола является адресация сети.

4 **ISDN** (англ. **IntegratedServicesDigitalNetwork)** — цифровая сеть с интеграцией служб. Позволяет совместить услуги телефонной связи и обмена данными. Основное назначение **ISDN** — передача данных со скоростью до **64** кбит/спо абонентской проводной линии и обеспечение интегрированных телекоммуникационных услуг (телефон, факс, и пр.). Использование для этой цели телефонных проводов имеет два преимущества: они уже существуют и могут использоваться для подачи питания на терминальное оборудование.

5 Инкапсуляция **—** в объектно-ориентированном программировании **—** сокрытие внутренней структуры данных и реализации методов объекта от остальной программы.

6 Видеоконференция. Материал из Википедии — свободной энциклопедии// **http://ru.wi ki pedi a.org**

7 Халиулин А.Г. Использование телекоммуникаций в уголовно-процессуальной деятельности // Прокурорская и следственная практика. **—1999. — №1-2. —** С. **176.**

8 Устоявшийся термин; правильнее — «виртуальная закрытая сеть». Слово **private,** в числе прочего, имеет значение «персональный», «секретный», «закрытый».

9 **VPN.** Материал из Википедии — свободной энциклопедии// **http://ru.wikipedia.org/wiki/VPN**

10 **IPsec** (сокращение от **IP Security)** — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу **IP.** Позволяет осуществлять подтверждение подлинности (аутентификацию),

проверку целостности и/или шифрование **IP**-пакетов. **IPsec** также включает в себя протоколы для защищенного обмена ключами в сети Интернет.

11 **OpenVPN** — свободная реализация технологии Виртуальной Частной Сети **(VPN)** с открытым исходным кодом для создания зашифрованных каналов типа «точка-точка» или сервер-клиенты между компьютерами. Она позволяет устанавливать соединения между компьютерами, находящимися за **NAT-firewall,** без необходимости изменения их настроек.

12 **PPTP** (англ. **Point-to-PointTunneli ngProtocol)** — туннельный протокол типа «точка-точка», позволяющий компьютеру устанавливать защищенное соединение с сервером за счёт создания специального туннеля в стандартной, незащищённой сети. **PPTP** помещает (инкапсулирует) кадры **PPP** в **I P**-пакеты для передачи по глобальной I P-сети, например Интернет.

13 Сумин С.А. Применение систем видеоконференц-связи при допросе защищаемых территориально удалённых лиц, участвующих в уголовном судопроизводстве на стадиях предварительного и судебного следствия: проблемы реализации и повышение эффективности// Вестн. Воронежск. инс-та МВД России. — **2011. № 3.** — С. **69.**

14 **Skype** — бесплатное проприетарное программное обеспечение с закрытым кодом, обеспечивающее шифрованную голосовую связь и видеосвязь через Интернет между компьютерами (VoIP), используя технологии пиринговых сетей, а также платные услуги для звонков на мобильные и стационарные телефоны. **Skype** имеет **663** миллиона пользователей по состоянию на сентябрь **2011** г.

15 Сумин С.А. Применение технических средств видеоконференцсвязи в процессуальной деятельности // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений: Сб. мат-лов международ, науч.-практ. конф. — Воронеж, **2010. —** С**.201-202.**

16 Стоит отметить, что для проведения следственного действия посредством видеоконференц-связи каждое территориальное подразделение ОВД должно быть зарегистрировано в соответствующей программе с технологией пиринговых сетей **(Skype, ICQ** и т. п.) и иметь доступ к сети Интернет.