Таким образом, наиболее экономически эффективным комплексом мероприятий, направленным на снижение заболеваемости ВИЧ и ВГС, является комплекс из синхронно реализуемых программ ПИШ (40 %), ОЗТ (20 %), АРТ (90 %) и ДВИЧ (90 %), так как только при синхронном применении разнонаправленных компонентов программы возможно существенное сокращение уровня смертности в связи с этими заболеваниями и повышение продолжительности жизни (сохраненные годы полноценной жизни) при приемлемых для государства экономических затратах.

УДК 343.982.067

В.Е. Козлов

ОБ ОТДЕЛЬНЫХ АСПЕКТАХ ОБНАРУЖЕНИЯ, ФИКСАЦИИ И ИЗЪЯТИЯ СЛЕДОВ-ПРЕДМЕТОВ В СЕТИ ИНТЕРНЕТ ПРИ РАССЛЕДОВАНИИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Важнейшими следами-предметами, подлежащими обнаружению, фиксации и изъятию в ходе производства следственных действий и проведения оперативно-розыскных мероприятий (ОРМ) при расследовании, а также выявления и раскрытия компьютерных (высокотехнологичных) преступлений, являются документы на бумажных и электронных носителях. Это могут быть распечатки работы прикладного программного обеспечения, листинги исходных текстов программ, иная информация, относящаяся к расследуемому событию [1, с. 148] (например, регистрационные файлы, формируемые на уровне операционных систем, прикладного программного обеспечения, а также баз данных). Особо значимыми при этом считаются те из них, которые ведет оператор электросвязи (ЭС) – провайдер интернета, осуществляя документирование и хранение сведений о действиях пользователя интернет-услуг (ПИУ).

Анализ семиуровневой модели ISO/OSI позволяет определить сведения, анализ которых необходимо осуществлять в ходе расследования компьютерных преступлений. К таковым относятся следующие.

Географическое местонахождение ПИУ – государство, провайдер интернета, иная организация, а также местное время ПИУ.

Тип средства компьютерной техники (СКТ) – операционная система, разрешение монитора, разработчик и версия коммуникационного программного обеспечения, при помощи которого ПИУ осуществляет обращение к интернет-ресурсу.

Факты работы ПИУ с того же СКТ, что и в течение предыдущего сеанса работы, а также – страницы Web или файлы, полученные ПИУ из интернет-ресурсов. Ссылки с этих ресурсов, использованных ПИУ, либо оставленных им без внимания.

Страница Web, с которой ПИУ знакомился до того, как попал на интернет-ресурс, и следующая страница, на которую перешел после этого. Вопросы, формулируемые и задаваемые ПИУ поисковым системам интернета.

Факты шифрования компьютерной информации на участке передачи ее между СКТ ПИУ и ресурсом, способы ее шифрования и получения ключей.

Списки почтовой рассылки ПИУ, а также групп новостей, с которыми он регулярно знакомится.

Требования к информации, хранящейся у ЭС, оказывающих услуги по доступу в интернет, сформулированы в постановлении Министерства связи и информатизации Республики Беларусь от 18 февраля 2015 г. № 6 «Об утверждении Инструкции о порядке формирования и хранения сведений о посещаемых пользователями интернет-услуг информационных ресурсах». Поставщики интернет-услуг обязаны с использованием собственного аппаратно-программного комплекса формировать и хранить актуальные сведения о посещаемых ПИУ интернет-ресурсах, которые включают в себя сведения о ПИУ, и обо всех услугах ЭС, им активированных, а также дату, время начала и окончания соединений, внутренний и внешний IP-адреса и порты оконечного абонентского устройства, доменное имя или IP-адрес и порт посещаемого ПИУ интернет-ресурса, объем переданных и принятых данных. Постановлением детализирована документированная информация, подлежащая хранению в течение одного года. Например, для физических лиц:

номер и дата заключения договора на оказание услуг ЭС, фамилия, имя, отчество, адрес пользователя или адрес установки оконечного абонентского устройства;

данные, позволяющие идентифицировать ПИУ или его оконечное абонентское устройство, MAC-адрес или идентификационный номер оконечного абонентского устройства ПИУ сотовой подвижной ЭС;

для абонентов сети сотовой подвижной ЭС – реквизиты документа, удостоверяющего личность.

Следует отметить, что названные правовые и организационные меры доказали свою эффективность во многих странах и вытекают из рекомендаций Международной Конвенции о киберпреступности (23 ноября

2001 г., г. Будапешт, Республикой Беларусь не ратифицирована). Однако существуют и определенные ограничения по использованию их результатов в предупреждении, выявлении, раскрытии и расследовании компьютерных преступлений, которые детерминированы возрастающей квалификацией ПИУ, заключающейся в использовании возможностей интернета для сокрытия преступной деятельности. Анализ семиуровневой модели ISO/OSI, а также доступных ПИУ технологий к таковым позволяет отнести:

proxy-серверы (Opera, Google и т. д.), а также VPN-сервисы и серверы «анонимизации»;

технологии децентрализованных сетей (Invisible Internet Project – I2P), гибридных анонимных сетей (The Onion Router – Tor).

Применение указанных технологий существенно затрудняет процесс идентификации ПИУ и использованных им интернет-ресурсов. Кроме того, для сокрытия действий, направленных на подготовку, совершение и сокрытие преступлений, все чаще отмечается использование виртуальных машин и шифрование носителей, либо размещение файлов виртуальной машины на зашифрованном носителе. В этих случаях их удаление из СКТ ПИУ делает невозможным применение криминалистических рекомендаций, посвященных обнаружению, фиксации и изъятию следовой информации с рабочего места ПИУ. Отмеченные обстоятельства позволяют говорить о потребности в осуществлении непрерывного научно-методического сопровождения оперативно-розыскной деятельности (ОРД) и следственной практики по делам о компьютерных преступлениях и прежде всего о внедрении в практическую деятельность следственных и оперативных подразделений новейших теоретико-прикладных разработок криминалистического оперативно-технического обеспечения выявления и расследования компьютерных преступлений. Таким образом, целесообразно выделить ряд проблемных вопросов, нуждающихся в комплексном теоретико-прикладном разрешении [2].

1. Вопросы использования криминалистических и иных знаний о компьютерной преступности при осуществлении противодействия общеуголовным, экономическим преступлениям, преступлениям, связанным с незаконным оборотом наркотиков, в особенности транснациональным, совершаемыми организованными преступными группами с использованием коммуникационных возможностей интернета, «теневого интернета» и «темного интернета».

2. Вопросы разработки и совершенствования положений тактики использования научно-технических средств, предназначенных для об-

наружения, фиксации и изъятия следов компьютерных преступлений, при производстве следственных действий и проведении ОРМ.

3. Вопросы совершенствования основных положений тактики производства следственных действий и проведения ОРМ по делам рассматриваемой категории, в целом, – методики раскрытия и расследования таких преступлений.

Названные обстоятельства обусловливают потребность дальнейшего развития криминалистической теории и теории ОРД, обогащения ее достижениями иных отраслей науки.

1. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. М. : Горячая линия – Телеком, 2002. 336 с.

2. Козлов В.Е. Противодействие компьютерной преступности: проблемные вопросы и пути их разрешения : монография. Минск : Акад. МВД Респ. Беларусь, 2006. 256 с.

УДК 343.98

А.К. Лебедева

НЕКОТОРЫЕ ОСОБЕННОСТИ СУДЕБНОГО ФОНОСКОПИЧЕСКОГО ИССЛЕДОВАНИЯ ОБЛИКОВЫХ ХАРАКТЕРИСТИК ЛИЧНОСТИ В СЛУЧАЯХ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ ДЛЯ ИЗМЕНЕНИЯ ГОЛОСА

В случае отсутствия возможности получения сопоставимых и пригодных образцов устной речи для проведения сравнительного исследования при невозможности решения идентификационных задач судебной фоноскопической экспертизы особое значение придается определению обликовых характеристик личности по фонограммам речи.

Эта задача в теории судебной экспертологии является одним из примеров обратной диагностической задачи [1, с. 86]. В процессе судебного экспертного исследования специалист устанавливает взаимосвязь между характеристиками речи и признаками облика человека, что позволяет в случае успеха получить ориентирующую информацию, необходимую для успешного розыска неизвестного лица.

В области судебной фоноскопической экспертизы [2, с. 54; 3, с. 314] к обликовым характеристикам, диагностируемым в процессе подобного исследования, относятся: половозрастные и анатомо-физиологические характеристики диктора, степень владения языком (на котором лицо говорит на исследуемой фонограмме), региональная принадлежность, эмоциональное состояние и психофизиологическое состояние