Министерство образования и науки РФ
Алтайский государственный университет

УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ И КРИМИНАЛИСТИЧЕСКИЕ ЧТЕНИЯ НА АЛТАЕ

ВЫПУСК XIV

Проблемы противодействие киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами

Сборник научных статей

Барнаул

Издательство Алтайского государственного университета
2017

УДК 343
ББК 67.410.2+67.52
У261

Ответственные редакторы:

С.И. Давыдов, заведующий кафедрой уголовного процесса и криминалистики, доктор юридических наук;

В.В. Поляков, доцент кафедры уголовного процесса и криминалистики, кандидат юридических наук.

У261 Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы противодействие киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами / Сборник научных статей / отв. ред. С.И. Давыдов, В.В. Поляков. - Барнаул: Изд-во Алт. ун-та, 2017. – Вып. XIV.- 118 с.

ISBN 978-5-7904-2251-5

В сборник включены статьи участников тематической XVI Всероссийской научно-практической конференции «Уголовно-процессуальные и криминалистические чтения на Алтае», посвященной проблемам противодействия киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами, и круглого стола по теме «Проблемы разработки методик расследования компьютерных преступлений». В статьях исследуются проблемы раскрытия, расследования и криминалистического предупреждения компьютерных преступлений.

Сборник издается при поддержке проекта РГНФ №16-33-01160.

ISBN 978-5-7904-2251-5

СОДЕРЖАНИЕ

ОСНОВНЫЕ ПОДХОДЫ К СОДЕРЖАНИЮ КРИМИНАЛИСТИЧЕСКОГО АНАЛИЗА ЛИЧНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ

Т.А. Алексеева, преподаватель кафедры уголовного права ЗСФ РГУП; старший преподаватель кафедры уголовного права ЮФ ТУСУР

Р.Л. Ахмедшин, д.ю.н., профессор, профессор кафедры криминалистики Юридического института Томского государственного университета

В.Л. Юань, преподаватель кафедры уголовно-процессуального права ЗСФ РГУП; старший преподаватель кафедры уголовного права ЮФ ТУСУР.

Изменение социо-политической обстановки неминуемо влечет изменение мировосприятия, которое многократно увеличивается если данное изменение идет параллельно с технологическими прорывами. Киберпространство новая реальность современности, предопределяющая перспективы развития современного информационного общества. Неудивительно, что перед криминалистической наукой стоит задача проведения опережающих исследований, предметом которых является преступная деятельность и деятельность по расследованию преступлений в киберпространстве.

Учитывая, что любая аналитическая деятельность возможна лишь при условии наличия определенного объема информации актуально исследование киберпространства как области содержащей криминалистически значимую информацию. Одной из разновидностей, может быть даже приоритетной, является исследование алгоритмов получения криминалистически значимой информации о лице совершившем преступное деяние.

Исследование личности в киберпространстве содержательно определяется:

- изучением информации о лице со сторонних ресурсов – точность данной информации может варьироваться в широком диапазоне;
- сбором информации о лице посредством опроса его знакомых (членов сообществ, участников конференций, активистов веб форумов и пр.) – точность данной информации несколько выше, но в значительной степени определяется фактором везения,

предопределившим вероятность вступления в контакт с человеком обладающим значимой информацией;

• исследованием информации, которое лицо оставило о себе в киберпространстве, как правило в социальных сетях – точность данной информации зависит от навыков анализа косвенной информации, которым обладает следователь или дознаватель.

Первые два описанных пункта вполне вписываются в систему тактических рекомендаций исследования личности в реальном пространстве, по сути мало отличаясь от канонических приемов исследования. Исследование личности, отраженной в материалах социальных сетей есть процесс достаточно творческий и в значительной степени непривычный. Неудивительно, что на данном этапе развития криминалистического знания крайне актуально разработка приемов анализа особенностей личности, прежде всего психологических.

Знание этих психологических особенностей позволяет не только более оптимально спланировать сам ход процесса расследования в целом, но и повысить эффективность проведения отдельных следственных действий, к примеру, допроса, о чем свидетельствуют имеющиеся на сегодня результаты проведенных научных исследований [1. С. 21-22, 2. С. 65-66, 3. С. 242-243].

Анализ фотоизображений, содержащихся на социальной странице Современное развитие науки и техники увеличило количество источников сведений о личности как минимум, еще на один. Речь идет о социальных сетях, в которых пользователи имеют возможность загружать различные изображения. Именно эти изображения, фотографии и картинки являются источниками, потенциально содержащими криминалистически значимую информацию о личности, анализ которой позволит подобрать наиболее эффективные методы психологического воздействия на такое лицо во время проведения следственных действий с его участием (к примеру, допроса), а также получить иные важные данные, имеющие прямую или косвенную криминалистическую ценность для решения криминалистических задач и достижения криминалистически значимой цели в процессе расследования уголовного дела.

Представляется целесообразным проведение анализа каждой фотографии пользователя с использованием трехступенчатого алгоритма. Первая ступень, это оценка источников криминалистически значимой информации, содержащихся в фотографиях, на которой

оценивается. Во-первых, количество фотографий. Первоначально, необходимо оценить суммарное количество всех фотографии, загруженных и привязанных к данному аккаунту (странице). Во-вторых, давность фотографий. Из суммарного количества всех доступных в аккаунте (странице) фотографий высчитывается количество фотографий, загруженных относительно недавно (примерно, в течение года). В-третьих, относимость фотографий. Здесь следует выделить из общего числа фотоснимков три показателя: во-первых, доля фотоснимков, которые имеют непосредственное отношение к личности пользователя, во-вторых доля фотоснимков, которые имеют опосредованное отношение к личности пользователя и в-третьих доля фотоснимков, которые не имеют ярковыраженного прямого отношения к личности пользователя.

Вторая ступень, это анализ источников криминалистически значимой информации, содержащихся в фотографиях, который включает в себя следующие критерии. Во-первых, формальный анализ фотографии. По данному критерию необходимо проанализировать внешнюю сторону фотографии и определить следующие ее характеристики: во-первых, наличие следов обработки фотоснимка; во-вторых, в каких условиях была произведена фотосъемка; в-третьих, каким образом было снято; в-четвертых, состав фотоснимка (однородная фотография или коллаж); в-пятых, тип фотографии (любительская, профессиональная). Во-вторых, содержательный анализ фотографии. По данному критерию необходимо проанализировать внутреннюю сторону фотографии и определить следующие ее характеристики: во-первых, ярковыраженные биологические параметры того, кто изображен на снимке на основе анализа внешности пользователя (пол, возраст, состояние здоровья, особенности пропорций тела, раса); во-вторых, очевидные социальные характеристики того, кто изображен на снимке на основе анализа одежды, аксессуаров, предметов, инструментов и обстановки вокруг пользователя (профессиональная деятельность, образование, жилье); в третьих, вероятные психологические данные того, кто изображен на снимке на основе анализа прически, одежды, аксессуаров, предметов, инструментов и обстановки вокруг пользователя (религиозные, политические, морально-этические (мировоззрение) взгляды, спортивный досуг, хобби); в четвертых, социальное взаимоотношение между присутствующими на фотоснимке (положение участников в кадре, положение рук и ног, позы, наличие одинаковых элементов

одежды, аксессуаров и др.); в пятых, где и(или) у кого происходила съемка кадра (обстановка на заднем фоне, здания, транспортные средства, строения, сооружения, предметы и вещи, посторонние люди, случайно вошедшие в кадр). В-третьих, контекстуальный анализ. По данному критерию необходимо проанализировать связующую сторону фотографии и определить следующие ее характеристики: во-первых, контекст фотоснимка в рамках жизнедеятельности пользователя; во-вторых, наличие других фотоснимков на данном аккаунте(странице), связанных с этой фотографией; в третьих, связь даты размещения фотографий с датой производства фотоснимка; в четвертых, география данного фотоснимка; в пятых, значение фотоснимка.

III. Вывод из оценки и анализа источников криминалистически значимой информации, содержащихся в фотографиях. На этой, заключительной ступени, следует выделить следующие этапы. Во-первых, вывод о связи аккаунта (страницы) с личностью пользователя. На данном этапе следует выяснить, насколько связан аккаунт (страница) с личностью пользователя с целью установления степени отражения свойств личности пользователя в данных самого аккаунта (страницы) и, как следствие, насколько высоко содержание криминалистически значимой информации о личности пользователя в фотографиях, т.е. какова сама ценность аккаунта (фотографий) как источника информации. Во-вторых, вывод о биографических фактах личности пользователя. Здесь следует сгруппировать все фотографии по принципу отражения в них тех или иных биографических фактов личности пользователя: во-первых, сведения о семье пользователя; во-вторых, сведения о месте жительства и жилищных условиях пользователя; в-третьих, сведения об окружении пользователя; в-четвертых, сведения о взглядах пользователя; в-пятых, сведения об интересах пользователя; в шестых, сведения о способностях пользователя; в седьмых, сведения о деятельности пользователя. В-третьих, вывод о вероятной акцентуации личности пользователя. Здесь следует на основе анализа фотографий пользователя попытаться выделить наиболее ярковыраженные типовые тенденции, характерные для одного определенного акцентуированного типа, отраженные в фотографиях этого пользователя на данном аккаунте(странице).

Таким образом, данные рекомендации имеют потенциал повысить эффективность подготовки к проведению ряда следственных действий, обеспечивая следователя определенным знанием психологии личности участников уголовного судопроизводства при

решении криминалистических задач и повышения результативности при достижении криминалистически значимой цели расследования преступлений по уголовным делам.

Появление социальных сетей, предоставляющих открытый доступ к личной информации, позволило следователям использовать указанную информацию для получения криминалистическо-значимой информации о личности преступника, его психологическом типе и модели типового поведения [4] непосредственно до начала производства следственных действий. Одним из источников информации о личности преступника, содержащихся в социальных сетях, является текст, который может быть проанализирован как с точки зрения содержания, так и посредством заключенных в нем символов [5].

Текстовую информацию, представляющую аккаунт человека, можно условно разделить на три группы: 1) текстовые сведения, расположенная непосредственно на личной странице; 2) переписка в разделе «Сообщения»; 3) текстовые файлы в разделе «Документы». Рассмотрим каждую из групп более детально.

Анализ **текстовых сведений, содержащихся на социальной странице** можно считать разновидностью биографического метода изучения личности [6], который применяться следователями на стадии подготовки к производству следственных действий.

К биографическим данным, полученным из социальных сетей, относятся: имя, фамилия, дата рождения, семейное положение, наличие близких родственников, образование, прохождение военной службы, место работы, страна/город рождения (проживания). По сути, данный блок содержит в себе сведения, необходимые следователю перед началом производства следственных действий. Указанная информация может быть проанализирована, главным образом, с точки зрения содержания, так у следователя появляется возможность сделать вывод о социальном статусе человека, уровне его образования и интеллектуального развития; способности противостоять следователю при осуществлении правомерного воздействия.

При анализе другого рода текстовой информации должно учитываться не только содержание, но и символьное значение [7]. К ней относится: *«статус»* - информация, которую человек посчитал важной и необходимой для освещения в настоящий момент; *«любимые цитаты»* - характеристика себя через призму высказываний других; *«о себе»* - идентификация и оценка себя самого; *«главное в людях»* -

качество, которое человек ценит в себе; *«вдохновляют»* – показатель интроветртности или экстравертности.

И последняя текстовая информация в этой группе – это личные комментарии на «стене» или в «ленте». Личные комментарии представляют собой пояснения к выбранным ресурсам социальной сети, либо к прикрепленным файлам, или ответы на комментариии других пользователей. Как правило, они носят достаточно откровенный и личный характер, так как предназначены для определенного круга лиц, имеющих заинтересованность в общении.

Проблемы при анализе информации из этой группы могут наступить, если страница в социальной сети закрыта для просмотра. В этом случае следователю стоит подключить анализ других источников: фотографий, музыки, видеозаписей и т.д. В случае же доступности страницы, следователь уже на этом этапе может получить необходимый объем сведений о личности преступника и, к тому же на этом этапе не требуется использования специальных средств. Конечно, может существовать риск фальсифицирования данных, однако, скорее всего, это будет носить единичный характрер.

Переписка в разделе «Сообщения», несомненно, представляет наиболее достоверную и объективную информацию о личности преступника. Если будет существовать возможность под каким-либо предлогом вступить в переписку с интересующим следствие лицом, то это предоставит следователю (или оперативному работнику) как доказательство по расследуемому делу (в случае, если предмет общения будет связан непосредственно с преступлением), так и информацию о личности преступника.

В случае наличия разрешения суда на получение доступа к персональным сообщениям преступника исключается риск разоблачения следователя (как это возможно при самостоятельной переписке), и в распоряжение следователя поступает дополнительный источник информации.

Проблемой анализа текста из второй группы является его недоступность и необходимость получения разрешения, что снижает оперативность получения информации. К тому же в случае, если следователю удается получить доступ к перепискам, необходимо изучить достаточно большой объем материала, прежде чем можно будет сделать хотя бы предварительные выводы.

Текстовые файлы в разделе «Документы» чаще всего недоступны для остальных пользователей, однако, в случае их

получения могут быть проанализированы на предмет увлечений человека, деловой и трудовой активности – обмен документами и информацией с коллегами и другими лицами. Свидетельствует об уровне социализации и вовлеченности в оперативный процесс обмена информацией.

Изобилие информации в современном обществе, быстрое ее изменение, развитие новых технологий диктует следователю необходимость использования всех возможных способов получения информации о преступнике, в том числе и социальные сети.

Список использованных источников и литературы

1. Алексеева Т. А. Особенности речи представителей отдельных психологических типов, свидетельствующие о лжи при производстве допроса // Вестник Томского государственного университета. Право. 2015. №1 (15). С. 21-28.

2. Ахмедшин Р. Л. Тактика коммуникативных следственных действий. Томск, Издательский Дом Томского государственного университета, 2014. 294 с.

3. Ведерников Н. Т. Избранные труды. Том 1. Томск, Издательство Томского университета, 2009. 250 с.

4. Ахмедшин Р.Л. Адаптация в криминалистике акцентуированной типологии личности // Сборник материалов криминалистических чтений. Барнаул, 2014. С. 17-18.

5. Алексеева Т.А. Символьное значение устной речи допрашиваемого лица // Российское правоведение: трибуна молодого ученого. Томск, 2012. Вып. 12. С. 228–229.

6. Юань В.Л. Биографический метод как базовый метод изучения личности допрашиваемого перед допросом // Проблемы использования криминалистических знаний в правоприменительной деятельности. Томск, 2014. С 112-114.

7. Алексеева Т.А. Анализ страницы в социальной сети как способ изучения личности допрашиваемого // Российское правоведение: трибуна молодого ученого: сб. статей. - Томск, 2015. - С. 215-216.

КРИМИНАЛИСТИЧЕСКАЯ КЛАССИФИКАЦИЯ ХИЩЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»

Е.А. Ануфриева, к.ю.н., доцент кафедры уголовного права и процесса Новосибирского государственного технического университета,
Н.А. Шаталкина, следователь СО МО МВД России «Заринский»

Внедрение компьютеризации и информатизации во все сферы общественной жизни и экономической деятельности привело к тому, что покупки различных товаров, оплата счетов и прочие бытовые операции все чаще люди производят с использованием своего домашнего компьютера или смартфона. Данным обстоятельством не могли не воспользоваться преступники. В связи с чем страну захлестнула волна хищений денежных средств с использованием сети Интернет.

Раскрытие и расследование данных преступлений представляет не мало трудностей для правоохранительных органов, что, в первую очередь, связано со специфическим механизмом образования следов при совершении хищений с использованием сети Интернет. Нередко правоохранительным органам либо вовсе не удается установить лиц, совершивших такие преступления, либо не удается доказать их виновность в совершении таких преступлений. Как представляется, обозначенные проблемы связаны с недостаточной разработанностью методико-криминалистического обеспечения расследования хищений, совершенных в сети Интернет. К настоящему моменту уже проведены отдельные исследования, направленные на создание криминалистических методик расследования таких преступлений [1, 3]. Вместе с тем, с учетом постоянно меняющихся способов совершения и сокрытия хищений, совершаемых с использованием сети Интернет, полагаем целесообразным поведение дальнейших исследований и формирование криминалистической методики расследования хищений, совершенных в сети Интернет.

Важнейшее значение при формировании криминалистической методики расследования таких преступлений отводится их криминалистической классификации. Как справедливо отметил А.Ю. Головин: «Классификационный метод является одним из важнейших средств криминалистического изучения преступной

деятельности. Именно в результате таких классификационных исследований формируется наиболее полная и разветвленная система криминалистических понятий и терминов, характеризующих преступление как объект криминалистического познания, создается база для последующих научных исследований преступлений отдельных видов, представления их результатов с использованием единой, системной, понятийно-терминологической основы, разработки практических рекомендаций по их расследованию» [2, С. 33].

Основаниями для криминалистической классификации преступлений наиболее часто являются обобщенные сведения об отдельных элементах криминалистической характеристики преступлений. Как представляется применительно к хищениям, совершаемым в сети Интернет, наиболее интересной является криминалистическая классификация в зависимости от способа их совершения. Так, исходя из данного критерия исследуемые преступления можно классифицировать по следующим основаниям:

1. Совершение хищений с использованием сети Интернет посредством обмана:

1.1. Потерпевший, находясь под воздействием обмана, сам добровольно перечисляет денежные средства преступнику:

а) создание сайтов (в том числе сайтов-двойников), групп и аккаунтов в социальных сетях (Одноклассники, Вконтакте), через которые якобы осуществляется:

- продажа товаров (одежда, оргтехника, БАДы, авиабилеты и пр.);

- оказание услуг (риелторы, целители и пр.).

б) поиск потенциальных жертв на популярных сайтах объявлений (Авито, Дром и пр.):

- предложения приобрести или продать товары, получить услуги лицам, разместившим объявления;

- самостоятельное размещение объявлений о продаже товаров или предоставлении услуг.

в) знакомство с потерпевшими на сайтах знакомств, в социальных сетях (Одноклассники, Вконтакте и пр.) с целью последующего завладения денежными средствами обманным путем:

- оплата за «доставку» подарка от поклонника;

- передача поклоннику, попавшему во временную трудную финансовую ситуацию, денежных средств в долг.

г) создание благотворительных сайтов, размещение в социальных сетях объявлений о сборе денег для помощи:

- людям, страдающим смертельными или другими серьезными заболеваниями (часто детям);
- бездомным животным;
- редким и исчезающим видам животных.

1.2. Преступник путем обмана получает доступ к платежным реквизитам потерпевшего:

а) поиск потенциальных жертв на популярных сайтах объявлений (Авито, Дром и пр.), убедив человека, в своем намерении приобрести продаваемый товар, и пользуясь их незнанием особенностей осуществления безналичного перевода денежных средств:

- получают у потерпевшего пароли, поступившее ему в смс-сообщениях через приложение «Мобильный банк», для доступа в его личный кабинет на сервисе «Сбербанк Онлайн»;
- путем обмана просят пройти к банкомату, где потерпевший под руководством мошенников подключает к своей банковской карте услугу «Мобильный банк» к абонентскому номеру преступников.

б) отправка на электронную почту сообщений от лица банков, Пенсионного фонда РФ иных организаций с просьбой предоставить в ответ сведений о своих банковских счетах.

2. Преступник с использованием вредоносного программного обеспечения получает доступ к платежным реквизитам потерпевшего:

2.1. размещение вредоносных программ под видом привлекающих внимание заголовков статей;

2.2. размещение вредоносных программ под видом полезного программного обеспечения;

2.3. отправка на смартфоны смс-сообщений со ссылками на вредоносные программы в сети Интернет.

Подводя итог вышеизложенному следует отметить, что предложенная криминалистическая классификация хищений, совершенных в сети Интернет, безусловно, не является исчерпывающей и нуждается в дальнейшем уточнении и детализации.

Список использованных источников и литературы

1. Атаманов Р.С. Основы методики расследования мошенничества в сети Интернет: автореф. дис. ... канд. юрид. наук. М., 2012. 28 с.
2. Головин А. Ю. Базовые криминалистические классификации преступлений // Известия ТулГУ. Экономические и юридические науки. 2013. №2-2. С. 31-40.
3. Филиппов М.Н. Расследование краж и мошенничеств, совершенных с использованием банковских карт и их реквизитов. М.: Юрлитинформ, 2014. 160 с.

К ВОПРОСУ ОБ КИБЕРГИГИЕНЕ И КИБЕР - ПРОФИЛАКТИКЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЧЕЛОВЕКА ОБЩЕСТВА И ГОСУДАРСТВА В СФЕРЕ ИНФОРМАТИЗАЦИИИ И СВЯЗИ КАЗАХСТАНА

В.И. Балко, преподаватель колледжа «Кайнар», г. Семей, Республика Казахстан
С.А. Сергеев, магистр юриспруденции, старший преподаватель кафедры уголовно-правовых дисциплин КазГЮИУ, г. Семей, Республика Казахстан

Человечество вступило в новую эпоху – эпоху информационного общества. Информатизация современного общества привела к формированию новых видов преступлений, при совершении которых используются вычислительные системы, новейшие средства телекоммуникации и связи, а в основе, которых лежат высокоточные (высокие) технологии. В РК за последние 10-15 лет резко увеличилось количество преступлений с использованием электронной аппаратуры, хищения наличных и безналичных денежных средств. Жертвами киберпреступников, орудующих в виртуальном пространстве, могут стать не только граждане РК, но и целые государства. При этом информационная безопасность (далее - ИБ) тысяч пользователей может оказаться в зависимости от нескольких преступников. За последние годы этот метод преступности стал более изощренным.

Киберпреступность на сегодняшний день является одной из наиболее серьезных угроз для национальной безопасности страны в информационной сфере. За истекший период текущего года по РК в сфере информатизации и связи увеличилось количество уголовных правонарушений. По информации Центра анализа и расследования кибератак (ЦАРКА) кибер атаки и подобные атаки на казахстанские сайты постоянно производятся. Основная причина уязвимости казахстанских сайтов – использование устаревшей версии системы управления сайтом (CMS). Поэтому аудиторы, расследующие киберпреступления, регулярно получают запросы из Казахстана [1].

В послании Президента страны народу Казахстана «Казахстан - 2030. Процветание, безопасность и улучшение благосостояния всех казахстанцев» в качестве долгосрочного приоритета определена национальная безопасность, одной из составляющих которой является ИБ [2]. В Послании Назарбаева народу Казахстана «озвучена

необходимость повышать грамотность граждан страны в области информационных технологий, доносить информацию об угрозах и рисках до всех слоев населения, формировать... базовые навыки по защите от киберугроз и безопасному использованию информационных систем». Современное состояние информационной безопасности в Казахстане показывает, что ее уровень в настоящее время не соответствует потребностям человека, общества и государства. Нынешние условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных ограничений на ее распространение. Особенно, если сотни радикально настроенных казахстанцев сражаются на стороне боевиков в Сирии и Ираке. С учетом суперновейших технологий зомбирования и программирования сознания транслируют сайты, специально созданные террористами». Поэтому президент Казахстана Назарбаев в своем ежегодном Послании народу Казахстана, опубликованному 31 января 2017г., поручил Правительству и Комитету национальной безопасности [КНБ] принять меры по созданию системы “Киберщит Казахстана”».

Тенденция развития информационных технологий улучшает качество жизни и экономию времени, но в то же время подвергает опасности общество и государство. Основные инструменты и инфраструктура киберпреступности включают в себя вредоносные программы, бот-сети, незаконное использование доменов, теневую экономику, предоставляющую товары и услуги. Социальные сети и облачные компьютерные услуги создают новые основы для киберпреступности и новые проблемы для правоохранительных органов. Мошенничество — это то киберпреступление, о котором в практике отдельных государств сообщается наиболее часто.

По словам экспертов, жертвами киберпреступников могут стать как один человек, так и группа лиц, к которым относятся учреждения, предприятия и организации, использующие автоматизированные компьютерные системы для обработки бухгалтерских документов, проведения платежей и других операций. Так, по данным МВД РК, наибольшее количество правонарушений было совершено в отношении таких компаний, как Microsoft, «1С», «Меломан», «Азия хит», но были и случаи причинения ущерба другим предприятиям и учреждениям, в том числе государственным. Пострадали от рук хакеров и некоторые банки и компании сотовой связи. Это одно из

подтверждений того, что интересы киберпреступников очень сильно изменились. Сегодня их целью ставятся уже не физические лица, а банки и компании. Поэтому киберпреступность угрожает не только отдельным лицам или организациям, в первую очередь финансовым организациям, в частности, банки, но потенциально - национальной безопасности любой страны, достигшей значительного уровня компьютеризации жизненно важных отраслей экономики. Специалисты отмечают, что жертвы с целью сохранения личного имиджа или имиджа компании, пытаются справиться с возникшей проблемой самостоятельно. Практика показывает, что правоохранительным органам становится известно не более чем о 5–10% совершенных компьютерных преступлений. Во многих случаях нарушения конфиденциальности, причинения морального и материального ущерба и в случаях обнаружения взлома вашей информационной базы необходимо сразу же обратиться в органы внутренних дел с заявлением. По словам специалистов, чаще всего «молчат» крупные бизнесмены и банкиры.

Сегодня, отмечают эксперты, ни один операционный процесс в бизнесе не существует без IT, соответственно, и рисков становится больше, а их масштаб сегодня более серьезный, чем несколько лет назад. Облачные технологии и мобильность создают новые угрозы кибербезопасности, как и теневой IT, то есть все то, что происходит за спиной компетентных служб. В качестве одного из самых ярких примеров слияния бизнеса и ИБ эксперты приводят финансовый сектор, в котором IT-решения все больше становятся факторами влияния. Банки стали цифровыми организациями, и скорость, с которой выдвигаются новые продукты, а также риски, связанные с динамичным выпуском продуктов, заставляют уделять повышенное внимание вопросам информационной безопасности.

Киберпреступность сегодня по объемам занимает лидирующие позиции среди всех типов банковского мошенничества. Существуют организации, которые этим занимаются, некоторые из них работают при участии Интерпола. Эти компании помогают выявлять фродстеров в России и СНГ. «Фрод» как вид мошенничества в области информационных технологий почти безграничен. Наиболее популярные схемы кибермошенничества в СНГ - это деньги, которые выводятся со счетов юридических лиц через систему банковского обслуживания, используя удаленное подключение или конкурентной

разведки или с помощью социальной инженерии (*метод управления действиями человека без использования технических*).

Второй вид мошенничества достаточно старый – это автозалив (вредоносная программа). В момент, когда совершается платеж со счета юридического лица, происходит подмена реквизитов и деньги уходят в пользу злоумышленника. По количеству все-таки лидируют кражи средств со счетов мобильных устройств на базе Android. Объем каждой мошеннической операции несравнимо мал с тем, что можно украсть через интернет-банкинг юридического лица. Но, с другой стороны, мошенники автоматизировали свое программное обеспечение и все происходит без непосредственного участия самого человека. Они лишь в конце дня «снимают сливки». При этом количество вредоносного обеспечения на Android поражает – от перехватывания СМС до формирования платежей. Все понимают, что за мобильными платформами будущее, и злоумышленники тоже, поэтому они весьма активно развиваются в данном направлении. «Фрод» стал более технологичным, организованным и более динамичным. Опять же, если раньше работали одиночки, то со временем стали создаваться преступные группировки. Между ними существует хорошо разделенный функционал – одни занимаются написанием кодов, другие подбором людей, через счета которых будут выводиться украденные средства, третьи занимаются фишингом и воруют, например, данные карт и т.д. Они могут друг друга не знать, а лишь отвечать за свою часть.

Во многих странах мира в целях пресечения факта информационного преступления в последние годы специалисты по компьютерной безопасности начали сотрудничество с психологами, которые составляют профиль так называемого хакера, фрикера и крэкера. Действия представителей всех трех групп уголовно наказуемы. Но хакеры помимо негативных последствий несут и некий позитив: если есть люди, которые могут взломать систему, то значит, будут нужны и люди, которые смогут ее защитить. Следует отметить, что хотя компьютерные специалисты и могут многое сказать о хакере и о методах его работы, но они никогда не смогут понять психологию его криминального мышления. Подобными вопросами занимаются клинические психологи, судебные эксперты и другие специалисты совместно с органами внутренних дел. Подобная практика активно используется в США, Европе и других странах, где киберпреступления широко развиваются. Некоторые ученые считают, что налаживание

подобной практики и в нашей стране, где преступления в сфере информационных технологий пока неразвиты, позволит еще в зачаточной форме уничтожить основы киберпреступности. Для этого необходимо активизировать потребность международного сотрудничества.

Опубликована концепция кибербезопасности Казахстана "Киберщит Казахстана", на которую запланировали выделить7,4 млрд тенге и которая разработана в целях обеспечения ИБ общества и государства в сфере информатизации и связи, а также защиты неприкосновенности частной жизни граждан при использовании ими информационно-коммуникационных технологий. В концепции предлагается определить уполномоченный орган по обеспечению информационной безопасности и его компетенцию, обособить сферу государственного контроля в сфере ИБ в самостоятельную область с выведением из-под регулирования Предпринимательского кодекса в отношении государственных объектов и критически важных объектов информационно-коммуникационной инфраструктуры. При уполномоченном органе по информационной безопасности, по мнению авторов, должен быть образован Совет по кибербезопасности, главной задачей которого должно стать поддержание в актуальном состоянии руководящих документов, нормативно-правовой базы, содействие приоритетному использованию продукции отечественной электронной и софтверной промышленности, проведение публичной оценки общественно значимых IT-проектов. Кроме того, для борьбы с киберпреступностью предлагается усилить личный состав специализированных подразделений, расширить арсенал технических средств фиксации и криминалистических исследований "цифровых" доказательств. Авторы концепции считают, что для объединения усилий необходимо при участии научного сообщества, частного сектора создать координационный Национальный оперативный центр информационной безопасности, который в онлайн-режиме будет обрабатывать информацию о состоянии защищенности наиболее важных компонентов национальной информационной инфраструктуры и обеспечит обмен информацией, что позволит: Совету Безопасности Республики Казахстан оценивать ситуацию и вырабатывать решения в условиях чрезвычайных ситуаций техногенного и социального характеров. Особых методов для борьбы с компьютерными преступлениями не выделяют ни криминалисты, ни ученые-юристы, ни практики, ни IT-специалисты, используются те же методы и

средства, что во всем мире. В мировой практике применяются в совокупности технические, правовые, организационные и превентивно - профилактические методы. К техническим методам можно отнести все те приемы, где для выявления незаконного проникновения в компьютерную сеть используется специальное оборудование. К организационным - мероприятия, которые направлены на повышение эффективности раскрытия киберпреступлений, в том числе совместные оперативно-розыскные мероприятия, направленные на выявление продукции и информации, запрещенной в свободном обороте, пропагандирующие экстремизм, терроризм, культ жестокости и насилия и детскую порнография. К правовым методам относятся разработка и совершенствования норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, принятие международных договоров в данной сфере. К привентивно - профилактическим методам относятся различные «объемы» кибергигиены и кибер профилактики в связи с текущим научно-техническим прогрессом и человеческим фактором. В статье рассмотрим превентивно - профилактические методы. Поэтому дадим определения понятиям «кибергигиена» и «кибер - профилактика».

Кибергигиена и кибер профилактика в узком смысле значения - это действия техническими, правовыми, организационными и превентивно - профилактическими методами, направленными на повышение информационной безопасности личности, общества и государства. Кибергигиена и кибер профилактика в широком смысле значения - это действия техническими, правовыми, организационными и превентивно - профилактическими методами, направленными на повышение информационной безопасности всех стран мира.

Рассмотрим пять уровней кибергигиены и кибер профилактики. Кибергигиена 1 уровня для физических лиц и к ним приравненных; кибергигиена и кибер - профилактика 2 уровня для юридических лиц малого и среднего бизнеса и к ним приравненных; кибергигиена и кибер - профилактика 3 уровня для юридических лиц большого бизнеса и к ним приравненных; кибергигиена и кибер - профилактика 4 уровня для юридических лиц тактического и государственного значения и к ним приравненных; кибергигиена и кибер - профилактика 5 уровня для юридических лиц стратегического и межгосударственного значения и к ним приравненных.

Рассмотрим некоторые действия, решения, которые положительно влияют на кибергигиену и кибер профилактику при их соблюдении на тот или иной уровень кибергигиены и кибер - профилактики (например, 1,2,3,4,5 уровень или 1-5). Для того, чтобы не стать жертвами киберпреступников, рекомендуется соблюдать следующие правила:

- духовность (1,2 -5);
- общий свод требований к информационной безопасности (1,2 - 5);
- не распространяйте Ваши паспортные данные, реквизиты банковские карты, данные для входа в Интернет-банк (логин и пароль), не используйте один пароль для всех интернет-ресурсов (1,2 - 5);
- при поступлении на мобильный телефон, компьютер сообщения о внезапном выигрыше, блокировке банковской карты в первую очередь свяжитесь с оператором связи, для прояснения ситуации (1,2 -5);
- не доверяйте объявлениям, поступившим на вашу электронную почту, обещающим решить все проблемы за незначительный период времени, в особенности, если изначально это требует вложения денежных средств (1,2 -5);
- тщательно перепроверяйте поступившую информацию на вашу почту о просящих вас оказать благотворительную помощь (1,2 - 5);
- при поступлении на мобильный телефон, компьютер сообщения о блокировке банковской карты в первую очередь свяжитесь с банком (1,2 -5);
- выбирать и поддерживать высокое качество пароля (1,2 -5);
- устанавливать и поддерживать безопасность программного обеспечения на цифровые устройства(1,2 -5);
- придерживаться политики ИБ (1,2 -5);
- запускать регулярные сканирования безопасности своих цифровых устройств. т.е. проводить постоянный контроль и мониторинг информационной системы (1,2 -5);
- избегать потенциальных источников заражения (1,2 -5);
- проводить тренинги в игровой форме и обучающие практики по защите персональных данных среди несовершеннолетних пользователей интернета и их родителей" (1,2 -5);

- использовать специализированные программные обеспечения для защиты информации, такие, как антивирусные программы, криптографические программы (1,2 -5);

- максимальная открытость информации для населения сайта Нац банка РК (1,2 -5);

- регистрация атак на компьютерные данные и системы (2 -5);

- предпринять процессуальные законодательные меры для того, чтобы компетентные органы смогли проводить расследование киберпреступлений и сохранить легко изменяемые электронные доказательства наиболее эффективно, включая оперативное обеспечение сохранности данных, обыск и выемку хранимых компьютерных данных, перехват данных и т.д. (2 -5);

- эффективное всемирное международное сотрудничество с учетом специальных процессуальных мер (2 -5);

- оперативный штаб по реагированию и координированию с профилирующей группой депутатов с активной позицией (2 -5);

- активное контактирование с МВД РК (1,2 -5);

- формирование ряда базовых правовых понятий киберпреступности (2 -5);

- использование современной версии системы управления сайтом (CMS) (2 -5);

- активная позиция в действиях регулятора с оптимальным давлением со стороны регулятора, чтобы у специалистов появилась возможность создавать собственные решения и сервисы (2 -5);

- повысить качество казахстанской модели высшего и послевузовского образования в области информационно-коммуникационных технологий, с распределением образовательных грантов в сфере информационной безопасности в системе подготовки специалистов в области ИКТ (2 -5);

- наличие экспертов в сфере информационной и сетевой безопасности (2 -5);

- охватывание гражданским и уголовным законодательством Казахстана полный спектр киберпреступлений (2 -5);

- накопление зарубежного и национального опыта противодействия мошенничеству (2 -5);

- Национальный банк может создавать центр по координации взаимодействия между банками для борьбы с финансовым мошенничеством (4 -5);

- разрабатывать уникальные методы борьбы с киберпреступностью, но также с кредитным, внутренним и другими видами мошенничества (4 -5);

- блокировка экстремистских материалов в Интернете, как важнейшая составляющая борьбы с терроризмом (4 -5);

- своевременно классифицировать и квалифицировать компьютерные атаки как акт вооруженного нападения (4 -5);

- государственным органам поддерживать высокий уровень отказоустойчивости и предупреждения возникновения технологических сбоев, а также своевременное устранение их последствий в инфраструктуре, входящей в состав "электронного правительства" и других государственных информационных систем и ресурсов (4-5.

Анализ современного состояния ИБ в Казахстане показывает, что ее уровень в настоящее время не соответствует потребностям человека, общества и государства. Существует дефицит специалистов по специальности “Система информационной безопасности”. Сегодняшние условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных ограничений на ее распространение. Для обеспечения государственных органов полной, достоверной и своевременной информацией требуются принятие обоснованных решений, в том числе для защиты государственных информационных ресурсов, а также разработки современных средств защиты информации и системы подтверждения соответствия импортируемых технических средств установленным требованиям, а также дальнейшей проработки вопросов противодействия техническим разведкам, защиты от информационного оружия и совершенствования нормативной правовой базы в данной сфере. Необходима комплексная координация мер по защите информации на межгосударственном и государственном масштабе и на ведомственном уровне для обеспечения целостности и конфиденциальности информации так как основной угрозой и слабым звеном ИБ по-прежнему остается человек, из-за человеческого фактора происходит большинство инцидентов.

Киберпреступление может быть задумано в одной стране, написано (вредоносные программы) в другой стране, подготовлена атака в третьей стране, проход по коммуникациям двух - пяти иных

стран, и совершено в 6,7,8 или 9 стране. Это обрекает нас на налаживание всех уровней взаимодействия, где единственно правильный способ - объединение и информирование на межгосударственном, государственном и ведомственном уровнях о существующих угрозах. Кибер - устойчивым лицом является тот, кто имеет надежную политику ИБ и систему, члены которой имеют хорошую кибергигиену и кибер - профилактику, что способствует предупреждению и раскрытию преступлений в области защиты персональных данных в сфере IT в телекоммуникационных системах гражданского и военного назначения, тесно связано с противодействием терроризму, предупреждением чрезвычайных ситуаций и другими направлениями в обеспечении безопасности.

Список использованных источников и литературы

1. Артур Мискарян. Правительство оценило в бюджете систему кибербезопасности страны. URL: http://abctv.kz/ru/news/na-sozdanie-%C2%ABkibershita-kazahstana%C2%BB-zaplanirovali-7-4-mlr (Дата обращения: 1.10.2017).

2. Послание Нурсултана Назарбаева народу Казахстана от 31 января 2017 «Третья модернизация Казахстана: глобальная конкурентоспособность». URL: zakon.kz/4841750-opublikovano-poslanie-nursultana.html (Дата обращения: 1.10.2017).

3. Оксана Коксегенова. Хакеры угрожают Казахстану. Обзор ситуации вокруг киберпреступности в Казахстане. Курсивъ. URL: http://profit.kz/articles/160/Hakeri-ugrozhaut-Kazahstanu/ (Дата обращения: 1.10.2017).

4. Ольга Фоминских. Украсть за 60 секунд. Популярные схемы киберворовства в СНГ. Интервью «Капитал.kz» Алексея Коняева, на конференции SAS Fraud and Risk Conference Kazakhstan.URL: https://kapital.kz/gosudarstvo/49264/ukrast-za-60-sekund.html (Дата обращения: 1.10.2017).

О ЗНАЧЕНИИ ЛИЧНОСТИ ПРЕСТУПНИКА, КАК ЭЛЕМЕНТА КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ПО ДЕЛАМ О ХИЩЕНИЯХ ДЕНЕЖНЫХ СРЕДСТВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ВРЕДОНОСНЫХ ПРОГРАММ

Г.Е. Брызгалов, майор полиции, адъюнкт Барнаульского юридического института МВД России

Изучение личности преступника, по уголовным делам о хищениях денежных средств, совершаемых с использованием вредоносных программ, с позиции криминалистики на практике представляет достаточно сложную задачу, решение которой, возлагается главным образом на должностное лицо, осуществляющее предварительное расследование либо же дознание.

При необходимости, помимо самостоятельной работы, следователь привлекает к установлению и изучению личности преступника сотрудников органов, осуществляющих оперативно-розыскную деятельность, специалистов и экспертов различного профиля, ставя перед ними конкретные задачи по его установлению и сбору информации о его местонахождении, связях, возможных соучастниках, технической оснащённости, уровню подготовленности и др.

С помощью указанных лиц он не только устанавливает и изучает личность преступника, но и использует полученную информацию для целей доказывания и (или) тактического применения. Таким образом, в следственной деятельности одновременно реализуются уголовно-правовой, уголовно-процессуальный и криминалистический аспекты изучения личности преступника.

В качестве положительного примера привлечения следователем к установлению и изучению личности преступника сотрудников органов, осуществляющих оперативно-розыскную деятельность можно привести осуществление предварительного расследования по уголовным делам о хищениях денежных средств, совершенных с использованием вредоносных программ в Алтайском крае.

В результате проведения сотрудниками отдела по раскрытию преступлений против собственности УУР ГУ МВД России по Алтайскому краю (далее - УУР ГУ) оперативно-розыскных мероприятий установлено, что жители города Санкт-Петербурга

осуществляют неправомерный доступ к мобильным абонентским устройствам жителей Алтайского края, функционирующим на базе операционной системы «Android». При этом доступ к указанным устройствам происходит при помощи вредоносного программного обеспечения, установленного под видом различных приложений. В результате чего вредоносная программа осуществляет блокировку СМС центра мобильного устройства и отправку СМС-сообщений на номер «900» мобильного приложения ОАО «Сбербанка России» с запросом о переводе денежных средств на абонентские номера сим-карт находящихся в пользовании преступников.

В момент совершения преступления фигуранты активно передвигались по территории Российской Федерации, осуществляли свою преступную деятельность на съёмных квартирах, не подпадая под подозрение местных сотрудников полиции, снимали похищенные денежные средства в других регионах, постоянно меняли средства связи и пользовались программами, имеющими защиту в виде шифрования, что значительно затрудняло проведение оперативно - розыскных мероприятий силами Алтайского края.

После проведения ОРМ «наведение справок» и сбора достаточной информации о деятельности преступной группы результаты оперативно-розыскной деятельности были представлены руководителю следственного органа (начальнику ГСУ ГУ МВД России по Алтайскому краю) для использования в доказывании по уголовным делам, находящимся в производстве следователей органов предварительного следствия Алтайского края [1].

Анализ практики расследования хищений денежных средств, совершаемых с использованием вредоносных программ, показал, что субъектами таких преступлений существенно различаются по уровню образования: от неоконченного среднего до наличия нескольких высших образований при этом характеризуются высоким уровнем интеллектуального развития.

Существуют несколько подходов к классификации личности компьютерных преступников по мотивам совершения преступлений, при этом к нашему способу совершения преступления подходят профессиональные компьютерные преступники с ярко выраженными корыстными целями. Данные преступники характеризуются многократностью совершения компьютерных преступлений корыстной направленности с обязательным использованием действий,

направленных на их сокрытие, и обладают в связи с этим устойчивыми преступными навыками.

В профессиональном плане преступники, особенно те, которые сами создают (разрабатывают) вредоносные программы и другие средства хищений, являются специалистами в области программирования, системного администрирования, автоматизированных систем, функционирующих в конкретных отраслях экономики (банковской, торговой и т.п.), а также владеют специальными навыками и умениями в сфере управления компьютерами и его составными компонентами.

Совершаемые действия преступниками, обладающими профессиональными навыками и жизненным опытом, носят осознанный корыстный характер, при этом, как правило, предпринимаются меры по противодействию раскрытию преступления и введению следствия в заблуждение. Практически все известные отечественные преступники в сфере компьютерной информации - представители мужского пола, однако имеются случаи, когда женщины являются промежуточными звеньями и исполнителями в преступных группах специализирующихся на хищениях денежных средств, совершаемых с использованием вредоносных программ [1].

Преступники-одиночки постепенно вытесняются, хорошо организованными и разветвленными преступными группами, объединяющими людей не только из разных регионов Российской Федерации, но и людей, находящихся за её пределами [2]. Данная тенденция предопределена тем, что большая часть хищений денежных средств, совершаемых с использованием вредоносных программ, представляет собой достаточно сложное явление, подготовка, совершение и сокрытие преступной деятельности данной разновидности требует участие людей с различными навыками, умениями, типовыми чертами характера и т.п. При этом каждый из этих людей может играть различную роль в совершении хищения и, следовательно, в разной мере может претендовать на место в преступной группе.

Существует значительное количество закрытых общему доступу сайтов, форумов, блогов и т.п., где концентрируются лица, склонные к совершению рассматриваемых и иных компьютерных преступлений, происходит обмен информацией и опытом, в том числе участники объединяются в группы, сплачиваются и разрабатывают новейшие изощренные способы и методы совершения преступлений с

использованием высоких технологий. Не видя друг друга, и зачастую не зная реальных имен сообщников либо пособников преступной деятельности, их местонахождения, круга знакомых и других данных, необходимых для их изобличения, преступники могут на протяжении длительного времени совершать такие преступления, при этом установление всех соучастников, в рамках осуществления предварительного расследования, путем проведения оперативно-розыскных мероприятий может занимать длительное время и требует нестандартности мышления и необходимую подготовку от сотрудников, включенных в состав следственно-оперативных групп для производства неотложных следственных и процессуальных действий по уголовным делам о хищениях денежных средств, совершаемых с использованием вредоносных программ.

Совершение хищений денежных средств, совершаемых с использованием вредоносных программ, объективно требуют более высокого уровня организованности, что предопределяет создание организованных групп, участники которых выполняют строго определенные преступные действия, направленные на получение единого результата. Так, например, преступное сообщество, совершающее хищение денежных средств с использованием вредоносных программ в системе дистанционного банковского обслуживания (Далее: ДБО), включает следующие подгруппы: лица, взаимодействующие с организатором и непосредственно вовлечённые в процесс хищений: заливщик, прозвонщик, руководитель обналичивания (дроповод); лица, взаимодействующие с руководителем обналичивания: поставщик юридических лиц, поставщик банковских карт, поставщик SIM-карт и дропов; лица, взаимодействующие с организатором, но не вовлеченные непосредственно в процесс хищений: программист, трафер, владелец/автор связки эксплойтов, криптор, поставщик доменов и серверов.

Кроме того, среди лиц, причастных к совершению хищений в системе ДБО, следует выделить так называемых «денежных мулов» или «финансовых агентов», которые предоставляют обнальщикам копии паспортов и иных документов, удостоверяющих личность, и (или) оформляют на себя документы (например, для регистрации или покупки фиктивных юридических лиц), в том числе банковские карты, с использованием которых осуществляются операции по обналичиванию похищенных денежных средств.

Необходимо еще раз отметить, что лица, участвующие в хищении денежных средств в системе ДБО, зачастую могут находиться не только в различных регионах Российской Федерации, но и за её пределами. Преступники получают необходимые данные и общаются с целью совершения хищений денежных средств в системе ДБО и иных компьютерных преступлений в глобальной сети Интернет.

Таким образом, данный вид преступной деятельности стал своего рода бизнесом, которому некоторые готовы посвятить всю жизнь. В связи с этим наблюдается расслоение злоумышленников на лиц, владеющих высочайшими познаниями в данной специфической области, которых можно отнести к категории «Elit», и лиц, получивших в свои руки готовый алгоритм, обеспечивающий выполнение определенного порядка действий, и не преминувших им воспользоваться, имеющих при этом весьма общее представление о процессах, происходящих в информационных системах. В связи с этим можно спрогнозировать рост преступных посягательств на сравнительно новые системы и сервисы, так как массовый пользователь не до конца осведомлен о принципиальной возможности такого посягательства, например, на его мобильное устройство.

Относительно психологических особенностей личности преступника, совершающего хищения с использованием вредоносных программ, можно заключить следующее: замкнутость, самоизоляция, стеснительность, скрытность и т.п. постепенно перестают быть их отличительной чертой. Четкое деление на «элиту» и любителей разовых выгод породило и два типа злоумышленников. Первые организованные, скрупулезные, педантичные, осторожные и не рискующие по пустякам. Вторые, напротив, не прочь прихвастнуть своими достижениями в определенном кругу (устраивая некоторое подобие соревнований), готовые обмениваться программными кодами и готовыми алгоритмами с себе подобными, соблюдая при этом не хитрые меры предосторожности, а то и без таковых вовсе [3].

Проведенный анализ статистических данных о динамике мошенничеств, совершенных с использованием информационных технологий, позволяет выделить основные тенденции борьбы с данными преступлениями:

- сокращение удельного веса законченных расследованием уголовных дел,

- увеличение удельного веса приостановленных уголовных дел (не установление лица, совершившего преступления) [4].

Таким образом, можно сделать вывод, что разностороннее изучение личности преступника позволит изменить тенденции борьбы с данными преступлениями.

В рамках данного исследования мы акцентировали внимание на криминалистических характеристиках личности преступников по уголовным делам о хищениях денежных средств, совершаемых с использованием вредоносных программ и их значении для раскрытия данного вида преступлений и всестороннего расследования уголовных дел специализирующимися следователями.

Список использованных источников и литературы

1. Уголовное дело № 360282 // Архив Октябрьского районного суда г. Барнаула, 2017.
2. Поляков, В.В. Характеристика личности киберпреступников / В.В. Поляков, Н.В. Людкова // Теоретические и практические проблемы организации раскрытия и расследования преступлений: сб. мат. Всерос. науч. практ. конф. 22 апреля 2016 г.; - Хабаровск: ДВЮИ МВД России. - С. 250-255.
3. Рогозин В.Ю. Изменения в криминалистических характеристиках преступников в сфере высоких технологий // Расследование преступлений: проблемы и пути их решения. 2015. №1. С. 56-58.
4. Шевко Н.Р., Зиннуров И.Ф. Тенденции борьбы с мошенничествами, совершенными с использованием информационных технологий // Ученые записки Казанского юридического института МВД России. 2016. Т. 1. №2 (2). С. 121-126.

НЕКОТОРЫЕ ПРАВОВЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Ю.М. Диденко, Алтайский государственный университет
А.А. Корчагин, к.ю.н., доцент, доцент кафедры уголовного процесса и криминалистики Алтайского государственного университета

Сегодня, в эпоху информационного общества, немыслимо отрицание того, что компьютерные технологии и телекоммуникационные системы пронизывают все сферы жизнедеятельности отдельно взятого человека и государства в целом. Процессы информатизации общества неминуемо приводят к фундаментальным изменениям в нем, появлению так называемого «сетевого поколения», поколения людей, неотъемлемой частью профессиональной, общественной, личной жизни которых является цифровое пространство.

В контексте совершенствования глобальных информационных технологий, формирования единого мирового информационного пространства особую значимость приобретают вопросы безопасности пользователей. Жертвами преступников, орудующих в виртуальном пространстве, пространстве, призванном упростить жизнь человека, ускорить ее темп посредством развития систем мгновенной передачи информации, становятся не только люди, но и целые государства. Количество преступлений в кибер-пространстве год от года растет пропорционально числу пользователей компьютерных сетей. В качестве примера рассмотрим динамику роста киберпреступности в банковской сфере. Так, в 2008 г. 98% преступлений, связанных с мошенничеством, составляли воровство и грабежи наличных денег, лишь только 2% приходилось на кибермошенничество, сейчас ровным счетом наоборот: 98% составляют киберпреступления и только 2% приходится на все остальное. Кроме того, пишет В. Ференец, данная тенденция каждый год лишь усиливается. К примеру, в 2015 г. Банк России зафиксировал около 32 тыс. попыток воровства денег у клиентов российских банков через электронные каналы, что по сравнению с 2014 г. обнаруживает рост в 12 раз [1, с. 98]. Анализ практики противодействия киберпреступности в России и за рубежом, возросшая степень общественной опасности, по справедливому утверждению В.А. Мазурова, выдвигает задачу оптимизации мер по

совершенствованию законодательного обеспечения противодействия существующим и прогнозируемым угрозам в этой сфере [2, с. 41].

Потребность в противостоянии киберпреступности очевидна, однако стремление изменить ныне существующее положение вещей наталкивается на определенные сложности, вызванные, прежде всего, отсутствием единообразного законодательного регулирования общественных отношений, связанных с использованием информационных ресурсов сети Интернет, как на национальном, так на международном уровне. Сегодня отечественные правоохранительные органы не в полной мере оказались готовы к эффективному противодействию новым видам преступных посягательств - киберпреступлениям.

Итак, для осуществления эффективной борьбы с киберпреступностью необходимо соответствующее правовое обеспечение, т.к. для установления того или иного состава преступления необходимо, чтобы в уголовном законодательстве была предусмотрена ответственность за соответствующее деяние. В российском уголовном законодательстве разделение киберпреступлений на определенные группы отражено в ряде глав Уголовного кодекса Российской Федерации (далее – УК РФ), в первую очередь, в главе 28 УК РФ – «Преступления в сфере компьютерной информации» (статьи 272 – 274 УК РФ) [3]. По этому поводу А.И. Халиуллин пишет, что спектр компьютерных преступлений может быть рассмотрен в узком и широком смысле [4, с. 35 - 36]. В узком смысле он ограничен главой 28 УК РФ. Для статей, входящих в эту главу, общими являются последствия совершения преступлений в форме негативного воздействия на целостность компьютерной информации, определение которой дано в примечании к ст. 272 УК РФ. В широком же смысле к компьютерным преступлениям справедливо относить те, в которых присутствует один из ключевых элементов. Во-первых, это компьютерная техника, которая выступает по мнению некоторых ученых, способом совершения преступления [5, с. 40]. Во-вторых, так называемые информационные преступления, объективная сторона которых заключается или в распространении запрещенной либо заведомо ложной информации, или в непредоставлении сведений [6, с. 13]. В-третьих, местом либо способом совершения преступления является его совершение в информационно-телекоммуникационных сетях. Виртуальное пространство в данном случае характеризуется отсутствием

общепризнанных границ государств и их юрисдикций, формированием потенциально конфликтной среды с относительно низким уровнем безопасности оборота информации.

УК РФ не содержит указания, что необходимо понимать под «киберпреступлениями». Во многих источниках под этими преступлениями понимают: компьютерные преступления [7, с. 24], преступления в сфере высоких технологий [8, с. 18], преступления в сфере безопасности обращения компьютерной информации [9, с. 125] и т.д. Однако ни один отдельно взятый термин не отражает в полной мере исследуемое криминальное явление, отсюда использование термина «киберпреступление» является наиболее нейтральным и устойчивым к изменениям технологической среды обмена информацией. Т.Л. Тропина определяет киберпреступление как виновно совершенное общественно опасное уголовно наказуемое вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные деяния, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ, а также с помощью или посредством иных устройств доступа к моделируемому с помощью компьютера информационному пространству [10, с. 23]. Халиуллин А.И., подчеркивая стремительно изменяющийся перечень соответствующих преступлений, определение киберпреступлений ограничивает указанием на важнейший признак – одновременное наличие двух объектов посягательства – общественных отношений в сфере безопасного обращения компьютерной информации и общественных отношений в реальном мире (жизни, здоровья, собственности и т.д.), а также место криминальных манипуляций с компьютерной информацией [11, с. 39].

Одной из проблем расследования киберпреступлений является недостаточная компетентность лиц, занимающихся их выявлением и раскрытием. Специалистам, имеющим исключительно юридическое образование, зачастую недостает знаний в области компьютерных технологий. Так, Е.С. Шевченко в своем исследовании проводит опрос среди следователей (респондентами стали 170 следователей и 20 дознавателей, расследовавших киберпреступления), по результатам которого обнаруживается следующее: 95% респондентов имеют только юридическое образование, лишь 5% из числа опрошенных получили дополнительную подготовку, например, образование по

специальности «Информатика и вычислительная техника». 63% опрошенных оценивают уровень владения персональным компьютером как уровень «среднестатистического пользователя», 37% – «продвинутого пользователя». Источником получения знаний в области компьютерных технологий 79% опрошенных следователей назвали самообразование, 21% – курсы повышения квалификации сотрудников правоохранительных органов, 5% – коммерческие курсы или специальное образование [12, с. 29].

В условиях недостаточности дополнительных знаний следователей спасает опыт, который чаще всего приобретается нелегким путем. Для решения обозначенной проблемы желательным было бы проведение их обучения по расследованию рассматриваемого вида преступлений, а также организация семинаров, посвященных модификации компьютерных технологий.

Следующая проблема заключается в несвоевременности выявления киберпреступлений. Запоздалое начало предварительного расследования может привести к серьезным последствиям, например, безвозвратной утрате важных доказательств, увеличению сроков предварительного расследования и т.д. Зачастую несвоевременное выявление киберпреступлений влечет за собой опасность уничтожения следов совершенного преступления. При расследовании киберпреступлений чаще всего имеют место такие следственные действия, как осмотр места происшествия, допрос, обыск, выемка и назначение судебных экспертиз. Последнее из указанных действие представляет собой самостоятельную проблему: следователям приходится сталкиваться с загруженностью государственных судебно-экспертных учреждений, что имеет следствием несвоевременность выполнения экспертиз. Также определенные сложности вызывает постановка грамотных вопросов перед экспертом, который проводит компьютерно-техническую экспертизу, что может связано с отсутствием у следователей практики расследования данной категории дел, сложностью технических терминов и отсутствием специальных знаний в этой сфере. Решение этого аспекта проблемы может быть найдено в плоскости взаимодействия следователя при назначении экспертизы с экспертом или специалистом, которые могут проконсультировать назначающего экспертизу по всем вопросам научно-методического характера.

Серьезной преградой, стоящей на пути противодействия преступлениям, совершаемым в информационном пространстве,

является транснациональность или трансграничность таких преступлений. Ответственность за эти деяния предусмотрена законодательством различных государств, трансграничность преступных деяний ощутимо усложняет установление места совершения преступлений, затрудняет раскрытие, расследование и профилактику совершения таких преступлений. Существуют совершенно различные комбинации, когда преступления могут начаться на территории одного государства, а продолжаться и закончиться на территории других государств. Также последствия, наступившие на территории одного государства, могут отразиться на территориях, находящихся под юрисдикцией иных государств. Расстояния, необходимость физического присутствия в таких ситуациях не играет никакой роли. Ю.В. Гаврилин отмечает, что если преступление связано с неправомерным доступом к компьютерной информации и осуществляется одновременно с нескольких компьютеров, то количество мест совершения преступления соответствует числу используемых компьютеров [13, с. 111 - 115].

При расследовании этого вида преступных деяний существенным становится вопрос определения государства, правомочного проводить расследование. В рамках Содружества Независимых Государств для решения данного вопроса требуется обращение к ч. 1, 3 ст. 91 Конвенции СНГ о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам от 7 октября 2002 г. В соответствии с этим документом, государство, подписавшее вышеназванную Конвенцию, обязуется по поручению другого договорившегося государства осуществлять уголовное преследование против собственных граждан, подозреваемых, обвиняемых в совершении преступлений на территории запрашивающего государства, при условии, что деяние является уголовно наказуемым и в этом государстве. Также Конвенция предписывает, что для быстрого и всестороннего расследования преступлений, совершенных одним или несколькими лицами на территориях двух и более договаривающихся государств либо затрагивающих их интересы, могут создаваться совместные следственно-оперативные группы [14].

Кроме того, трансграничный характер компьютерных преступлений негативно отражается на раскрытии и расследовании данного вида преступных деяний не только на уровне межгосударственном уровне, но и на уровне межрегиональном, т.е.

внутри Российской Федерации. При установлении межрегионального характера совершенного преступления материалы проверки направляются по месту окончания преступления. Этот факт с неизбежностью приводит к затягиванию сроков проверки, а также утрате следов совершения преступления.

Резюмируя вышесказанное, отметим, что вопросы о месте совершения компьютерного преступления и применимом праве в отношении такого вида преступных деяний решаются индивидуально. Это и объясняет сложность международно-правового взаимодействия правоохранительных органов. В.Г. Степанов-Егиняц констатирует, что при совершении трансграничного преступления возбуждение и расследование уголовного дела может относиться к компетенции той страны, в которой преступник находился в момент совершения общественно опасного деяния. В случае наступления общественно опасных последствий в других странах вопрос о привлечении к уголовной ответственности должен решаться по соглашению государств с учетом соблюдения общепризнанного правового принципа non bis in idem (при буквальном прочтении означает «не дважды за то же») и в тесном сотрудничестве со страной, потерпевшей ущерб. С другой стороны, если лицо, совершившее преступление, неизвестно, но известно лицо потерпевшее, уголовное дело должно быть возбуждено на территории государства, в котором работает потерпевший. Согласимся с мнением В.Г. Степанова-Егиняца, что в случае, когда преступник находился в момент совершения им деяния в пределах территории России, то уголовное дело при наличии соответствующих оснований должно возбуждаться органом внутренних дел по месту обращения потерпевшего. После проведения необходимых следственных действий и установления места, где было совершено компьютерное преступление, все материалы уголовного дела могут передаваться в органы внутренних дел по месту совершения преступления [15].

Таким образом, следует признать, что раскрытие и расследование киберпреступлений являет собой сложную задачу для большинства сотрудников органов предварительного расследования. Отчасти такое положение дел обусловлено отсутствием системных обобщений материалов следственной и судебной практики, недостатком методических рекомендаций по организации расследования данного вида преступлений, недостаточно высоким уровнем подготовки следователей по соответствующей специализации

в высших учебных заведениях, а также нехваткой опыта работы сотрудников правоохранительных органов с рассматриваемой категорией дел. Однако, как бы то ни было, на сегодняшний день совершенствование противодействия киберпреступности располагает достаточными возможностями, коренящимися, прежде всего, в области повышения уровня мониторинга этого вида преступлений; разработки программ повышения квалификации следователей (дознавателей) по расследованию исследуемой категории дел; повышения технических возможностей экспертов, специальность которых ориентирована на область исследования компьютерных технологий; увеличения объема научно-методической литературы, посвященной прикладным аспектам расследования киберпреступлений и др. Вместе с тем, необходимо учесть, что даже самые передовые законотворческие шаги, предпринимаемые без проведения комплексного и всестороннего анализа отношений, складывающихся в сфере борьбы с киберпреступностью, адекватного подхода к определению путей их решения, не получает должной оценки практиками. Реальное создание правового механизма по противодействию киберпреступности будет обеспечено при корреляции количества статей уголовного закона с их качеством.

Список использованных источников и литературы

1. Ференец, В. «Бумажная» безопасность - это не про нас [Интервью с С. Лебедем] / В. Ференец // Банковское обозрение. – 2016. – № 9. – С. 96 - 99.
2. Мазуров, В.А. Кибертерроризм: понятие, проблемы противодействия /В.А. Мазуров // Доклады ТУСУРа. – 2010. – № 1 (21), ч. 1. – С. 41 - 45.
3. Уголовный кодекс Российской Федерации: федеральный закон от 13 июня 1996 № 63-ФЗ (ред. от 29.07.2017) // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954.
4. Халиуллин, А.И. Подходы к определению киберпреступления / А.И. Халиуллин // Российский следователь. – 2015. – № 1. – С. 34 - 39.
5. Селиванов, Н.А. Расследование особо опасных преступлений: Пособие для следователей /Н.А. Селиванов. – М.: Лига Разум, 1998. – 444 с.
6. Дворецкий, М.Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы

квалификации и наказания / М.Ю. Дворецкий. – Тамбов: Издательство Тамбовского государственного университета имени Г.Р. Державина, 2003. – С. 13 – С. 8 - 35.

7. Суслопаров, А.В. Компьютерные преступления как разновидность преступлений информационного характера. Автореф. дис. ... канд. юрид. наук / А.В. Суслопаров. – Владивосток, 2010. – 29 с.

8. Нарижный, А.В. Использование специальных познаний при выявлении и расследовании преступлений в сфере компьютерной информации и высоких технологий. Автореф. дис. ... канд. юрид. наук / А.В. Нарижный. – Краснодар, 2009. – 21 с.

9. Степанов-Егиянц, В.Г. Преступления в сфере безопасности обращения компьютерной информации: сравнительный анализ. Дис. … канд. юрид. наук / В.С. Степанов-Егиянц. – М., 2005. – 168 с.

10. Тропина, Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук / Т.Л. Тропина. – Владивосток, 2005. – 235 с.

11. Халиуллин, А.И. Подходы к определению киберпреступления / А.И. Халиуллин // Российский следователь. – 2015. – № 1. – С. 34 - 39.

12. Шевченко, Е.С. Актуальные проблемы расследования киберпреступлений / Е.С. Шевченко // Эксперт-криминалист. – 2015. – № 3. – С. 29 - 30.

13. Гаврилин, Ю.В. Расследование преступлений, посягающих на информационную безопасность в экономической сфере: теоретические, организационно-тактические и методические основы. Автореф. дис. ... д-ра юрид. наук / Ю.В. Гаврилин – М., 2009. – 404 с.

14. Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (Заключена в г. Минске 22 января 1993) // Собрание законодательства РФ. – 1995. – № 17. – Ст. 1472.

15. Степанов-Егиянц, В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации / В.Г. Степанов-Егиянц. – М.: Статут, 2016. – 190 с.

АКТУАЛЬНЫЕ ВОПРОСЫ ВЫЯВЛЕНИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ШИФРОВАНИЯ ДАННЫХ В СЕТИ ИНТЕРНЕТ

В.Х. Каримов, к.ю.н., доцент кафедры уголовного права и криминологии Алтайского государственного университета

Глобализация и интеграция информационных ресурсов в едином пространстве стала не просто реальностью, но и повседневностью в жизни общества, государства, да и простых граждан. Она затрагивает практически все сфере человеческой жизнедеятельности. Между тем информационные технологии таят в себе не только блага, но и представляют серьезную угрозу безопасности общества. Так, за последний десяток лет, незаметно для нас, преступность, применяя достижения научно-технического прогресса серьезно эволюционировала. Безусловно, и прежние «традиционные» общеуголовные деяния, совершаемые, зачастую в алкогольном или наркотическом опьянении, никуда не исчезли. Таких преступников разоблачить не сложно, методика расследования, научно-технические средства давно разработаны, и мы видим результативность раскрытия таких деяний. Но, следует отметить, появилась и совершенна иная, так называемая «беловоротничковая» преступность, образованная, использующая самые передовые достижения научно-технического прогресса. Выявление и расследование таких преступлений представляет серьезные трудности. Не нож, кастет или фомка находятся в руках современных преступников, а знания, информационные технические средства и технологии. Такая преступность опасней общеуголовной, поскольку влияет на нормальное развитие государства и общества, его безопасность, а негативные процессы, обуславливают общий рост преступности.

Государство, не только наше, но и практически всех стран мира, отстает в борьбе с обозначенными деяниями, как в техническом, так методическом и правых аспектах. Между тем, следует констатировать, что малейшее промедление в противодействии такой преступности еще более усугубит ситуацию. Особую тревогу представляет всеми востребованная глобальная всемирная сеть Интернет, которая стала огромным рынком распространения оружия, детской порнографии,

поддельных документов, денежных средств, баз персональной информации, различных технических приспособлений для доступа к банковской информации, торговли людьми и наркотиками и др. В последнее время, наблюдается тенденция и в угрозе национальной безопасности, взломы электронной почты и иных ресурсов первых лиц государства, получение доступа к материалам, представляющим совершенно секретную информацию, как в России, так и за рубежом – тому подтверждение.

Безусловно, многие страны пытаются противодействовать незаконной деятельности в сети Интернет, в частности, блокируя и запрещая нелегальный контент. Например, на начало мая 2017 года в реестре Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций России имелось свыше записей: запрещенных сайтов - 72285, в реестре блогеров: - 2149; в реестре организаторов распространения информации – 73 [1]. Между тем, такие блокировки и иные меры противодействия, по нашему мнению, не эффективны. Злоумышленникам достаточно подобрать новое доменное, иными словами назвать себя по-иному, и можно продолжать заниматься своей преступной деятельностью. В настоящее время рынок только зарегистрированных и продаваемых составляет, по некоторым оценкам свыше составляет 250 миллионов, он легален и никем не контролируем.

Для отслеживания опасных для общества информационных ресурсов совсем недавно был приняты поправки к законодательству, в частности Федеральный закон № 374-ФЗ от 6 июля 2016 г «О внесении изменений в отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» и др., согласно данному Закону операторы связи будут обязаны хранить звонки и сообщения абонентов за период, определяемый Правительством Российской Федерации (но не более, чем за 6 месяцев), а информацию о фактах приема, передачи, доставки и обработки сообщений и звонков — 3 года.

По нашему мнению, принятие подобного решения, при всей необходимости усиления борьбы с терроризмом не решит возложенных на него задач, несмотря на огромные материальные затраты на реализацию, поскольку коснется контента, по сути контроля над сообщениями, в первую очередь добропорядочных

граждан. Криминальный мир уже сейчас, перешел на мессенджеры зашифрованных сообщений, таких как Telegram, WhatsApp, распространяет информация в так называемом «Даркнете» (темном интернете), где сведения не только шифруются, но и скрываются IP-адреса реальных пользователей, что позволяет совершенно безнаказанно совершать преступные деяния. Таким образом, требуется комплекс правовых, технический и иных мер, направленных на предотвращение использования систем шифрования данных криминальным миром, раскрытия преступлений, совершаемых с их использованием.

Термин «Даркнет» появился еще в 70-х годах XX века и получил известность благодаря публикации статьи «The Darknet and the Future of Content Distribution». По мнению авторов данной статьи П. Биддла, П. Инглэнда, М. Пейнада и Б. Уиллмана, Даркнет это некая файлообменная сеть, которая возникает при появлении общедоступных данных, при распространении которых пользователи будут копировать объекты, если это возможно и если они этого захотят при этом они будут соединены каналами с высокой пропускной способностью [2]. Следует заметить, что «даркнет» это некое собирательное понятие, и он может быть основан на разных концепциях и технологиях. Наиболее известными являются системы Tor и I2P. Названные технологии используют многоуровневую криптографию, вследствие чего у заинтересованных структур, в том числе и правоохранительных, возникают сложности в расшифровке контента.

При общей концепции сокрытия персональной информации от других пользователей, имеются существенные отличия в рассматриваемых системах. Так, Tor скрывает информацию о пользователе во время передачи данных путем создания цепочки фактически несуществующих IP адресов (так называемая луковичная технология), при этом обмен информации осуществляется в обычном интернете, а в I2P создаются анонимные сети, которые включают лишь объединяющихся и подключившихся с помощью специального программного обеспечения пользователей, при этом, через специальные шлюзы они имеют анонимный выход на просторы обычного интернета.

Система Top (The Onion Router) является более известной и распространённой, в силу ее доступности и простоты. Она, фактически, представляет собой специфичный TOR Browser, который

легко установить на компьютер и можно начать использовать сразу же после установки, преодолев минимум настроек. Он, хоть и более медленный, но обладающий функцией поиска как по адресной строке, так и по ключевым словам, на просторах как обычного интернета, так в массивах, имеющих специфичное расширение, не видимое обычным браузерам. В нем информация шифруется уже на первом этапе, реализуются такие механизмы как многоступенчатое шифрование интернет-трафика – составляющие так называемой луковой маршрутизации затем предается по созданной цепочке, и скрывается также на последнем звене.

Данную систему активно используют преступники для анонимного доступ, к закрытым сегментам, где активно происходит торговля криминальным товаром – оружием, наркотиками, детской порнографией и др., там прячутся управляющие серверы, координирующие DDoS-атаки, различные хакерские форумы, где обсуждают способы получения данных банковских карт и прочее. Следует отметить, что информацию, проходящую через систему TOR все-таки возможно перехватить при входе и выходе из сети, через администраторов сети и провайдеров. Так, в начале апреля 2017 года в г. Москве был задержан администратор выходного узла сети Tor. гр-н Б., который, по мнению следствия, опубликовал в Интернете призывы не только к массовым беспорядкам, но и к террористической деятельности [3].

Конечно, установление администраторов выходного узла сети Tor недостаточно для успешного выявления преступных связей, поскольку они могут находиться и за рубежом, поэтому требуется проведение комплекса следственных действий и оперативно-розыскных мероприятий. Успешным примером такого раскрытия может быть дело Росса Ульбрихта, владельца ресурса «Силк роуд», на котором распостряналися криминальный товар. Он был задержан в 2013 году в США (Сан-Франциско). Следует заметить что, Росс Ульбрихт не был профессоналом конспирации и еще при запуске ресурса, рекламируя его как место проведения незаконных сделок, он предлагал направлять предложения на адрес rossulbricht@gmail.com, фактически расскрыв свои персональные данные., Он пользовался социальными сетями, Gmail, Youtube, LinkedIn и т. д., оставляя везде личные данные, а в сервер, используемый для администрирования Silk Road, заходил из интернет-кафе рядом с местом проживания. Благодаря анализу имеющейся информации ФБР вышла на

предполагаемого виновника, а проведя операцию, аналогичную ОРМ в нашей стране – оперативный эксперимент, окончательно изобличила виновника. Во время расследования этого дела американские правоохранительные органы изъяли из оборота около 174 тыс. биткоинов, эквивалентных примерно $40 млн по текущему курсу, которые использовались в денежных операциях на сайте Silk Road.

Аналогичные примеры есть и в других странах. Так, в 2006 году спецслужбы Германии осуществили захват шести компьютеров, работавших узлами сети Tor на основании того, что они были незаконно использованы для доступа к детской порнографии. В 2007 году немецкая полиция арестовала в Дюссельдорфе А. Янссена, организовавшего у себя на компьютере сервер Tor, через который неизвестный отправил ложное сообщение о теракте. В 2009 году в чёрный список Фаервола в КНР были включены 80 % IP-адресов публичных серверов Tor.

В России в конце 2016 года была задержана хакерская ОПГ, которая назвалась «Шалтай-Болтай». Судом было арестовано три человека. Данная группа по версии следствия несколько лет взламывала аккаунты высокопоставленных чиновников, крупных фирм и СМИ и в дальнейшем распространяла сведения, с использованием средств шифрования данных, в том числе продавала их

Проект I2P более узкоспециализирован и рассчитан на людей, обладающих базовыми сетевыми знаниями и, соответственно менее распространён, в виду необходимости обладания базовыми знаниями по установке и использованию специфичного программного обеспечения, и необходимости входа не просто так, находится в просторах информации доступной через поисковик, а быть с определенной целью в определенной тематической группе.

Соответственно, I2P представляет большую сложность для специализированных служб по выявлению реальных адресов. Он был запущен в еще начале 2000-х годов как технология анонимного общения и передачи информации, с отличительной особенностью более высокого уровня защиты децентрализованной анонимной сети. Данная система работает быстро и устойчива к внешним влияниям, даже под давлением организаций, обладающих значительными финансовыми или политическими ресурсами [4]. В ней нет привычных центральных и DNS-серверов, но используется хеш-таблица DHT (Distributed Hash Table), построенная на базе Kademlia, что позволяет

устранить серьезную точку отказа системы. В качестве примера можно привести историю, когда в 2007 году в Китае файрволом был перекрыт доступ к главной директории сервисов Tor. I2P в данном случае, не была заблокирована, поскольку опиралась на пиринговую технологию для обмена информацией о роутинге. Каждый участник сети является роутером, через который передается транзитный трафик, поэтому, в системе нет особого отличия между сервером и обычным клиентом.

Таким образом, в настоящее время, мы наблюдаем уход криминального мира из Интернета с открытым доступом в системы шифрования и сокрытия адресов, в так называемый «Даркнет». Бороться с ним можно в трех направления.

Во-первых, глобальной блокировкой TOP-серверов, запретом систем шифрования данных;

Во-вторых, поскольку при первом варианте, могут будут затронуты права и свободы граждан, то возможна точечная борьба с создателями, распространителями и администраторами криминальных ресурсов.

Сказанное возможно, как посредством комплекса оперативно-розыскных и технических мероприятий и дальнейшим проведением следственных действий. Например, установление администратора выходного узла сети Tor, а через него выход на иных участников. Кроме того, у Tor есть ряд уязвимостей, и в определенной ситуации они позволяют скомпрометировать пользователя. В частности, трафик идет в открытом виде, то есть он может быть перехвачен третьими лицами.

Не останавливаясь более подробно на технических аспектах в силу их специфичности, следует отметить, что ответственность создателей, распространителей и администраторов криминальных ресурсов не урегулирована нормами уголовного права. Конечно, можно привлечь за незаконное распространение запрещенных законом предметов, но, указанные выше лица, как правило, являются лишь некими посредниками, и такой обязательный элемент субъективной стороны как наличие умысла доказать проблематично. Например, создатель ресурса, безусловно понимая, что он создается в преступных целях, размещает строку, что запрещается выкладывать на него нелегальный контент.

Кроме того, меняется и система проведения криминальных сделок. Если ранее администраторов таких сайтов можно было привлекать как пособников, поскольку они содействовали в

осуществлении сделок между продавцами и покупателями следующим образом. Для нормального функционирования криминальной сети и предотвращения случаев возможного обмана, продавец договаривался с администрацией форума, сайта-площадки в сети Тор о продаже, например, оружия. Он выкладывал тему с описанием товара, ценой, фото, способами связи и публичным ключом для шифрования. Заинтересованные клиенты списывались с продавцом, и если договорились, то на сцене появляется еще один важный участник — «гарант», (он же с точки зрения уголовного права – пособник), который является посредником, гарантирующим, что никто никого не обманет. Покупатель переводил всю сумму в пересчете на биткоины (виртуальная валюта) гаранту, гарант говорил продавцу, что деньги у него, продавец делал закладку оружием и сообщал место покупателю. Если покупатель доволен товаром и не имеет претензий, он сообщает это гаранту, гарант переводит деньги продавцу за вычетом своей доли (3-7%) и доли сайта (3-5%). Но, теперь многие сайты вводят в строй систему автоматической торговли. Деньги за товар переводятся не гаранту, как было раньше, а сайту, где они замораживаются до тех пор, пока покупатель и продавец не подтвердят сделку.

Таким образом, возникает вопрос кого привлекать за посредничество? По нашему мнению, необходимо привлекать создателей и администратор таких ресурсов. Между тем, их деяния не охватываются главой 28 УК РФ (Преступления в сфере компьютерной информации), поскольку не предназначены для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации как указано в диспозиции статьи 273 УК РФ, не иными составами данной главы. Следует понимать, что характер и степень общественной опасности создания и распространения таких ресурсов велика. Налицо пробел в законодательстве.

По нашему мнению, следует главу 28 УК РФ дополнить статьей 273.1 УК РФ «Создание, администрирование и распространение информационных ресурсов в сети Интернет, предназначенных для размещения запрещенной законом информации». А для предотвращения таких преступлений предусмотреть специальные основания освобождения от уголовной ответственности; «Лицо, впервые совершившее преступление, предусмотренное статьей 273.1 УК РФ, освобождается от уголовной ответственности, если сообщило

в правоохранительные органы о факте преступления и активно способствовало его расследованию, либо своевременно прекратило функционирование информационного ресурса».

В заключении следует отметить, что, безусловно, одним изменением в законодательстве ситуацию изменить сложно, требуется комплексная государственная политика государства с выделением соответствующих материальных, технических и иных ресурсов.

Список использованных источников и литературы

1. Единый реестр запрещенной информации. Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. Официальный сайт // [Электронный ресурс]. URL: http://97-fz.rkn.gov.ru/organizer-dissemination/personalarea/

2. Biddle, Peter; England, Paul; Peinado, Marcus; Willman, Bryan. The Darknet and the Future of Content Distribution. [Электронный ресурс]. URL: http://msl1.mit.edu/ESD10/docs/darknet5.pdf

3. Установлен и задержан мужчина, подозреваемый в призывах к организации массовых беспорядков в центре Москвы // Официальный сайт Следственного комитета России. [Электронный ресурс]. URL: http://sledcom.ru/news/item/1114182/

4. Lars Schimmer. Peer Profiling and Selection in the I2P Anonymous Network. [Электронный ресурс]. URL: http://i2p-projekt.de/_static/pdf/I2P-PET-CON-2009.1.pdf.

ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННЫХ (ЦИФРОВЫХ) ДОКАЗАТЕЛЬСТВ В КРИМИНАЛИСТИКЕ

А.А. Корчагин, к.ю.н., доцент, доцент кафедры уголовного процесса и криминалистики Алтайского государственного университета

В последние годы в гражданском и уголовном праве увеличился электронный документооборот, на смену бумажным технологиям приходят так называемые «безбумажные», основанные на использовании средств электронно–вычислительной техники и электросвязи, одним из продуктов которых являются электронные документы. Они стали повсеместно и широко применяться во многих сферах деятельности. В вязи с этим достаточно активно обсуждаются варианты включения в УПК норм, регламентирующих такой вид доказательств, как «электронные доказательства», что позволит сформировать новый подход в работе судебной системы и судебно-экспертной деятельности, а также будут способствовать улучшению качества и сокращению сроков осуществления правосудия, что, безусловно, отразится на качестве и оперативности проводимых экспертными учреждениями судебных экспертиз и как результат обеспечит эффективное исполнение судебных решений.

Анализ юридической литературы, материалов следственной и судебной практики свидетельствует о том, что «электронные» доказательства стали все чаще использоваться по уголовным делам. Например, за последние 20 лет среди выявленных корыстных преступлений, характеризующихся повышенной общественной опасностью, широкое распространение получили посягательства, которые объединены одним общим криминалистическим признаком, а именно компьютерной информацией как предметом и (или) орудием их совершения [1, С.22-24].

Электронное доказательство понимается как объект, несущий информацию, имеющую смысловое значение, и существующий только в электронной среде. Значит, можно сказать, что электронные доказательства возникают из электронной среды, но не все они могут быть квалифицированы как документы. Есть электронные доказательства – документы (электронные), и есть электронные вещественные доказательства [2, С.16].

К электронным доказательствам в криминалистике можно так же отнести:

- электронную информацию;
- электронные сообщение и т.д.

Итак, предметность электронного доказательства относительна; вещественность вторична, информативность первична. А потому, во-первых, электронным доказательством необязательно должен быть документ (протокол), а во-вторых, само по себе вещество по своей сути не информативно, доказательством не является, пока не будет субъекта доказывания. А вот кем будет презюмироваться в законе этот субъект – следователем, который проводит всестороннее, полное, объективное предварительное расследование (доказывание), или офицером, уполномоченным на досудебный уголовный розыск (уголовное преследование), который осуществляет поиск обвинительных доказательств, – это принципиальный вопрос. В первом случае следователь формирует доказательство, во втором – это только обвинительный материал, из которого в суде, возможно, будет сформировано доказательство. Так же и в случае с электронной информацией: она становится доказательственной тогда, когда субъект доказывания интерпретирует ее в качестве таковой, делая объектом познания (доказывания изменения, произошедшие в информационной среде).

"Электронная" информация стала широко использоваться во всех областях человеческой жизни, в том числе и криминальной. Электронная информация используется (задействуется) в процессе доказывания с целью получения сведений, выраженных в знаковой (цифровой) форме. И если «вещественное доказательство является непосредственным носителем информации, необходимой для установления обстоятельств дела» [3, С.154], то компьютерная информация выступает средством фиксации сведений с помощью аппаратных и программных средств (заложенного в программе алгоритма). Доказательственное значение компьютерной информации определяется ее содержанием, а не физическими свойствами носителя данной информации [4, с. 166]. Не только преступления в сфере компьютерной информации (предусмотренные ст. 272-274 УК РФ) но и многие «традиционные» общественно опасные деяния оставляют после себя электронные следы в компьютерных сетях, на магнитных или оптических носителях, экранах мониторов. В связи с этим возникает практическая проблема использования данных следов в

процессе расследования и рассмотрения уголовного дела. В юридической литературе указанная проблема не получила широкого освещения. Ее решение не просто найти и в действующем законодательстве. Так, не каждый следователь ответит на вопрос о том, какое доказательственной значение может иметь размещенное чеченскими террористами в интернете объявление – заказ на убийство В. В. Путина, получившее широкий резонанс в средствах массовой информации [5, С.18-19].

Прежде всего, для уголовно-процессуального использования электронная информация должна получить свое закрепление на каком-либо носителе. Электронная информация может найти свое отражение в фотоснимке, видеозаписи (с экрана компьютера), памяти человека – очевидца. Разумеется, электронные данные могут быть записаны на магнитный носитель или распечатаны на бумаге. Все это может иметь место в виде непроцессуальной (предпроцессуальной) фиксации. В то же время электронная информация может быть сразу зафиксирована в уголовно-процессуальном порядке – в протоколе следственного действия. Электронная информация может быть вещественным доказательством. Безличный, бессубъектный характер позволяет отнести определенную разновидность электронной информации к категории вещественных доказательств. В отличие от обычного вещественного доказательства, каковым выступает предмет, а его доказательственное значение определяется физическими свойствами или местоположением, электронное вещественное доказательство – это след, оставленный преступлением в информационной среде, т.е. это информация. Электронная информация может быть относимой к делу точно так, как и любые другие не процессуальные данные. Следовательно, она свободно может использоваться в качестве ориентирующей, тактической информации. Однако для того, чтобы служить доказательством по уголовному делу, фактические данные должны обрести еще и свойство допустимости. Они должны быть получены 1) надлежащим субъектом доказывания, 2) надлежащим способом собирания доказательств и 3) из надлежащего источника доказательств.

Электронная информация может быть в вещественных доказательствах и иных документах, а так же в памяти человека, ее наблюдавшего. В этом случае возможен его допрос в качестве свидетеля. Тогда электронная информация предстанет в уголовном деле уже в виде показаний. Таким образом, электронная информация

может иметь доказательственное значение в виде следующих доказательств: протоколов следственных действий, иных документов, вещественных доказательств и показаний.

Ученые еще со времен появления вычислительных средств в своих работах отражали проблемы с использованием электронных документов в качестве доказательств. Одно из ранних упоминаний об электронных документах как источнике доказательств по уголовному процессу можно найти в докторской диссертации В. К. Лисиченко, выдающегося ученого-криминалиста. В своей работе «Криминалистическое исследование документов» автор приходит к выводу, что повсеместное внедрение вычислительной техники «создает объективные основания для того, чтобы сведения о фактах и практической деятельности людей, закрепленные знаками искусственных языковых систем (машинных языков), рассматривались в общенаучном и правовом смысле как самостоятельная разновидность документов». В практической деятельности использование этого типа доказательств проблематично.

Согласно ст. 88 УПК РФ, электронные доказательства в уголовном процессе обязаны быть в соответствии с требованиями достоверности (подтверждать реальные факты), допустимости (иметь форму, отвечающую требованиям закона), относимости (должна существовать логическая связь между доказательствами, сведениями и обстоятельствами преступления).

Относимость электронного документа говорит о том, что он входит в тот круг доказательств, которые могут иметь значение для установления обстоятельств, входящих в предмет доказывания по конкретному делу. Подобные материалы будут относимы в случае, если электронный документ содержит в себе информацию, имеющую значение для дела. Правила допустимости доказательств должны обеспечить достоверность средств доказывания и тем самым создать надежный фундамент для признания доказанными или недоказанными определенных обстоятельств. Обязательное требование к доказательствам – то, чтобы они были собраны в соответствии с требованиями закона – надлежащим субъектом, в надлежащем порядке и из надлежащих источников.

В уголовно-процессуальном кодексе отсутствует определение электронных документов как в качестве доказательств, так и в качестве вещественных доказательств, что не позволяет их

использовать в полноценном криминалистическом исследовании [2, С.17].

В конце 80-х начале 90-х годов XX века в связи со сменой поколений электронно-вычислительной техники, появлением персональных электронно-вычислительных машин (ПЭВМ) – персональных компьютеров и мобильных аппаратов цифровой электросвязи, произошло резкое увеличение числа договорных отношений, связанных с изготовлением, передачей и использованием программ для ЭВМ, баз данных и иных разновидностей электронных документов. Аналогично этому процессу возросло и количество преступных посягательств в сфере их оборота. Данные обстоятельства потребовали от законодателя принятия срочных мер по урегулированию общественных отношений в этой сфере и установлению норм правовой охраны электронных документов как объектов права собственности, что и было сделано в течение нескольких лет.

В настоящее время в п. 11.1, ч. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» указано: «…электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах» (п. 11.1 введен Федеральным законом от 27.07.2010 № 227-ФЗ).

С учетом требований к обязательным реквизитам документов, обеспечивающих их юридическое значение, все документы должны быть правильно оформлены, приняты (подписаны) уполномоченными лицами и учтены. Придание юридической силы электронному документу в электронном документообороте обеспечивает электронная подпись на основании Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

В ч. 1 ст. 2 Закона дается определение электронной подписи: это информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию; в ч. 11 ст. 2 уточняется, кто относится к участникам электронного взаимодействия; в ч. 1 ст. 6 информация в электронной форме, подписанная

квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе. На мой взгляд, можно говорить о возможности применения в качестве доказательства как непосредственно самого электронного документа, так и электронно-цифровой подписи. Здесь необходимо различать доказательственную силу электронно-цифровой подписи и доказательственную силу электронного документа. ЭЦП доказывает авторство и придаёт электронному документу свойство допустимости, в то время, как последний доказывает иные факты.

П. Зайцев определил электронный документ как источник судебного доказательства и предложил понимать под ним «сведения об обстоятельствах, подлежащих установлению по делу, записанные на перфокарту, перфоленту, магнитный, оптический, магнитооптический накопитель, карту флэш-памяти или иной подобный носитель, полученные с соблюдением процессуального порядка их собирания» [6, С.41].

Сфера действия Федерального закона – это регулирование правовых отношений при использовании электронной подписи в следующих случаях:

1) при совершении гражданско-правовых сделок;

2) при оказании государственных и муниципальных услуг;

3) при исполнении государственных и муниципальных функций;

4) при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами (в ред. Федерального закона от 05.04.2013 № 60-ФЗ).

Интересен научный взгляд П. С. Пастухова на вышеобозначенную проблематику. Автор в своей статье «К вопросу о создании процедуры использования «Электронных доказательств» в уголовном судопроизводстве» предлагает, исходя из зарубежного опыта правовой регламентации порядка использования электронной информации в уголовно-процессуальном доказывании, изменить технологию доказывания – освободить ее от следственной формы и ввести состязательный порядок. В качестве наиболее наглядного примера приводится письменный протокол следственного действия, от

которого следует отказаться. На смену протоколу должен прийти электронный документ в виде видеозаписи следственного действия или оперативно-розыскного мероприятия. По мнению автора, электронные документы могут быть признаны допустимыми в качестве доказательств в суде. При этом классификационный список электронных документов состоит из аудио- и видеозаписи в цифровом формате.

В информационном обществе информация рассматривается в качестве одного из важнейших ресурсов, аналогичных по значимости запасам энергии, ископаемым и др., который хотя всегда существовал, но не рассматривался ни как экономическая, ни как иная категория. Этому вопросу посвящено много публикаций, в которых отразились и разные мнения и определения, и разные научные школы, рассматривающие это понятие.

Нельзя не согласиться с мнением автора Т. Э. Кукарниковой по поводу того, что «электронные документы по содержанию и связи с преступлением, также как и обычные документы, могут быть подразделены на вещественные доказательства, документы и иные документы». Сегодня эта тема становится все актуальней, и не без основания.

Более конкретно относительно электронных документов, как разновидности электронных доказательств высказался И.Н. Подволоцкий: «Электронный документ, – пишет он, – это любые сведения, хранимые, обрабатываемые и передаваемые с помощью автоматизированных информационных и телекоммуникационных систем, на основе которых суд, прокурор, следователь, дознаватель в порядке, определенном уголовно-процессуальным законодательством, устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела, полученные с соблюдением процессуального порядка их собирания и приобщенные к уголовному делу специальным постановлением (определением)» [7, С.121].

Анализ части 2 статьи 74 УПК РФ и смежных с ней статей показывает, что электронные документы допускаются в качестве доказательств лишь как вещественные доказательства (ст. 81 УПК РФ) и иные документы (ст. 84 УПК РФ), при этом вопрос о «процессуализации» «электронных доказательств» должен решаться не через создание нового источника доказательств через смену

парадигмы доказательственного права: должна быть создана система уголовно-процессуальных доказательств состязательного уголовного судопроизводства [8,С.193].

Изначально обратимся к толковому словарю В. И. Даля, из которого следует, что под прилагательным «вещественный» понимается составленный или образованный из вещества, материальный, доступный чувствам нашим, т.е. не духовный. Имеющиеся в современной уголовно-процессуальной литературе определения вещественных доказательств не позволяют с точностью сказать о том, что авторы данных дефиниций в полной мере основываются на приведенном выше толковании слова «вещественный».

Вопрос об отграничении документов – вещественных доказательств от иных документов является самостоятельной научной проблемой. Для того чтобы электронный или бумажный документ признать вещественным доказательством, необходимо выполнение двух условий. Во-первых, зафиксированная в документе информация должна указывать на преступление как «главный факт» в предмете доказывания (а не на причины и условия, способствовавшие совершению преступления, характеристику личности обвиняемого, размер ущерба, подлежащего возмещению). Во-вторых, информация в документе – вещественном доказательстве должна быть объективной, то есть такой, которая напрямую отражает преступление. Другими словами, информация не должна быть следствием воспроизведения из памяти. Не должно быть промежуточного носителя информации в виде сознания человека. Например, заведомо ложное сообщение об акте терроризма, размещенное в интернете, будучи приобщенным к уголовному делу в виде распечатки, магнитного носителя, фотографии или видеозаписи, станет вещественным доказательством [2, с.14]. Однако в литературе встречается мнение, что электронный документ должен быть отнесен только к письменным доказательствам. Сторонники этого взгляда приводят в свою защиту следующее: как и вещественные доказательства, электронный документ имеет определенную материальную природу его носителя. Однако вещественные доказательства – это вещи, которые служат доказательством сами по себе, в силу определенных физических свойств, а не в силу запечатленной на них знаковой (буквенной) информации. Поэтому электронный документ является письменным, а не вещественным доказательством.

Однако, чаще всего электронную документацию прилагают к уголовному делу в категории иных документов, поскольку они выступают всего лишь отображением обычной жизнедеятельности конкретного человека, либо организации, и не были созданы в процессе расследования. Данные сведения собирают на досудебном производстве следователи, прокуроры или другие уполномоченные лица. Электронные документы могут послужить в качестве доказательств на всех этапах расследования: от обвинения в уголовном деле до обжалования вынесенного решения.

После сбора доказательств наступает самый сложный момент – их проверка. Сложность заключается в том, что обычно на жестких дисках и им подобных носителях информации количество файлов измеряется зачастую десятками тысяч, причем часть из них – системные файлы, часть – прикладные программы – их наличие предполагает их использование или изучение, но гораздо большую доказательственную силу имеют сами данные, полученные с помощью этих программ – из них можно определить, что было объектом работы конкретных программ. Также, данные могут быть спрятаны, зашифрованы или стерты (преднамеренно уничтожены). В связи с этим исследование собранных доказательств должно производиться соответствующим экспертом с последующей выдачей соответствующего заключения. Поэтому необходимо также использовать также данные оперативной разработки, полученные через телефонные компании, провайдеров Интернет и т. д., говорящие о том, что с данного компьютера осуществляется выход в сеть, и в частности, осуществляется доступ непосредственно к объекту преступления.

Программно-технической экспертизой (ПТЭ) решаются следующие задачи:

1) распечатка всей или части информации, содержащейся на жестких дисках компьютеров и на внешних магнитных носителях, в том числе из нетекстовых документов;

2) распечатка информации по определенным темам;

3) восстановление стертых файлов и стертых записей в базах данных, уточнение времени стирания и внесения изменений;

4) установление времени ввода в компьютер определенных файлов, записей в базы данных;

5) расшифровка закодированных файлов и другой информации, преодоление рубежей защиты, подбор паролей;

6) выяснение каналов утечки информации из ЛВС, глобальных сетей и распределенных баз данных;

7) установление авторства, места подготовки и способа изготовления некоторых документов;

8) выяснение технического состояния и исправности СКТ.

Наряду с этими основными задачами при проведении ПТЭ могут быть решены и некоторые вспомогательные задачи:

1) оценка стоимости компьютерной техники, периферийных устройств, магнитных носителей, программных продуктов, а также проверка контрактов на их поставку;

2) установление уровня профессиональной подготовки отдельных лиц в области программирования и работы с СКТ;

3) перевод документов технического содержания.

В заключение необходимо сказать, что интерес законодателя к проблеме электронных доказательств будет постоянно увеличиваться по мере масштабного внедрения электронного документооборота и количества используемых в нем электронных документов в повседневную жизнь государства и общества. Очевидно, что без фундаментальных научных исследований в этой предметной области деятельность судов и правоохранительных органов будет оставаться неэффективной.

Список использованных источников и литературы

1. Вехов В. Б. Работа с электронными доказательствами в условиях изменившегося уголовно-процессуального законодательства // Рос. следователь. – 2013. – № 10. – С. 22–26.

2. Кукарникова Т. Э. Электронный документ в уголовном процессе и криминалистике: автореф. дисс. к.ю.н. – Воронеж, 2003. – 24 с.

3. Зуев В.Л. Доказывание по делам о преступлениях с административной предъюдицией: Дис. … канд. юрид. наук. – М., 1991. –190 с.

4. Зигура Н.А. Компьютерная информация как вид доказательств в уголовном процессе России :дис… канд. юрид. наук. – Челябинск, 2010. – 234 с.

5. Калиновский К.Б., Маркелова Т.Ю. Доказательственное значение «электронной» информации в российском уголовном процессе // Российский следователь. – 2001. – № 6. –С. 16-19.

6. Зайцев П. Электронный документ как источник доказательств // Законность. – 2002. – № 4. – С. 40–44.

7. Подволоцкий И.Н. Правовые и криминалистические аспекты понятия «документ» // «Черные дыры» в российском законодательстве. – 2003. – № 2. – С. 123–125.

8. Пастухов П.С. «Электронные доказательства» в состязательной системе уголовно-процессуальных доказательств // ОБЩЕСТВО И ПРАВО. – 2015 № 1 (51). – С.194–196.

ОБЫСК КАК СРЕДСТВО ОТЫСКАНИЯ, ОБНАРУЖЕНИЯ И ИЗЪЯТИЯ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ И ИНФОРМАЦИИ НА НИХ (ПОДГОТОВИТЕЛЬНЫЙ ЭТАП)

А.А. Кузнецов, к.ю.н., профессор, профессор кафедры криминалистики Омской академии МВД России
С.В. Пропастин, к.ю.н., доцент, заместитель начальника кафедры криминалистики Омской академии МВД России
А.Б. Соколов, к.ю.н., доцент кафедры криминалистики Омской академии МВД России

В настоящее время удельный вес преступлений в сфере компьютерной информации (как правило, это совокупность составов преступлений, предусмотренных статьями 272, 273,274 УК РФ) продолжает оставаться на достаточно высоком уровне. Так, за период времени с января по декабрь 2014 г. органами внутренних дел зарегистрировано 1 739 преступлений в сфере компьютерной информации (из них раскрыто 1 321) в 2015 г. – 2 382 (1 213), в 2016 – 1 748 (903). За период с января по июль 2017 года органами внутренних дел зарегистрировано 1 356 преступлений в сфере компьютерной информации (из них раскрыто 720). Приведенные статистические данные указывают на наличие исследуемой группы преступлений, подчеркивая тем самым актуальность исследуемой тематики. Существует и определенное количество публикаций, в которых рассматриваются проблемные вопросы работы с компьютерной информацией и отдельными ее носителями применительно к расследованию отдельных видов и групп преступлений [2].

В настоящее время в ходе расследования преступлений в сфере компьютерной информации, производя отдельные следственные действия, следователь сталкивается с различного рода проблемами, связанными с отысканием, обнаружением и изъятием электронных носителей и информации на них. Среди прочих, обыск, является одним из эффективных средств получения доказательств – электронных носителей и информации на них. Тем не менее, результативность указанного следственного действия зачастую зависит от подготовки к его проведению, хотя и иные этапы проведения следственного действия не менее важны. Именно подготовка носит ярко выраженную специфику, знание которой позволит повысить качество и

результативность обыска, как средства отыскания, обнаружения и изъятия электронных носителей и информации на них.

Под обыском понимается проводимое следователем в установленном законом порядке самостоятельное следственное действие, направленное на отыскание, обнаружение и изъятие электронных носителей информации [1, с. 229-235; 3], могущих иметь значение для уголовного дела. Результаты проведенного нами выборочного исследования уголовных дел показали, что обыск как следственное действие, проводился по 82,8% [4], что подчеркивает значимость исследуемого средства поиска доказательств.

Деятельность следователя на подготовительном этапе обыска, направленного на отыскание, обнаружение и изъятие электронных носителей и информации на них, помимо общих [5], состоит из ряда специфических действий. К таким следует отнести:

1. **Формирование информационного образа искомого объекта.** Как было указано ранее, обыск является одним из средств отыскания, обнаружения и изъятия электронных носителей и информации на них. Поэтому для следователя важным является вопрос о признаках искомого объекта. От того, насколько четко следователю удастся сформировать в своем сознании информационный образ, зависит решение поставленной перед обыском задачи. При этом целесообразно уяснить степень детализации признаков искомого объекта, а также учитывать возможность маскировки соответствующих признаков под другой объект.

Результаты анализа уголовно-процессуального законодательства позволяют очертить степень детализации признаков. Так, ч. 1 ст. 182 УПК РФ закреплены словосочетания «в каком-либо месте», «у какого-либо лица», «орудия преступления, предметы и документы». Неопределенность одних и общий характер других дозволяют нам ограничить характеристику искомого объекта лишь общими признаками. Например, для проведения обыска будет достаточным знание того, что искомый объект – электронно-вычислительная машина, персональный компьютер, компьютерные программы и т.п.

В 2004 году неустановленное лицо получило несанкционированный доступ к охраняемой компьютерной учетной информации, принадлежащей организации: к индивидуальному логическому имени «guser20» и паролю, осуществив их копирование. После чего с использованием модема и персонального компьютера с

установленным на нем программным обеспечением подключилось по телефону к глобальной сети Интернет от имени легального пользователя. По данному факту было возбуждено уголовное дело. Следователь, установив номер телефона (и адрес его нахождения), с которого осуществлялось подключение, а также получив сведения от специалиста об обязательном применении для совершения преступления персонального компьютера, модема и программного обеспечения, принял решение о проведении обыска по месту нахождения номера телефона. Следователь вынес постановление, в котором ходатайствовал перед судом о производстве обыска в жилище. Здесь же в качестве искомых объектов следователь указал «персональный компьютер и гибкие магнитные диски с компьютерными программами».

Как показывают результаты изучения практики расследования, в процессе обыска изымаются, как правило, электронные носители информации следующих видов:

– системный блок персонального компьютера, в том числе с находящимся в нем жестким диском (43,7% уголовных дел);

Системный блок предназначен для хранения и закрепления комплектующих элементов персонального компьютера (системной платы, процессора, модулей оперативной памяти, блока питания и т.д.). Корпус системного блока имеет, как правило, вертикальную конструкцию (Desktop). Элементами системного блока можно назвать шасси (корпус), а также переднюю, заднюю и боковые стенки. На передней стенке находится лицевая панель, на которую выведены кнопки управления (кнопки включения/перезагрузки операционной системы), дисковод для гибкого магнитного диска и/или компакт-диска, а равно порты USB. Боковые стенки не представляют интерес, так как в стандартной сборке не содержат каких-либо деталей. Со стороны задней стенки можно наблюдать специальные разъемы для подключения внешних устройств – портов, каждый из которых имеет свое назначение (например, разъем LAN предназначен для подключения к локальной сети и/или глобальной сети Интернет).

Жесткий диск (встроенный внутри системного блока) предназначен для хранения компьютерной информации. Жесткий диск изнутри подразделяется на три блока: хранилище информации (стеклянные или металлические диски), «механику» (отвечает за позиционирование дисков и головок, вращение дисков) и «электронику» (содержит микросхемы, отвечающие за обработку

данных, коррекцию ошибок и управление механической частью; содержит кэш-память). При условии, если речь идет об исправном жестком диске, следователь с внешней стороны может наблюдать форму и материал его корпуса, а также разъемы (для соединения жесткого диска посредством кабеля с системной платой и блоком питания);

– оптический диск (39,0% уголовных дел);

Оптический диск представляет собой плоскую пластину круглой формы. Одна сторона предназначена для записи (в зависимости от вида оптического диска для записи может быть предназначено две стороны), назначение другой – сообщить пользователю полезную информацию. В качестве последней могут выступать сведения о торговой марке изготовителя (Verbatim), формате (DVD+R) и емкости диска (4,7 Гб), максимальной скорости чтения (16х) и максимальной продолжительности записанного видео в определенном формате (120 минут);

– персональный компьютер, в том числе ноутбук (32,8% уголовных дел);

Персональный компьютер – собирательный объект, состоящий из монитора, системного блока и устройств управления и ввода/вывода информации (мышь, клавиатура). Аналогичным образом устроен ноутбук, только все названные части объединены в одно устройство. Отметим, что, по общему правилу, практика изъятия персонального компьютера целиком (за исключением ноутбука) нецелесообразна. Ведь следователя по большей части интересует информация на электронных носителях, которые можно изъять отдельно. Вместе с тем изъятие следователем персонального компьютера целиком, в отдельных случаях, может быть признано целесообразным (например, для последующей экспертизы с целью установления механизма совершения преступных действий);

– карта памяти (67,1% уголовных дел). Данный носитель имеет преимущественно прямоугольную и квадратную формы (могут присутствовать специфические формы сторон). На лицевой стороне карты отображается ее формат (Memory Stick), емкость (4 Гб) и модель (Scan disk Ultra II).

Помимо сказанного, обратим внимание на то, что в единичных случаях изымались листы бумаги с распечаткой текстов компьютерных программ, справочная литература (по программированию, техническим характеристикам электронных

носителей информации и других элементов компьютера), сотовые телефоны и карты памяти.

Кроме того, целесообразно получить сведения о категории информации, обрабатываемой с помощью средств компьютерной техники и/или находящейся на электронных носителях. В частности речь может идти об общедоступных и/или конфиденциальных сведениях. Если следователь имеет сведения о том, что на электронных носителях может присутствовать общедоступная информация, то это не требует дополнительных мер на этапе подготовки. В противном случае следователь должен будет предпринять действия, направленные на санкционирование изъятия электронных носителей, содержащих охраняемую законом тайну.

В результате изучения нами уголовных дел было установлено, что большая часть обысков по делам, где фигурируют электронные носители, проводилась в жилом помещении (по 45,3% уголовных дел). Поэтому следователь, по общему правилу, помимо вынесения постановления должен получить судебное решение на производство обыска. Кроме как для обыска в жилище законодатель не требует от следователя получения судебного решения (статьи 29 и 182 УПК РФ). Вместе с тем, получение данного решения необходимо в ситуации проведения обыска в банках и иных кредитных организациях для изъятия предметов и документов, содержащих информацию о вкладах и счетах (системное рассмотрение УПК РФ, определение Конституционного Суда РФ от 19 января 2005 года № 10-О). Следуя этой логике, может возникнуть целесообразность получения судебного решения для производства обыска в помещении коммерческой организации, если речь идет об изъятии электронных носителей информации, могущих содержать, например, коммерческую тайну. Однако, считаем данную позицию дискуссионной. Так, в противовес может быть отмечено, что обыск предполагается в отношении «нарушителей». Поэтому факт изъятия у них искомых объектов не ведет к нарушению прав. Выемка же предполагается в отношении «законопослушных граждан», поэтому изъятие у них объектов обусловливает получение судебного решения.

Заметим также, что в ходе обыска могут изыматься предметы и документы, изъятые из оборота (часть 9 статьи 182 УПК РФ).

При изучении материалов практики нами был обнаружен лишь один случай, когда в ходе обыска изымались предметы и документы согласно части 9 статьи 182 УПК РФ. Однако это не означает

отсутствие вероятности применения части 9 статьи 182 УПК РФ. Так, неправомерный доступ к компьютерной информации может охватываться одним умыслом с публичным призывом к осуществлению экстремистской деятельности (статья 280 УК РФ). В соответствии со статьей 13 ФЗ РФ от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности» на территории России запрещаются издание и распространение печатных, аудио-, аудиовизуальных и иных материалов, содержащих хотя бы один из признаков экстремизма. Таким образом, следователь должен быть готов оценить обнаруженные материалы (в бумажной и/или электронной форме) на предмет наличия в них признаков экстремизма (нацистская символика и т.д.) с последующим изъятием таковых.

Добавим, что с 1 сентября 2012 года вступил в силу ФЗ РФ от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». В соответствии со статьями 5 и 11 данного закона, запрещается оборот отдельной информационной продукции (например, порнографического характера). Учитывая тот факт, что уже в настоящий момент практика сталкивается с совокупностью преступлений, предусмотренных статьями 272 и 242 УК РФ (242.1 – в отношении изображений несовершеннолетних), допустимо прогнозировать, что следователь должен быть готов изымать материалы, к примеру, порнографического характера (в бумажной и/или электронной форме). В любом случае, не подлежит изъятию в порядке части 9 статьи 182 УПК РФ компьютерное оборудование, в том числе системные блоки с жесткими дисками, так как это нарушает конституционное право на неприкосновенность частной собственности (статьи 35, 55 Конституции РФ).

Интересно, но практике известны отдельные случаи, когда в ходе обыска по делам, где фигурировали электронные носители информации, дополнительно изымались не свойственные объекты. Например, по уголовному делу об изготовлении телефонов-«двойников» в квартире подозреваемого был изъят газовый пистолет.

2. **Определение времени и места обыска**. По преступлениям, где фигурируют электронные носители, осуществляется оборот компьютерной информации. Данная информация может быть легко уничтожена или изменена лицом, имеющим знания, умения или опыт в области оборота компьютерных технологий. Поэтому проведение обыска в связи с обнаружением или возможностью обнаружения

электронных носителей носит неотложный характер (особенно, когда речь идет о «сетевых» преступления).

При этом могут быть получены основания для проведения обыска в связи с возникновением исключительных случаев, не терпящих отлагательства (часть 5 статьи 165 УПК РФ):

– возникновение оснований в ходе других следственных действий. Например, Д., используя право доступа к локальной сети организации, имея знания и умения в области компьютерного программирования, создал вредоносную программу «скрипт», заведомо приводящую к несанкционированному удалению информации и нарушению работы ЭВМ (г. Кемерово). После чего подключился к сети Интернет и с использованием удаленного доступа и названной программы произвел изменения кода программ организации по учету времени работы и объема полученной информации (сетевого трафика) пользователей Интернетом (последствия – уничтожение информации, нарушение работы ЭВМ). В процессе расследования следователь допросил в качестве свидетеля системного администратора пострадавшей организации. Администратор, среди прочего, пояснил, что при изучении следов неправомерно доступа им было обнаружено имя пользователя под логином Replay_5, а также телефонный номер. С данного номера с применением модема было осуществлено подсоединение преступника к сети организации. Ранее в организации работал Д., который использовал названный логин. Кроме этого, телефонный номер принадлежит Д. Следователь, учитывая глубокие знания Д. в области оборота компьютерной информации и возможность незамедлительного уничтожения им следов преступления, находящихся в электронно-цифровой форме, мог бы принять решение о проведении обыска в порядке части 5 статьи 165 УПК РФ;

– в зависимости от характера (обстановки) совершенного преступления. Например, происходит реализация результатов оперативно-розыскной деятельности в отношении организованной преступной группы, специализирующейся на использовании вредоносных программ для нарушения работы ЭВМ, системы ЭВМ или их сети (DDOS-атаки). Следственно-оперативная группа прибыла на место вероятного нахождения компьютеров, с помощью которых совершались преступления, однако таковые там отсутствовали (но есть следы из нахождения). Следователь по возбужденному уголовному делу может принять решение о проведении обыска с целью отыскания

названных ЭВМ и/или электронных носителей, программного обеспечения.

Так, в июле 2009 года А., являясь единственным участником и директором ООО «Изумрудный город», имея прямой умысел, направленный на осуществление незаконной предпринимательской деятельности без специального разрешения, с целью извлечения дохода в особо крупном размере, под видом проведения всероссийской стимулирующей лотереи «Сладкая жизнь!» незаконно осуществляла предпринимательскую деятельность по организации и проведению азартных игр с использованием игровых автоматов в игровых залах. В результате преступных действий А. получила доход в крупном размере (г. Омск). В процессе расследования следователь произвел выемку игровых автоматов из игровых залов. В ходе допроса свидетелей и согласно результатам оперативно-розыскной деятельности было установлено, что в помещениях игрового зала находится определенное количество игровых автоматов с заданной характеристикой. С целью изъятия данных автоматов была проведена выемка. Однако в игровых залах были обнаружены не все игровые автоматы. Следователь, учитывая указанное обстоятельство, незамедлительно произвел обыск в игровых залах, в ходе которого обнаружил и изъял искомые игровые автоматы.

Выбор времени проведения обыска зависит от ряда обстоятельств. Так, время проведения обыска может зависеть от последовательности действий следователя, предшествующих обыску (например, выбран тактический прием «внезапность обыска», и следователь предварительно приглашает обыскиваемое лицо якобы для допроса; в этом случае производство обыска планируется после прибытия обыскиваемого лица на допрос). Кроме этого, время обыска и его продолжительность зависит от возможности участия отдельных лиц (проведение обыска с участием эксперта ОВД в качестве специалиста может быть затруднено вследствие загруженности последнего).

Дополнительно целесообразно получить сведения о месте проведения обыска:

– о режиме функционирования обыскиваемого места. В частности желательно определить режим работы объекта, характеристики технических систем охраны;

– об источниках электропитания, используемых для обеспечения работы средств компьютерной техники на месте обыска.

В частности желательно установить их тип (электросеть, автономные, бесперебойные, комбинированные), а также место расположения пунктов обесточивания;

– о средствах компьютерной техники, которые могут находиться в месте обыска на момент его проведения. В частности желательно установить характеристики данных средств;

– о способах защиты средств компьютерной техники и информации на них от несанкционированного доступа. В частности желательно установить виды и характеристики применяемых способов защиты, а равно данные, позволяющие преодолеть средства защиты;

– о средствах связи и телекоммуникаций, применяемых для обеспечения работы средств компьютерной техники и/или информационного обмена на месте обыска. В частности желательно установить их тип, категорию (общедоступные или конфиденциальные) и другие характеристики.

3. **Определение круга участников обыска**. К участию в обыске целесообразно или необходимо (в зависимости от ситуации) пригласить:

– специалиста (обнаружение электронного носителя, восприятие его информационного содержания и т.д.);

– сотрудников органов внутренних дел (проникновение, охрана помещения, предотвращение противодействия следственно-оперативной группе);

– сотрудников оперативных подразделений, в том числе специализирующихся на оперативно-розыскной деятельности по преступлениям в сфере компьютерной информации (содействие в поисковых действиях);

– понятых (должны быть, как минимум, сведущи в компьютерной технике и порядке работы на ней на уровне пользователей);

– лицо, в помещении которого проводится обыск (совершеннолетних членов его семьи), его защитника или адвоката;

– представителя организации, в помещении которой проводится обыск.

4. **Сбор сведений об обыскиваемом лице**. Наличие у следователя информации о личности обыскиваемого способствует повышению эффективности обыска. Здесь следователя могут интересовать такие данные, как:

– наличие у обыскиваемого лица знаний, умений и опыта в области оборота компьютерных технологий. В зависимости от этого следователь может пригласить для участия специалиста в определенной области (например, специалиста в области операционной системы Windows или Linux). Кроме этого, следователь может получить сведения о программах, преимущественно используемых обыскиваемым, что позволит заранее определиться с характеристикой искомого объекта;

– продолжительность работы в сфере в области оборота компьютерных технологий. Дело в том, что подозреваемые, долгое время работающие с компьютерной информацией, готовятся к противостоянию с органами расследования. Но при этом рассчитывают исключительно на логические приемы противодействия и не в состоянии оценить собственные силы в эмоциональном плане. Знание этого может помочь следователю выбрать соответствующий тактический прием (например, наблюдение за эмоциональным состоянием обыскиваемого).

5. **Определение способа проникновения на объект и создание надлежащих условий**. Одним из вопросов, оказывающих большое влияние на качество обыска по делам нашей категории, является проникновение на объект. В криминалистической литературе повсеместно упоминается, что вхождение на объект, подлежащий обыску, должно носить внезапный характер. Применительно к расследованию преступлений в сфере компьютерной информации данной требование является необходимым, ведь речь идет об электронных носителях, информации в электронной форме. Такие объекты могут быть приведены в негодность уже одним нажатием клавиши на персональном компьютере. Кроме того, могут быть задействованы специальные устройства или программы, повреждающие или уничтожающие искомые объекты.

По нашему мнению, возможно применение нескольких вариантов для обеспечения внезапного проникновения на объект:

– вызвать обыскиваемое лицо для производства допроса в рабочий кабинет следователя (статьи 187-188 УПК РФ). В период проведения допроса орган дознания по ранее данному поручению следователя проводит обыск по месту проживания допрашиваемого (в порядке, установленном частью 11 статьи 182 УПК РФ). Однако данный вариант имеет недостатки, так, во-первых, у подозреваемого, по месту его проживания, могут отсутствовать совершеннолетние

члены семьи. Во-вторых, обыск по рассматриваемой нами категории дел имеет сложности (например, применение тактического приема «наблюдение за реакцией обыскиваемого»), поэтому поручать его органу дознания нецелесообразно;

– вызвать обыскиваемое лицо для производства допроса в рабочий кабинет следователя (статьи 187-188 УПК РФ). После их прибытия – ознакомление с постановлением о производстве обыска (решением суда), предложение выдать искомые объекты. В дальнейшем следователь и обыскиваемое лицо вместе с защитником (для иного лица – с адвокатом) убывают к месту проведения обыска.

В любом случае после проникновения следователь должен принять меры для обеспечения сохранности электронных носителей и информации на них. К таким мерам следует отнести:

– запрет кому-либо из присутствующих: прикасаться к работающим компьютерам, магнитным носителям, включать и выключать компьютеры; выключать энергоснабжение объекта;

– не производить никаких манипуляций с компьютерной техникой, если результат заранее не известен (например, если на подготовительном этапе получена консультация специалиста);

– удаление с места обыска легковоспламеняющихся веществ и материалов.

Одновременно принимаются меры к охране обыскиваемого места, в связи с чем целесообразно организовать охрану: периметра обыскиваемых площадей; места нахождения, в том числе хранения средств компьютерной техники и/или электронных носителей информации, а также иных объектов, могущих иметь значение для проведения обыска (например, места хранения средств защиты от несанкционированного доступа или паролей); пунктов (пульты) связи, охраны и электропитания, расположенные в месте обыска.

Дополнительно, ко всему сказанному отметим подготовка специальных средств, в том числе программного обеспечения, и упаковочного материала (специализированный лабораторно-исследовательский переносной компьютер, соединительные кабели и аппаратные средства, портативный принтер, загрузочные носители и накопители большой емкости, программное обеспечение общего и специального назначения; особенность – подготовка программного обеспечения, позволяющего осуществить выборочный поиск информации по заданным параметрам). При этом следует учесть, что в настоящее время поиск информации на электронном носителе по

заданным параметрам (например, по ключевому слову) осуществляется в рамках судебной компьютерно-технической (компьютерной) экспертизы. Так сложилась практика, однако, на наш взгляд, есть основания для ее пересмотра. Во-первых, поиск по ключевому слову можно провести с использованием стандартных возможностей операционной системы (через кнопку «ПУСК» и меню «ПОИСК»). Во-вторых, осуществлением поиска не предполагает проведение специального исследования (можно привлечь эксперта в качестве специалиста и с использованием специальных программ найти искомый объект);

Подводя итог, отметим, что подготовка к производству обыска, как средства отыскания, обнаружения и изъятия электронных носителей и информации на них, помимо общих, включает: формирование информационного образа искомого объекта; определение времени и места обыска; определение круга участников обыска; сбор сведений об обыскиваемом лице; определение способа проникновения на объект и создание надлежащих условий для обеспечения сохранности электронных носителей и информации на них. Осуществление подготовительных действий призвано способствовать повышению качества рабочего этапа проводимого обыска. Именно на этом этапе реализуются цели и задачи данного следственного действия, применяются выбранные тактические приемы, изымаются электронные носители информации и/или их объекты-носители.

Список использованных источников и литературы

1. См.: Быков В.М., Черкасов В.Н. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы: монография. – М.: Юрлитинформ, 2015. – 328с.

2. Рекомендации по поиску, фиксации, изъятию и хранению электронных носителей; определен порядок и пределы получения информации с электронных носителей для целей раскрытия и расследования преступлений. См, например, Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием пластиковых карт и их реквизитов: монография. – Волгоград: Волгоградская академия МВД России, 2005. – 276 с.; Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы: монография. – Омск: Омская академия МВД России, 2009. – 479 с.;

Способы получения доказательств и информации в связи с обнаружением (возможностью обнаружения) электронных носителей: учебное пособие В.Ф. Васюков, Б.Я. Гаврилов, А.А. Кузнецов [и др.]; под общ. ред. Б.Я. Гаврилова. – М.: Проспект, 2017 и др.

3. В ходе обыска могут быть обнаружены не только электронные носители информации, но и объекты, дающие основания для выдвижения версий о наличии и месте нахождения данных носителей (например, инструкция о пользовании накопителем на жестком магнитно-оптическом диске), а также информация в электронной форме.

4. Нами было изучено 64 уголовных дела, связанных с расследованием преступлений в сфере компьютерной информации.

5. Общими элементами подготовительного этапа производства следственного действия являются: анализ материалов уголовного дела; определение целей (задач); выбор тактики (линии поведения); составление плана и т.д.

ЗНАНИЕ О ПРИРОДЕ ОБЩЕСТВЕННОЙ ОПАСНОСТИ ПРЕСТУПЛЕНИЙ В СФЕРЕ НЕЗАКОННОГО ОБОРОТА НАРКОТИЧЕСКИХ СРЕДСТВ КАК ПРЕДПОСЫЛКА КРИМИНАЛИСТИЧЕСКОГО ПРОТИВОДЕЙСТВИЯ ИМ В КИБЕРПРОСТРАНСТВЕ

Е.С. Мазур, д.мед.н., профессор, зав. кафедрой уголовного права Западно-Сибирского филиала РГУП, г. Томск)
Л.Ю. Монгуш, магистрант 2 курса Западно-Сибирского филиала РГУП, г. Томск)

Трудно переоценить актуальность такого социально негативного явления как наркомания, ставшего трагедией современного социума. По масштабности распространения она сопоставима разве что с экологической катастрофой. Об этом свидетельствуют и исследования специалистов, приводящих внушительную цифру об употреблении наркотиков – 200 миллионов человек имеют опыт употребления наркотиков, 100 миллионов человек употребляют их регулярно, 50 миллионов человек больны наркоманией. Причем среди людей, страдающих от наркомании, значительную долю составляют несовершеннолетние и молодежь, и, как следствие, эта категория людей вряд ли уже способна к воспроизводству материальных и духовных ценностей, особенно в динамичных условиях социума.

Неудивительно, что увеличивающееся количество зависимых от наркотиков лиц увеличивает диапазон способов незаконного сбыта наркотических средств, который в последнее время активно использует и киберпространство. Мало выявлять Интернет-сайты и сервисы, посредством которых происходит реализация наркотических веществ, необходимо также уметь оценивать является ли данный интернет-ресурс результатом деятельности небольшой группы когнитивно развитых представителей криминалитета или в данном конкретном случае мы наблюдаем элемент системы наркоторговли – централизованной и эволюционирующей. Понимание криминологической и криминалистической природы противодействия преступлениям, связанным с незаконным оборотом наркотических веществ также будет способствовать противодействию в Интернет-пространстве пропаганды потребления наркотиков. Однако для реализации вышесказанного необходимо еще раз отметить

общественно опасные проявления рассматриваемой группы преступлений.

Для раскрытия проблем, связанных с незаконным оборотом наркотических средств, представляется необходимым обратиться к вопросу о взаимосвязи наркомании и преступного поведения, поскольку эти явления детерминированы единой социальной природой. Из криминологической и криминалистической литературы нам известно, что «фоновым» явлением преступности служит именно социально отклоняющееся поведение, а вектором этой связи служит признание социально отклоняющегося поведения как преступного, сопряженного с рядом преступлений, негативно влияющего на некоторые группы населения в области формирования ценностных установок и ориентаций и своеобразной зоной риска, в которую человек входит в качестве потенциальной жертвы или преступника.

Так, на территории Республики Тыва в 2015 г. в суд поступило 798 дел по данной категории преступлений, в 2016 г. – 801 дело, а за 4 месяца 2017 г. – 192 дела, значительную часть среди этих преступлений составляли кражи, грабежи, причинение вреда здоровью различной степени тяжести, убийства. Причем, именно добывание средств для приобретения наркотических средств составляет значительную часть краж и грабежей, что подтверждается и исследователями-криминологами, установившими, что из десяти имущественных преступлении шесть совершены наркоманами [1, с. 15].

Кроме этого, криминальный вид предпринимательства в области незаконного оборота наркотиков является высокодоходным; общественности известны случаи вовлечения сотрудников правоохранительных органов в наркосистему, потворничества незаконному прекращению соответствующих уголовных дел и развития коррупции в целом [2, с. 35-37], а по утверждению С.Г. Олькова «представители наркобизнеса активно внедряются в политику, противодействуя законной деятельности органов государственной власти» [3, с. 92-93]. Рядом ученых, например, А.Л. Репецкой отмечается процесс превращения сбыта наркотиков в транснациональную преступную деятельность [4, с. 30-31], а особенности географического положения России служат фактором концентрации наркотиков в стране, поступающих из стран ближнего и дальнего зарубежья.

Нельзя не отметить и тот факт, что в виктимологическом аспекте, люди, страдающие наркоманией, обладают повышенной виктимностью, поскольку для этой категории лиц характерно плохое здоровье, психические аномалии и общая социальная дезадаптация.

Определяя общественную опасность преступлений как обязательный признак сущности преступления и его социальной природы, отметим ее взаимосвязь с вредоносностью преступления и причинением ущерба обществу и фактической предопределенностью его повторения [5, с. 1-7].

Заметим, что порождение негативных тенденций для общества является сущностью вредоносности преступления в сфере незаконного оборота наркотиков, что выражается в медико-биологическом, социальном и психологическом аспектах. Не вдаваясь в узкоспециальную медицинскую сферу, отметим, что наркомания приводит к истощению нервной системы, ослаблению иммунитета, нарушению обмена веществ, преждевременному старению организма, развитию психических аномалий, возможности рождения неполноценных детей, а психическая зависимость толкает человека на пренебрежение путями добычи наркотиков. Кроме этого, развитие болезни приводит к формированию представления о наркотике как первостепенной ценности, доминирующей в структуре психики, а проявлением физической зависимости является абстинентный синдром как тягостное расстройство, возникающее в случае перерыва в регулярном употреблении наркотиков.

Спектр социальной вредоносности преступлений достаточно широк. Достаточно упомянуть о неспособности людей, страдающих от наркомании, к позитивной деятельности. Человек, страдающий наркоманией, утрачивает значимость концептуальных ключевых ценностных понятий и ориентиров, например, добра и справедливости, наркотические интересы приобретают все большее значение, приходя на смену нравственным критериям, наркоман при этом не способен адекватно увидеть и оценить себя в системе мироустройства, т.к. разрушены естественные механизмы оценки окружающего мира и себя в нем.

Нельзя не сказать и о пропаганде со стороны наркоманов своего образа жизни, т.к. считают его нормальным и адекватным, что приводит к приумножению социальной среды наркоманов, формированию собственной субкультуры со своими ценностями, языком, стереотипами, установками, понятиями и др. Формирование

данной субкультуры отметил С. В. Березин: рассматривая ее направленность и содержание, он отмечал ее в качестве полноценной социальной антисистемы [6, с. 8].

Рассматривая общественную опасность в психологическом аспекте, можно отметить развитие дезадаптивного поведения ввиду заболевания наркоманией. Сначала происходит процесс потери социальных связей в малых коллективах, например, семье. Известно, что наркоман поначалу вынужден скрывать свою привязанность, а в дальнейшем он уже не способен на выполнение тех общественных и социальных функций, которые выполнял ранее без труда. Это приводит к формированию в сознании наркомана представлений об опасности той группы, в которой он пребывал, т.к. социум обременен негативными для наркомана эмоциями. Такая установка приводит наркомана в социальную среду себе подобных, где нет психологического отчуждения, есть положительные эмоциональные связи, а употребление наркотиков – образ жизни.

Психология рассматривает наркоманию в социокультурном аспекте как проблему личности, которая меняется в процессе развития наркотической зависимости. Это изменение отражено в наличии внутренних конфликтов, их постепенном обострении, развитии психической дезадаптации, которая становится все более очевидной. Лень, пассивность, бесплодные фантазии, неспособность принимать решения, отсутствие усидчивости, снижение умственных способностей, развитие апатии – вот далеко не полный перечень последствий наркомании. К числу же особенностей наркоманов относят их этическую деградацию, психологическую опустошенность, отсутствие эмпатии и душевную холодность даже с самыми близкими людьми. Все обозначенные изменения свидетельствуют о психосоциальной деградации личности.

Отметим в заключение, что угроза здоровью населения, регресс в области психического и физического здоровья человека, подрыв экономического потенциала страны, негативные тенденции в демографической сфере, самоизоляция наркоманов от социокультурного окружения – все это в определённой степени является следствием критической ситуации с распространением наркотиков, при этом расширяется и зона криминального риска. Противодействие распространению наркотиков через Интернет актуальная криминалистически значимая задача современности.

Список использованных источников

1. Прохорова М. Л. Наркотизм: уголовно-правовое и криминологическое исследование / М.Л. Прохорова. – СПб.: Юридический центр Пресс, 2002. – 285 с.
2. Ивасенко В. Б. О развитии правовой основы национальной безопасности в сфере противодействия незаконному обороту наркотиков на Государственной границе Российской Федерации. / В.Б. Ивасенко // Оперативник (сыщик). – 2005. – № 4. – С. 35-39.
3. Ольков С. Г. Юридический анализ (исследовательская юриспруденция): в 2 т. / С.Г. Ольков. – Тюмень, 2003. – Т. 2. – 140 с.
4. Репецкая А. Л. Криминологическая характеристика мировой индустрии наркобизнеса – ведущего направления деятельности транснациональной организованной преступности / А.Л. Репецкая. – М.: ЮристЪ, 2003. – 163 с.
5. Фефелов П. А. Механизм уголовно-правовой охраны: Основные методологические проблемы: / П.А. Фефелов. – Екатеринбург, 1993. – 50 с.
6. Березин С. В. и др. Предупреждение подростковой и юношеской наркомании / под ред. С.В. Березина, К.С. Лисецкого. – Самара: Самарский университет, 2002. – 206 с.

ПРАВОВЫЕ И ПРАКТИЧЕСКИЕ АСПЕКТЫ ПОЛУЧЕНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ О КИБЕРПРЕСТУПНИКАХ

В.В. Павлюков, старший инспектор учебно-методического отдела Луганской академии внутренних дел имени Э.А. Дидоренко

Способы оперативного получения информации и своевременное ее использование при раскрытии и расследовании преступлений являются одними из основных задач оперативно-розыскной деятельности. Для реализации таких задач оперативный сотрудник постоянно нуждается в информационных источниках. Общеизвестно, что таким современным и постоянно развивающимся информационным источником является глобальная компьютерная сеть Интернет. Практически каждый может получить доступ к Интернету, где возможно искать, сохранять, удалять и передавать компьютерную информацию на дальние расстояния за считанные секунды.

Поскольку Интернет является общедоступной системой, возникает необходимость контроля информационных потоков. Это связанно с тем, что интернет-ресурсы используют в противоправной деятельности, в том числе лица, которых в литературных источниках принято называть киберпреступниками.

Киберпреступностью именуют совокупность преступлений, совершаемых в киберпространстве с помощью, посредством или против компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству [8, с. 48].

Киберпреступником (хотя мы и отдаем себе отчет в уязвимости этого термина) принято именовать лицо, которое совершает противозаконные действия с использованием сети Интернет. Зачастую, чтобы безнаказанно осуществлять подобную деятельность, лицо дезинформирует других пользователей, используя вымышленные анкетные данные и адреса.

Ученые А.А. Алябьев и А.В. Лагуточкин справедливо отмечают, что современный криминальный мир уже не мыслит своего преступного функционирования без Интернета и указывают на то, что проведение оперативно-розыскных мероприятий в сети Интернет должно стать главенствующим в борьбе с новейшими угрозами в условиях функционирования государства [1, с. 67]. Однако в практической деятельности бытует мнение, что для получения

оперативно-значимой информации по выявлению преступления и лица, его совершившего, необходимы навыки и умения в области программирования и компьютерных технологий.

Помимо прочего, и интернет-компании не охотно идут на помощь полиции. Так, корпорация Google получает от российских государственных органов сотни запросов о пользователях, при этом отмечается, что ни один из них не был удовлетворен [15].

А.Л. Осипенко указывает на проблему выявления стабильных каналов получения оперативно-розыскной информации непосредственно в сетевом пространстве и считает, что упорядочивание этих каналов и оптимизация поступающих из них информационных потоков сохраняет особую актуальность. Для принятия решений в этом направлении ученый предлагает с позиции оперативно-розыскной науки системно изучать закономерности отражения оперативно-розыскной информации в сетевых ресурсах и особенности применения разведывательно-поисковых методов для ее обнаружения, получения, проверки и фиксации [10, с. 14].

В поисках решения указанных проблем целесообразно рассмотреть конкретные правовые способы и средства поиска и выявления правонарушителей, использующих в преступных целях сеть Интернет. Анализируя ФЗ РФ «Об оперативно-розыскной деятельности», как основное «плечо», на которое необходимо опираться в борьбе с киберпреступлениями, следует указать на новые шаги, предпринятые законодателем в этом направлении, а именно принятие Госдумой РФ «Антитеррористического пакета Ирины Яровой» [4]. Так, ФЗ РФ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» от 06.07.2016 N 374-ФЗ [9] были внесены изменения в статью 6 ФЗ РФ «Об оперативно-розыскной деятельности». Он был дополнен новым оперативно-розыскным мероприятием – «получение компьютерной информации». Из мероприятий, обозначенных в данной статье ранее, можно выделить еще два, которые оперативный сотрудник прямо либо косвенно может использовать для получения оперативно-значимой информации из интернет-источников. Это: контроль почтовых отправлений, телеграфных и иных сообщений и снятие информации с технических каналов связи. Однако, данные мероприятия не в полной мере адаптированы к рассматриваемым нами

ситуациям, поскольку предусмотренные ими действия зачастую осуществляются при обстоятельствах, когда факт совершения противоправного деяния уже наличествует и установлена личность киберпреступника.

В свою очередь, добавление нового пункта – «получение компьютерной информации» – уже вызвало неоднозначную реакцию, в первую очередь на полицейских форумах сети Интернет. Участники обсуждения считают, что получение компьютерной информации не что иное, как составная часть оперативно-розыскного мероприятия «снятие информации с технических каналов связи». Интересное мнение высказал администратор форума «Skyment», который считает: «Простой запрос в "поисковик" подпадёт под ОРМ...» [12]. Мы же считаем, что под мероприятием, именуемым «получение компьютерной информации», нужно подразумевать действие, направленное на получение компьютерной информации у отечественных операторов и провайдеров телекоммуникаций [11, с.179]. Такое заключение вытекает из «Антитеррористического пакета Ирины Яровой», где в первую очередь было акцентировано внимание на увеличении сроков хранения компьютерной информации операторами связи. Однако здесь возникает проблема, связанная с зашифрованным трафиком. По этому поводу гендиректор InfoWatch Наталья Касперская сетует, что «сейчас у нас есть кусок Интернета, который совершенно неподконтролен собственной стране, это неправильно» [2].

Поэтому уместно рассмотреть такие ОРМ, которые позволили бы получать и зашифрованную компьютерную информацию. А.В. Мовчан предлагает использовать метод компьютерной разведки, выделяя его как необходимое оперативно-поисковое мероприятие, заключающееся в целенаправленном поиске и получении информации из компьютерных систем и сетей, доступ к которым не ограничивается их собственником, владельцем или держателем или не связан с преодолением системы логической защиты, осуществляемым работниками оперативных или оперативно-технических подразделений с целью выявления сведений криминогенного и криминального характера [7, с. 110]. Однако интернет-источники противоречат данному высказыванию, а именно, разведка в системах телекоммуникаций включает в себя получение несанкционированного доступа к информации, перехват сообщений и перехват данных [14]. То есть, с использованием компьютерной разведки возможно решить

проблему, связанную с установлением личности злоумышленника, и фиксации его преступной деятельности в сети Интернет, где необходимо получить ту компьютерную информацию, которая не только шифруется в процессе передачи, но и доступ к которой закрыт.

В данной ситуации целесообразно указать не только на проводимые мероприятия, но также обозначить возможные практические пути решения, при помощи которых будет осуществляться компьютерная разведка. Рассматривая понятие компьютерной разведки, было бы не лишним обозначить возможности компьютерных технологий, а именно их внедрение на этапе проведения ОРМ с целью получения оперативно - значимой информации. Стоит также указать, на вышеуказанный пример с Google, где преодоление системы логической защиты является единственным и необходимым действием, направленным на получение оперативно-значимой информации.

Рассмотрим стандартную ситуацию. Чтобы оставить информацию в сети Интернет, необходимо пройти регистрацию. При этом заполняется регистрационная форма, состоящая из полей, в которых пользователь указывает свои анкетные данные, такие, как ФИО, страну и город проживания, контактный телефон, электронный почтовый адрес. После регистрации все сведения, которые внесены в регистрационную форму, записываются и хранятся в базе данных сайта для последующей авторизации пользователя. С вышеуказанной информацией в базе данных сервера, где размещен сайт, записываются и хранятся:

- дата регистрации пользователя на сайте;
- IP-адрес компьютера, с которого производилась регистрация;
- данные о версии браузера и операционной системе, при помощи которой осуществлялась регистрация.

Полученную информацию владелец сайта использует, например, как статистические данные. Эти данные фиксируются и далее могут визуально отображаться специальным программным обеспечением. Процесс фиксации статистических данных происходит скрытно и зачастую без ведома пользователя. Владелец сайта может использовать статистические данные, чтобы определить местонахождение пользователя, предложить информацию, соответствующую его фактическим географическим данным, заблокировать пользователя и т. д.

Полученная информация может выступать не только как статистическая, но также иметь решающее значение при поиске и фиксации лиц, осуществляющих противоправные действия в сети Интернет. Как правило, при регистрации на сайтах киберпреступник указывает ложные данные о себе и вводит в заблуждение пользователя. Из-за этого становится практически невозможным установить реальную информацию о нем и выявить его местонахождение без доступа к статистическим данным. Не принимая во внимание то обстоятельство, что компьютер также оставляет данные о себе при посещении сайта, зачастую киберпреступник считает, что его противоправные действия останутся безнаказанными и уверен, что отследить его местонахождение практически невозможно из-за того, что он внес вымышленные данные в форму регистрации. В связи с этим можно предположить, что, для того, чтобы выявить киберпреступника, нам необходимо получить статистические данные, оставленные им при посещении сайта.

Законодательное получение таких данных относится к такому оперативно-розыскному мероприятию, как снятие информации с каналов связи. Согласно ст. 8 ФЗ РФ «Об оперативно-розыскной деятельности», снятие информации с технических каналов связи допускается на основании судебного решения и при наличии ограниченного перечня оснований, указанных в этой статье. Необходимо заметить, что подобное мероприятие является длительным по времени реализации и не всегда дает положительный результат.

В борьбе с киберпреступностью уместно сослаться на мнение ранее упомянутых ученых, которые убеждены, что в процессе оперативной работы очень важно применять такие оперативно-розыскные мероприятия, которые в случае их осуществления не требуют санкций со стороны руководителя оперативно-розыскного органа или суда. Все это значительно упростит работу в информационном пространстве Интернет, сэкономит время и ресурсы, позволит действовать избирательно и эффективно [1, с. 68].

Учитывая сказанное, целесообразно рассмотреть методы, которые используют в своей деятельности сами правонарушители для получения интересующих их данных о пользователях сети. Для получения логинов и паролей на сайтах они чаще всего прибегают к созданию и использованию фишинговых сайтов (сайтов-ловушек). **Фишинг -** вид интернет-мошенничества, целью которого является

получение доступа к конфиденциальным данным пользователей - логинам и паролям [13].

Ю.В. Гольчевский и А.Н. Некрасов выделяют самые распространенные фишинговые сайты - поддельные или несуществующие интернет-магазины, а также сайты, которые полностью копируют официальные сайты банков или финансовых организаций, известных социальных сетей и т. д. [3, с. 254]. Для начала работы на таких сайтах требуется ввод логинов, паролей, номеров пластиковых карт и других данных, которые киберпреступник может использовать в противоправных целях.

Например, настоящий адрес популярнейшей социальной сети «Одноклассники» выглядит так: www.odnoklassniki.ru. Киберпреступники с целью обмана пользователя регистрируют доменные имена, максимально похожие на оригинал, при этом доменное имя поддельного сайта отличается лишь одной-двумя буквами (www.odnoklasniki.ru, www.odnokassniki.ru и т.п.). На беглый взгляд для пользователя такой адрес покажется подлинным. Далее на эти адреса мошенники загружают полные визуальные копии настоящего сайта «Одноклассники» и заманивают пользователя на свой сайт для получения логина, пароля и т. п. [6].

Взяв на вооружение такой способ «компьютерной разведки» оперативный сотрудник также может создать и использовать свой сайт для установления данных о киберпреступнике. Законодатель не запрещает создавать сайты сотрудникам ОВД. Более того, в ч. 1 ст. 11 Закона «О полиции» указывается на то, что полиция в своей деятельности обязана использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру.

Процесс создания сайта не является дорогостоящим и не требует санкционированного разрешения. Для создания сайта необходимо приобрести домен (.ru, .com, .net), создать сайт при помощи специальных сервисов или программ (AdobeDreamweaver, WordPress, Joomla) и разместить его на хостинге. Уже сейчас все это обойдётся в считанные копейки: по состоянию на 12.10.2017 г. покупка домена в зоне «.ru» на официальном регистраторе доменных имён REG.RU составляет 199 рублей, а месячная стоимость услуг хостинга на этом сайте составляет 126 рублей [5]. После создания сайта и размещения его на хостинге, оперативному сотруднику необходимо включить инструмент AWstats. Он служит инструментом

веб-аналитики, который будет собирать статистику о трафике на сайте и о посетивших сайт пользователях [16]. На данный момент не только REG.RU, но и большинство хостинг-провайдеров предоставляют такой инструмент веб-аналитики, как AWstats.

В программном обеспечении AWstats реализована возможность получения данных, способствующих фактическому установлению компьютера, при помощи которого киберпреступник совершает противоправные действия. При помощи AWstats мы можем получить такие данные:

- IP-адрес компьютера, с которого осуществлялся переход на наш сайт;
- время перехода на сайт;
- активность на сайте;
- посещаемые страницы сайта.

Эти данные могут храниться и обрабатываться в режиме реального времени. При этом оперативному сотруднику не обязательно постоянно наблюдать за конкретным пользователем. Нужно создать такие условия, чтобы киберпреступник перешел на созданный им сайт. Зайдя в интерфейс программы AWstats, программа покажет, когда и с какого IP-адреса заходил пользователь на сайт. Это даст возможность, не имея полного доступа к сайту, при помощи которого мошенник совершает противоправные действия, оперативно устанавливать статистические данные, а именно время перехода и IP-адрес компьютера, с которого осуществлялся переход киберпреступником по ссылке. Полученные данные позволят значительно сузить круг подозреваемых.

После того, как сотруднику станет известен IP-адрес компьютера, он может установить принадлежность данного IP-адреса к провайдеру. Для этого лучше всего подходит бесплатный сайт http://2whois.ru/, который покажет, какому провайдеру принадлежит запрашиваемый IP-адрес, физический адрес провайдера и его владельца с контактным телефоном. Оперативному сотруднику останется установить связь с провайдером для предоставления анкетных данных владельца IP-адреса.

Не обращаясь к владельцу сайта, где злоумышленник осуществляет свою противоправную деятельность, оперативный сотрудник при помощи фишингового сайта может получить логин и пароль злоумышленника. Такие действия дадут возможность ознакомиться с перепиской злоумышленника и оперативно выявить

дополнительную информацию о противоправной деятельности и установить криминальные связи.

Стоит также отметить, что умение проводить разведку с использованием современных компьютерных технологий имеет большое значение в поиске правонарушителей и выявлении их противоправных действий не только в виртуальном, но и в реальном пространстве.

В поисках путей внедрения компьютерной разведки как необходимого современного мероприятия в оперативно-розыскной работе, нами был рассмотрен и предложен вариант создания и настройки личного сайта оперативного сотрудника ОВД, после перехода на который киберпреступник оставит оперативно-значимую информацию о себе. Такие деяния помогут не только установить местонахождение лица, совершавшего противозаконные действия, но также узнать логин, пароль, электронную почту, IP-адрес киберпреступника, что даст возможность получать доступ к аккаунту последнего.

И в заключение. Дополнение перечня оперативно-розыскных мероприятий, указанных в статье 6 ФЗ РФ «Об оперативно-розыскной деятельности», не изменило наше мнение о целесообразности дополнения его таким мероприятием как «компьютерная разведка». Подобный шаг повысит эффективность оперативно-розыскной работы в сети Интернет.

Список использованных источников и литературы

1.Алябьев А. А., Лагуточкин А. В. Проблемы осуществления оперативно-розыскных мероприятий в информационном пространстве сети Интернет // Проблемы правоохранительной деятельности. – 2013. – №1. – С. 66-69.

2.Власти идут на перехват. Работа над дешифровкой интернет-трафика признана официально // URL: https://www.kommersant.ru/doc/3099556 (дата обращения: 13.10.2017).

3.Гольчевский Ю. В., Некрасов А. Н. К вопросу о кибербезопасности Интернет пользователей // Известия Тульского государственного университета. Технические науки. – 2013. – №3. – С.253-261.

4.Госдума приняла антитеррористический пакет Ирины Яровой // URL: http://pravo.ru/news/view/130575 (дата обращения: 26.07.2016).

5.Зарегистрировать домен//URL: https://www.reg.ru/domain/new(дата обращения: 27.07.2016).

6.Как отличить сайт - оригинал от сайта - подделки и мошеннического сайта? // URL: http://www.vseafery.ru/afery-v-internete/kak-otlichit-sait-original-ot-saita-poddelki-i-moshennicheskogo-saita (дата обращения: 27.07.2016).

7.Мовчан А.В. Отдельные аспекты применения компьютерной разведки в оперативно-розыскной деятельности // Проблемы правоохранительной деятельности. – 2014. – №2. – С.107-112.

8.Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. – 2012. – № 24. – С.45-55.

9.О внесении изменений в Федеральный закон "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: ФЗ РФ от 06.07.2016 N 374-ФЗ // СПС «КонсультантПлюс» (дата обращения: 27.07.2016).

10. Осипенко А.Л. Новые технологии получения и анализа оперативно-розыскной информации: правовые проблемы и перспективы внедрения // Вестник Воронежского института МВД России. – 2015. – № 2. – С.13-19.

11. Павлюков В.В. Правовые аспекты получения и защиты компьютерной информации в сети Интернет // Вестник Дальневосточного юридического института МВД России – 2017. – № 3 (40). – С. 178-182.

12. Форум сотрудников ОВД // URL: https://www.police-russia.ru/showthread.php?p=3553535 (дата обращения: 26.07.2016).

13. Фишинг URL: https://ru.wikipedia.org/wiki/Фишинг (дата обращения: 20.07.2016).

14. Электронные методы и средства разведки // URL: https://wiki2.org/ru/Электронные_методы_и_средства_разведки (дата обращения: 11.10.2017).

15. Google пошел на сотрудничество с правоохранительными органами России, удовлетворив их запрос о раскрытии данных пользователей. Согласно отчету Google Transparency Report, за июль-декабрь 2012 года корпорация удовлетворила 1% запросов российских государственных органов на раскрытие данных пользователей // URL: https://wek.ru/google-

sotrudnichaet-s-silovikamihttps://wek.ru/google-sotrudnichaet-s-silovikami (дата обращения: 12.10.2017).

16. What is AWStats // URL: http://www.awstats.org (дата обращения: 23.07.2016).

ОСМОТР МЕСТА ПРОИСШЕСТВИЯ ПРИ ПРЕДВАРИТЕЛЬНОЙ ПРОВЕРКЕ СООБЩЕНИЙ О КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЯХ. I. ОРГАНИЗАЦИОННЫЕ ОСНОВЫ[1]

В.В. Поляков, к.ю.н., доцент кафедры уголовного процесса и криминалистики Алтайского государственного университета
А.С. Никитин, следователь Славгородского межрайонного следственного отдела следственного управления Следственного комитета РФ по Алтайскому краю

Понятие «организация предварительной проверки преступлений» тесно связано с понятием «организация расследования преступлений» и соотносится с последним, как частное с общим, при этом сам термин «организация», согласно законам формальной логики, в науке рассматривается в трех значениях: как процесс, качество и объект [1]. В настоящей статье объектом исследования является организация предварительной проверки компьютерных преступлений в качестве процесса, т.е. целенаправленной деятельности по упорядочению связей между частями одного из видов государственной властной деятельности, реализуемой в форме такого процессуального действия как осмотр места происшествия [1].

Существующие рекомендации проведения проверочных мероприятий по преступлениям в сфере компьютерной информации, особенно касающиеся их наиболее опасных разновидностей, отсутствуют или имеют типовой характер, не в полной мере учитывая конкретные обстоятельства и различные ситуации в целом. Возникающие при этом на практике затруднения требуют своего научного исследования и практического разрешения. Следует заметить, что в криминалистической литературе значительное внимание уделяется особенностям проведения следственных действий в стадии предварительного расследования компьютерных преступлений. Однако не уделено должное внимание проблемам, стоящим на пути повышения эффективности следственной и оперативно-розыскной работы по доследственной проверке сообщений о компьютерных преступлениях, от результатов которой зачастую

[1] Публикация подготовлена в рамках поддержанного РГНФ научного проекта №16-33-01160.

зависит успех расследования. В итоге остаются неразрешенными многие тактические вопросы получения и использования криминалистически значимой информации, особенно имеющей доказательственный потенциал [2].

При проверке сообщений о компьютерных преступлениях получение судебных доказательств возможно, как правило, путем: истребования и изъятия документов, средств компьютерной техники и иных предметов; назначения компьютерных экспертиз; производства осмотра места происшествия, программно-аппаратных средств компьютерной техники, электронных документов. В ходе иных действий обычно происходит получение поисково-ориентирующей и поисковой криминалистически и оперативно значимой информации.

Одним из наиболее эффективных действий при проверке сообщений о компьютерных преступлениях, с точки зрения получения судебных доказательств, является осмотр места происшествия. Это связано с тем, что в его ходе разрешается довольно широкий круг разнородных вопросов [5]. К их числу, в частности, относятся: наблюдение, изучение обстановки и существования тех или иных признаков у осматриваемых объектов, выдвижение и проверка криминалистических версий, производство различных вычислений, сравнений наблюдаемых объектов между собой, описание и иное запечатление криминалистически значимой информации, фиксация, изъятие и оценка обнаруженных следов преступлений [4]. Таким образом, эффективное производство данных действий в рамках предварительной проверки сообщений невозможно без их грамотной организации.

Осмотр места происшествия состоит из трех последовательно развивающихся стадий: подготовительной, рабочей и заключительной [6]. При расследовании преступлений, совершаемых в сфере компьютерной информации, по своей сути и объему работ на подготовительной стадии имеется значительное количество специфических моментов, обусловленных компьютерно-технической составляющей данных преступлений. Так, следователи, специалисты и понятые должны обладать минимальными знаниями компьютерной информации, техники и технологий, позволяющими понимать специфику электронно-цифровых следов, механизма их образования, типичных средств и способов совершения компьютерных преступлений и многого другого [7].

На наш взгляд, важно выделить тактические особенности

осмотра места происшествия на этапе предварительной проверки сообщений о компьютерных преступлениях в следующих ситуациях:

- когда поступает сообщение или заявление о преступлении;
- когда предоставлены оперативно-розыскные материалы, содержащие сведения об обнаруженных признаках преступления.

В первой ситуации осмотр места происшествия будет обладать признаком неотложности, во втором ситуации, как правило, осмотр носит задачу поиска и фиксации конкретных доказательств, тем самым имея некоторое сходство с обыском.

В ситуации, когда осмотр места происшествия производится неотлагательно, любое промедление может обернуться потерей доказательств и наступлением иных неблагоприятных последствий. В связи с этим следователям и дознавателям необходимо предложить четкие научно-практические рекомендации по эффективному производству данного следственного действия и недопущению при его проведении типичных ошибок.

На подготовительной стадии осмотра места происшествия следователь должен организовать следственно-оперативную группу, которая бы смогла эффективно выполнить работу под его руководством. От правильного состава группы во многом зависит качество проведения следственного действия. При ее формировании следует обеспечить участие минимум одного субъекта, свободно владеющего навыками работы с компьютерной техникой (пользование стандартным программным обеспечением компьютера, навыки по доступу в сеть «Интернет», использованию онлайн-сервисов и пр.). Некоторые трудности вызывает необходимость обеспечения участия в осмотре места происшествия компетентных специалистов и понятых. Их привлечение, особенно в условиях периферийных районов, может быть невозможно или крайне затруднено в силу их отсутствия или сопряжено с существенными материально-финансовыми затратами. Решение данных проблем занимает много времени, в ходе которого обстановка места происшествия может критически измениться. В случаях, когда собирание доказательств не вызывает затруднений (изъятие системного блока компьютера, запись файлов на электронный носитель информации и пр.), привлечение понятых, имеющих специальные технические познания, не обязательно, так как происходящие действия можно зафиксировать с помощью средств видеозаписи.

В тех случаях, когда требуется незамедлительно осуществить

осмотр места происшествия, но отсутствуют необходимые для этого участники, в том числе, когда сам следователь не может незамедлительно прибыть на объект осмотра, то возникает практика поручения проведения следственного действия сотрудникам оперативно-розыскной деятельности (ч. 4 ст. 38 УПК РФ). Поручение может содержать тактические рекомендации, которые должны неукоснительно соблюдаться, например, об одновременном осмотре нескольких мест происшествия.

Место происшествия по компьютерным преступлениям, в которых был задействован удаленный доступ, может охватывать достаточно большую территорию. Это обуславливает потребность в оказании оперативной помощи следствию. Содействие следственным органам может быть оказано в различных формах и различными субъектами. Так, потерпевшие и очевидцы, сообщившие о преступлении, могут участвовать в пресечении преступной деятельности или ее неблагоприятных последствий, а также они могут принять меры по сохранению следов преступления. Однако помощь следствию со стороны непрофессионалов всегда связана с тактическим риском. Вполне возможна ситуация, когда следователь по ошибке обратится за помощью к лицам, заинтересованным в исходе дела, которые своими умышленными действиями могут удалить или повредить следы преступления. Со стороны подобных лиц возможно также введение следствия в заблуждение путем искажения иной криминалистически значимой информации. Такие действия могут быть продиктованы различными мотивами, например, отведением от себя внимания правоохранительных органов. Не исключено также халатное отношение осуществляющих помощь лиц, которые не несут за это ответственность. Другой проблемой является добросовестное заблуждение или некомпетентность лиц, содействующих следствию, например, экстренное обесточивание объекта преступного посягательства при подозрении, что преступление имеет длящийся или эпизодический характер. Такое решение может быть необоснованным, а его последствия могут привести к потере информации, имеющей важное доказательственное значение.

В случае предполагаемой сложности производства осмотра места происшествия руководством следственного подразделения целесообразно разрешить вопрос о формировании двух следственных групп (редко более) с обязательным назначением следователя, руководящего ими. Руководящий следователь определяется с составом

обоих групп, по своему усмотрению назначая «старшего» первой группы, который будет ее курировать, выполнять поручения и докладывать о работе. Выбор «старшего» первой группы определяется, как правило, исходя из его компетентности и предполагаемых межличностных взаимоотношений в группе.

Полагаем, что по компьютерным преступлениям зачастую выезд на место происшествия двух следственных групп более эффективен. В зависимости от конкретных обстоятельств дела на место происшествия бывает целесообразно отправить первую группу как можно быстрее. В ее состав можно включить сотрудника уголовного розыска совместно с участковым уполномоченным полиции. Вместе с указанными лицами целесообразно отправить двух гражданских лиц, которые смогут выступить в качестве понятых. При наличии у следователя общественного помощника, в зависимости от уровня его компетенции, возможно, также его привлечение. Полагаем, что имеется практическая необходимость в создании на общественных началах группы «дежурных специалистов» в сфере компьютерной информации (включая последних, например, в ряды внештатных сотрудников некоторых правоохранительных органов), которых можно было бы привлекать в состав первой группы, так как потребность в них наиболее велика.

Первая следственная группа может наиболее быстрым образом выполнить следующие задачи.

Первоочередные – пресечение преступной деятельности и неблагоприятных последствий преступления, а также охрану объектов и лиц, представляющих криминалистическое значение, например, мест нахождения компьютерной техники с явными следами преступления, подозреваемых, потенциальных объектов новых преступных посягательств, удаление посторонних лиц с места происшествия и пр. [3]

Разведывательные – выяснение и оценку обстановки, сложившейся на месте происшествия (например, количества и качеств аппаратных средств компьютерной техники и их программного обеспечения, в том числе, по защите информации, вредоносных программ, наличие технической возможности для дальнейшего совершения преступлений или сокрытия следов преступной деятельности, особенности следовой информации, общественного мнения о произошедшем событии и пр.). Данная информация поможет руководителю объединенной следственной группы уточнить

криминалистические версии и внести необходимые коррективы в план расследования и следственного действия.

Факультативные - установление круга очевидцев происшествия и их «отработка», визуальное обследование объекта и поиск следов преступления (например, поиск нетипичной компьютерной техники), фиксация обнаруженных следов с возможным их изъятием (когда для этого не требуются специальные познания), принятие мер к сохранению потенциальных источников доказательств, осуществление мероприятий, связанных с проверкой поводов для возбуждения уголовных дел, а также иные действия.

В период времени, когда первая группа будет занята исполнением своих задач, у следователя будет возможность уточнить состав второй группы, особенно в части привлечения специалистов в конкретных, узких областях знаний, например, сетевых технологий, защиты информации, программирования и пр. Для более тщательного осмотра, в том числе дополнительного, а также проведения иных следственных действий, потребность в которых может возникнуть, следователь также сможет подготовить необходимую криминалистическую и специальную технику, например, программно-аппаратные средства для копирования компьютерной информации и средства личной безопасности.

Таким образом, предложенная форма выезда на осмотр места происшествия двух групп имеет следующие преимущества:

- экономию времени, связанного с подготовкой к выезду на место происшествия;
- оперативное прибытие на место происшествия;
- пресечение преступной деятельности и неблагоприятных ее последствий;
- охрану места происшествия и следов преступления;
- формирование более полной картины произошедшего события благодаря тому, что «старшим» первой группы будут докладываться криминалистически значимые сведения, которые некомпетентные лица могли бы не учесть, либо исказить.

Несмотря на положительные стороны выезда на осмотр места происшествия двух групп имеются также некоторые негативные моменты, среди которых можно выделить следующие:

- экономические, связанные с увеличенными материально-финансовыми расходами;
- кадровые – задействование дополнительного количества

личного состава структурных подразделений правоохранительных органов.

В ситуации, когда в ходе осмотра места происшествия имеется потребность в оперативном сопровождении, следователь привлекает сотрудников оперативно-розыскных органов. Ими может осуществляться не только снятие информации с технических каналов связи, получение компьютерной информации, оперативное обследование помещения, а также иные оперативно-розыскные мероприятия, но и осуществление наблюдения за нетипичным поведением каких-либо лиц, пресечение негативных последствий от эффекта «внезапности», препятствие сопротивлению задержанных и т.д.

В ситуациях производства осмотра места происшествия на основе оперативно-розыскных материалов необходимость в неотложности его проведения возникает реже. В отличие от «неотложного» осмотра уже на подготовительной стадии следователь может обладать некоторой проверенной информацией о преступлении, например, о количестве и характеристиках изымаемых объектов. На основании полученных сведений следователь определяется с количеством следственных групп и их составом. При этом на подготовительной стадии к осмотру места происшествия возникает потребность в конкретных организационных действиях, например, привлечения специалистов в определенных областях знаний. Специалисты могут помочь конкретизировать действия следователя по подготовке к осмотру. Осмотр места происшествия, проводимый по оперативно-розыскному материалу, имеет свои преимущества перед осмотром, проводимым в условиях неотложности, а именно, позволяет следователю:

- более детально спланировать проведение осмотра;
- выбрать удобное время для его проведения;
- затратить меньше времени (из-за поиска и фиксации, как правило, конкретной интересующей информации);
- включить в состав следственной группы оптимальное число участников (учитывая конкретные сведения из оперативно-розыскных материалов).

Отметим, что на организацию предварительной проверки по оперативно-розыскным материалам негативно влияет низкий уровень оснащенности специальными техническими средствами оперативных подразделений правоохранительных органов, затрудняющий

проведение ими мероприятий по данной категории преступлений. Так, для раскрытия компьютерных преступлений необходима современная криминалистическая техника, которая, как правило, находится в единичных экземплярах при централизованных управлениях (областного и федерального значения). Порядок ее использования сложен, а также неразрывно связан с проблемой очередности. Это увеличивает сроки ее получения в отдаленных районах. Помимо этого, истекшая или ограниченная годность лицензий на применение специальных программ и оборудования также негативно отражается на использовании современных криминалистической технически.

Предложенные организационно-тактические рекомендации получения судебных доказательств и иной криминалистически и оперативно значимой информации в различных следственных ситуациях могут оказать помощь в расследовании компьютерных преступлений, особенно по наиболее сложным и опасным их разновидностям, совершаемым высокотехнологичными способами.

Список использованных источников и литературы

1. Валов, С.В. О содержании понятия «организация расследования преступлений» / С.В. Валов // Вестник экономической безопасности, 2016. – № 1. – С. 38-41.

2. Варданян, А.В. Расследование преступлений в сфере высоких технологий и компьютерной информации / А.В. Варданян, Е.В. Никитина. - М.: Юрлитинформ, 2007. – 312 с.

3. Вехов, В.Б. Особенности организации и тактика осмотра места происшествия при расследовании преступлений в сфере компьютерной информации / В.Б. Вехов // Российский следователь. - 2004. – № 7. – С. 2-5.

4. Гаврилов, М.В. Осмотр при расследовании преступлений в сфере компьютерной информации / М.В. Гаврилов, А.Н. Иванов. - М.: Юрлитинформ, 2007. - 168 с.

5. Поляков, В.В. Особенности производства осмотра по компьютерным преступлениям / В.В. Поляков // Российский следователь. - 2017. - № 21. - С. 14-17.

6. Поляков, В.В. Этапы осмотра места происшествия по компьютерным преступлениям / В.В. Поляков // Закон и право. - 2016. - № 11. - С. 112-114.

7. Шевченко, Е.С. Актуальные проблемы расследования киберпреступлений / Е.С. Шевченко // Эксперт-криминалист. – 2015. – № 3. – С. 29–32.

ОСМОТР МЕСТА ПРОИСШЕСТВИЯ ПРИ ПРЕДВАРИТЕЛЬНОЙ ПРОВЕРКЕ СООБЩЕНИЙ О КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЯХ. II. ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ ПРОБЛЕМЫ[2]

В.В. Поляков, к.ю.н., доцент кафедры уголовного процесса и криминалистики Алтайского государственного университета
А.С. Никитин, следователь Славгородского межрайонного следственного отдела следственного управления Следственного комитета РФ по Алтайскому краю

Осмотр места происшествия, происходящий в ходе предварительной проверки сообщений о компьютерных преступлениях, помимо организационно-тактических вопросов проведения, имеет ряд теоретико-практических проблем, неразрешенность которых препятствует повышению эффективности правоприменительной практике при расследовании данных преступлений.

Дискуссионными остаются вопросы о возможности и степени вмешательства в личную жизнь граждан при производстве осмотра их жилища на этапе предварительной проверки поступившего сообщения о компьютерном преступлении. В ч. 2 ст. 176 УПК РФ говорится о том, что до возбуждения уголовного дела возможен осмотр места происшествия, документов и предметов, но об осмотре жилища, упоминаемого в части 1 данной статьи, речи не идет. Вероятно, это связано с появлением закономерных неудобств, а также возможных нарушений частной жизни или законных прав и интересов граждан, в жилище которых производится осмотр. Проблема заключается в том, что в ходе предварительной проверки сообщений о компьютерных преступлениях предполагается меньшая обоснованность необходимости производства осмотра в жилище граждан, чем в ходе возбужденного уголовного дела. Это же ведет к возможным злоупотреблениям со стороны следственных органов. Некоторыми учеными высказывается мнение, что на осмотр жилища во время проверки сообщения о преступлении должно в полной мере

[2] Публикация подготовлена в рамках поддержанного РГНФ научного проекта №16-33-01160.

распространяться правило о возможности его проведения в нетерпящих отлагательства и иных исключительных случаях до возбуждения уголовного дела на основании постановления следователя без получения судебного решения, с последующим уведомлением судьи и прокурора [9, с. 14]. Принимая во внимание особую значимость первичного осмотра места происшествия, на наш взгляд, необходимо дополнить содержание ч. 2 ст. 176 УПК РФ осмотром жилища, разрешив его производство до возбуждения уголовного дела в исключительных случаях.

Суду при проверке законности осмотра жилища на этапе предварительной проверки, на наш взгляд, следует уделять особое внимание обстоятельствам, из числа так называемых «нетерпящих отлагательств». К последним следует отнести: категорию состава преступления, по которому проводится проверка; роль лица, в жилище которого проводился осмотр; степень его причастности к произошедшему событию; сложность материала проверки; время проведения осмотра и др. Учитывая специфику преступлений, совершаемых в сфере компьютерной информации, их, зачастую, можно относить к категории особо сложных, что должно учитываться судом при проверке законности произведенного осмотра жилища. Отсюда следует, что следователю целесообразно при вынесении постановления о производстве осмотра в жилище ссылаться на вышеперечисленные обстоятельства.

Как показывает практика, фактически необходимость в осмотре всего жилища в ходе предварительной проверки сообщений о компьютерных преступлениях не всегда существует. Зачастую, основная криминалистически значимая информация, которая подлежит проверке, находится в средствах компьютерной техники и носителях информации, то есть в «виртуальном пространстве». В связи с этим иногда возможно ограничиться осмотром конкретных предметов компьютерной техники и документов, которые содержат криминалистически значимую информации [2]. Однако сделать это, при нежелании сотрудничества со следствием владельцев таких предметов, бывает практически невозможно. Для получения доступа к таким предметам потребуется физически к ним добраться, то есть проследовать по жилищу в соответствующие комнаты, где они находятся. В настоящее время законно сделать это можно только путем производства осмотра жилища. В противном случае не ясно будет откуда в уголовном деле появились осматриваемые предметы,

возникнет вопрос о том, что их могли подбросить и т.п. Осмотр не всего помещения, а только тех комнат, в которых находятся предметы компьютерной техники, представляется не имеющим особой целесообразности. Таким образом, не гибкость законодательства может приводить к необоснованному вмешательству в личную жизнь граждан в тех случаях, когда этого можно было бы избежать.

Сложность вызывает вопрос о «глубине» осмотра места происшествия, средств компьютерной техники и электронных документов. Это связано с пограничным характером осмотра с иными следственными действиями, например, обыском, экспертизой. Так, например, при осмотре запущенных в операционной системе процессов или лог-файлов, свидетельствующих о произошедших действиях, описании программного обеспечения, установленного на средства компьютерной техники, достаточно просто перейти к поисковой направленности своих действий, тем самым совершить ошибку, связанную с подменой одного следственного действия другим, а именно – обыском [6]. На наш взгляд, объективно установить границу осмотра и обыска при работе с компьютерной информацией достаточно сложно. Этому вопросу необходимо уделить отдельное уголовно-процессуальное и криминалистическое внимание. На практике это означает, что лучше дополнительно после осмотра провести обыск, либо сразу его избрать единственной процессуальной формой производимых действий. Похожей позиции придерживается Р.И. Оконенко. По его мнению, исследование компьютера необходимо осуществлять в форме обыска и только на основании судебного решения [5], что делает невозможным проведение этих действий в рамках доследственной проверки [3].

На практике нередко возникает вопрос о том, как поступить с выявленными в обстановке места происшествия следами компьютерных преступлений [8]. Полагаем, что в тех случаях, когда осмотр компьютерной информации требует продолжительного времени, а также может быть рискованным или затрудненным в конкретных условиях места и времени, следы преступления сначала подлежат фиксации и изъятию, а в последующем должны быть детально осмотрены в качестве предметов или иных документов. Так, после прибытия на место происшествия следственной группы следователю совместно со специалистом следует выявить предметы, риск утраты которых по истечению времени будет наиболее велик, и приступить к фиксации последних незамедлительно. Обратим

внимание, что фиксация объектов, их изъятие и составление протокола следственного действия по времени могут не совпадать, поэтому следователю необходимо изначально заняться обнаружением, фиксацией и изъятием объектов, представляющих наибольший интерес, и лишь после этого приступать к составлению протокола осмотра места происшествия.

Анализ судебно-следственной практики выявил проблему необходимости осмотра закрытой от публичного доступа компьютерной информации, находящейся на удаленных ресурсах (например, в социальных сетях, мессенджерах, электронной почте, облачных хранилищах), когда следствию не оказывается требуемое содействие. В таких случаях следователю стоит собрать информацию, находящуюся в общем доступе, постараться получить объяснения от собственников и пользователей данных ресурсов. Далее, необходимо истребовать и изъять документы, которые могут способствовать получению идентификационных данных и иных искомых сведений, и назначать по ним соответствующие исследования. Также необходимо направить поручения о производстве оперативно-розыскных мероприятий, позволяющих установить и проверить конкретные сведения. Как показывает практика, результат усилий по разрешению описанной проблемы редко приводит к получению судебных доказательств, чаще позволяя получить только ориентирующую информацию. В тех случаях, когда удается получить согласия собственников удаленных ресурсов, например, на открытие доступа к их профилям в социальных сетях, где содержатся переписка и иная личная информация, на наш взгляд, целесообразно на законодательном уровне разрешить «упрощенный» (т.е. несудебный) порядок получения таких сведений, которые позволят включить их в проводимые проверочные действия.

При обнаружении вероятно относящихся к преступлению каких-либо программно-аппаратных средств (телефонов, компьютеров, онлайн-сервисов и др.), следует установить их владельцев. Им необходимо разъяснить по каким причинам обнаруженное имеет интерес для следствия, и постараться получить согласие на проведение осмотра. В случае, когда получен необоснованный отказ владельцев программно-аппаратных средств, представить их на осмотр, это фиксируется следователем в протоколе, после чего данные предметы осматриваются и подлежат изъятию принудительно. В отдельных случаях, например, во избежание огласки

полученных сведений, содержащихся в изымаемых программно-аппаратных средствах, их осмотр на месте происшествия проводить не следует, так как на этапе проверки сообщений о преступлениях отсутствует запрет, аналогичный разглашению данных на предварительном расследовании (ст. 161 УПК РФ).

Следует отметить, что в настоящее время законодательно не регламентирован порядок осмотра компьютерной информации, хранящейся на изъятых программно-аппаратных средствах, тем более, что там может содержаться информация о частной жизни, личной или семейной тайне, электронная переписка и иные личные сообщения. Судебная практика в таких случаях обычно признает действия следователя незаконными, ссылаясь на нарушение прав граждан на частную жизнь, что ведет к исключению полученных в ходе осмотра доказательств [1, 4]. На наш взгляд, одним из путей разрешения данной ситуации является внесение дополнений в федеральное законодательство, заключающееся в необходимости получения судебных санкций на осмотр программно-аппаратных средств. Однако эта процедура применима лишь на стадии предварительного следствия, что ограничивает возможности проверки сообщений о преступлениях [7].

Полагаем, что разработка криминалистических рекомендаций по предварительной проверке сообщений о компьютерных преступлений осложняется большим количеством правовых пробелов и коллизий, возникших вследствие отсутствия специальных норм в уголовно-процессуальном законодательстве, а также устоявшейся практики правоприменения. В связи с этим данная тема сохраняет свою актуальность и требует комплексного подхода к ее дальнейшему исследованию.

Список использованных источников и литературы

1. Апелляционное определение Саратовского областного суда № 22К-2932 от 24.07.2013 // Rospravosudie.com – URL: https://rospravosudie.com/court-saratovskij-oblastnoj-sud-saratovskaya-oblast-s/act-473138560/

2. Иванов, И.И. Организация обыска и осмотра компьютерной техники с участием специалиста / И.И. Иванов, А.А. Нигоева // Проблемы организации расследования преступлений: материалы всерос. науч.-практ.конф., Краснодар, 21–22 сент. 2006 г. – Краснодар, 2006. – С. 116–121.

3. Калиновский, С.Б. «Доследственный» обыск – незаконное ноу-хау // Уголовный процесс. – 2015. – № 1. – С. 9–12.

4. Кассационное определение Омского областного суда № 22К-2225/12 от 24.05.2012 г. по делу № 22-2225/12 // Rospravosudie.com – URL: https://rospravosudie.com/court-omskij-oblastnoj-sud-omskaya-oblast-s/act-476337125/

5. Окоменко, Р.И. К вопросу о правомерности осмотра компьютера как следственного действия / Р.И. Окоменко //Адвокат. - 2015. - № 1. - С. 27 – 30.

6. Поляков, В.В. Особенности производства осмотра по компьютерным преступлениям / В.В. Поляков // Российский следователь. - 2017. - № 21. - С. 14-17.

7. Постановление Пленума Верховного суда РФ от 24.12.1993 № 13 (ред. от 06.02.2007) «О некоторых вопросах, связанных с применением статей 23 и 25 Конституции Российской Федерации» // Sudact.ru – URL: http://sudact.ru/law/postanovlenie-plenuma-verkhovnogo-suda-rf-ot-24121993.

8. Романенко, М.А. Следственный осмотр по делам о преступных нарушениях авторских прав в сфере программного обеспечения / М.А. Романенко // Вестник Омского университета. Серия «Право». - 2008. - № 1 (14). - С. 171–175.

9. Ряполова, Я.П. Процессуальные действия, проводимые в стадии возбуждения уголовного дела: автореф. дис. … канд. юрид. наук.: 12.00.09 / Я.П. Ряполова. - Москва, 2013. – 28 с.

СПЕЦИФИКА ПРОИЗВОДСТВА ОСМОТРА ПО КОМПЬЮТЕРНЫМ ПРЕСТУПЛЕНИЯМ

Л.Г. Суханова, ассистент кафедры уголовного процесса и криминалистики Алтайского государственного университета
Л.В. Гребенщикова, Алтайский государственный университет

Развитие компьютерных технологий сопровождается ростом компьютерной преступности и, что еще более важно, ее качественным изменением. Преступления совершаются более изощренными способами с применением специальных программно-аппаратных средств и сетевых технологий [1, с. 124].

Для квалифицированной борьбы с компьютерной преступностью создано специализированное подразделение - Управление «К» БСТМ МВД России, которое помогает в сложных ситуациях выявления, расследования и пресечения фактов совершения компьютерных преступлений. По словам начальника БСТМ МВД России генерал-майора полиции А. Мошкова, в сфере компьютерной преступности существует две устойчивые тенденции. Первая связана с преступлениями, совершаемыми профессионалами, которые создают мощные вирусные программы, способные парализовать работу целых предприятий и организаций. Вторая группа - это мошенники, размещающие в интернете объявления о продаже оптом товара по низким ценам. Ранее компьютерные преступления в основном совершались лицами, обладающими определенным уровнем специальных познаний в сфере высоких технологий, то в настоящее время, в связи с появлением в сети Интернет программ, предназначенных для несанкционируемого доступа к информации и инструкций к ним, их может осуществить обычный пользователь. Изменения, происходящие в киберпреступности во многом обуславливают необходимость совершенствования криминалистических приемов борьбы с ними в рамках следственных действий. Это в первую очередь касается наиболее распространенных следственных действий по данной категории преступлений – следственных осмотров.

В связи с актуальностью данной проблемы, считаем целесообразным рассмотреть процессуальные и криминалистические аспекты проведения осмотра как следственного действия по компьютерным преступлениям.

В ходе осмотра складываются несколько типичных следственных ситуаций: осмотр места происшествия; осмотр места, откуда был произведен неправомерный доступ; осмотр компьютерного оборудования, изъятого в ходе других следственных действий.

Для получения необходимых сведений по уголовным делам, которые послужат в дальнейшем доказательствами, необходимо предварительно тщательно подготовиться к проведению следственного действия. Не любые сведения, полученные следователям, приобретут силу доказательств, для этого их необходимо оценить с точки зрения относимости, допустимости, достоверности.

В правоприменительной практике встречаются проблемные ситуации, когда интересующая следствия информация является труднодоступной для осмотра. В данном случае помощь могут оказать специалисты, обладающие специальными познаниями в области компьютерной информации. Считаем, что следователь также должен обладать вышеуказанными знаниями, в частности, достаточными для правильного выявления, изъятия, фиксации доказательств по компьютерным преступлениям. В практической деятельности встречаются следователи, которые имеют помимо юридического образование в области технического и информационного обеспечения, что существенного повышает эффективность производства следственных действий.

В криминалистической литературе высказывается ряд рекомендаций для проведения вышеуказанного следственного действия, такие как обеспечение участия соответствующих специалистов в области компьютерной техники, инструктаж членов следственно-оперативной группы, обеспечение участия понятых, обладающих познаниями в области компьютерной техники и технологий [2, с. 70].

Поскольку следователь выезжает на место осмотра в составе следственно-оперативной группы, оперативники обладают процессуальным статусом, который предполагает наличие субъективных прав и обязанностей при участии в следственном действии [3, с. 113]. В обязанности оперативного сотрудника подразделения, занимающегося борьбой с преступлениями в сфере высоких технологий, входит оказание помощи следователю в производстве осмотра места происшествия, выполнение его поручений и проведение розыскных мероприятий [4, с. 255]. Им осуществляются

опросы граждан с целью выявления свидетелей, получения иной информации важной для установления личности преступника, розыска похищенной информации; координация действий следственно-оперативной группы и других оперативных сотрудников, параллельно осуществляющих оперативно-розыскные мероприятия и другие поручения, которые ему укажет следователь. Некоторыми учеными высказывается мысль о необходимости указания факта обладания у понятых специальных познаний в области компьютерной техники и информации. С этим доводом можно не согласиться, поскольку уголовно-процессуальный кодекс императивно устанавливает участие понятых только в конкретных составах преступлений, закрепленных в ч.1 ст. 170 УПК РФ. Из этого следует, что у следователя, дознавателя есть выбор варианта поведения, который регламентирован статьей 170 УПК РФ, а именно – существует альтернатива участию понятых - в случае производства следственного действия без участия понятых применяются технические средства фиксации его хода и результатов.

На наш взгляд, участие понятых служит фикцией доказательств, устанавливает некую презумпцию достоверности результатов проведенного следственного действия. Если следователю заблаговременно обеспечить участие понятого, обладающего специальными знаниями, это будет дублированием полномочий по привлечению специалиста, которому следователю также нужно привлечь. Задаемся вопросом, зачем усложнять задачу следователя по приискании «специального» понятого, когда перед указанным следственным действием ему нужно совершить и иные подготовительные мероприятия, включая поиск обычных понятых? Необходимо учитывать, что у следователя в производстве достаточно дел, и перед ним стоит множество процессуальных задач для разрешения, соответственно нужно выбирать более экономически-затратный вариант его поведения.

Обобщая предлагаемые в научной литературе рекомендации по производству следственного осмотра по делам о преступлениях в сфере компьютерной информации, выделим следующие моменты, имеющие принципиальное значение: в ходе производства следственного действия следователь должен запретить прикасаться к компьютерному оборудованию, находящемуся в месте осмотра всем, кроме специалиста; заранее подготовить технические носители для копирование интересующей следствие, упаковать изъятые объекты следует способом, исключающим их повреждение [5, с. 46].

При проведении осмотра в порядке ст. 144-145 УПК РФ участники еще не обладают процессуальным статусом, соответственно не имеют прав и обязанностей, и не могут нести ответственность в соответствии с законодательством РФ [6, с. 16]. Поэтому считаем, что следователь при производстве следственных и процессуальных действий до возбуждения уголовного дела по компьютерным преступлениям должен быть предельно внимательным в целях сохранения информации полученной в ходе вышеуказанных действий, поскольку восстановить данные сведения в будущем не представится возможным.

Список использованных источников и литературы

1. Поляков В.В. Характеристика высокотехнологичных способов совершения преступлений в сфере компьютерной информации: матер. ежег. Всерос. науч.- практ. конф., посвященной 50-летию юридического факультета и 40-летию Алтайского государственного университета «Уголовно-процессуальные и криминалистические чтения на Алтае». - Барнаул: Изд-во Алт. ун-та, 2012. -Вып. 11-12. - С. 123-126.

2. Поляков, В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации : дис. ... канд. юрид. наук: 12.00.09 / В.В. Поляков. – Омск, 2008. – С. 70.

3.Поляков, В.В. Этапы осмотра места происшествия по компьютерным преступлениям / В.В. Поляков // Закон и право. - 2016. - № 11. - С. 112-114

4. Никитин, А.С. Некоторые вопросы, связанные с изъятием компьютерной информации в рамках доследственной проверки / А.С. Никитин, В.В. Поляков // Проблемы правовой и технической защиты информации. Выпуск IV / Сборник научных статей. - Барнаул: Изд-во Новый формат, 2016. – С. 254-259.

5. Степанов-Егиянц В.Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями // Российский следователь. - 2012. - № 24. - С. 43-46

6. Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: автореф. дис. ... д-ра юрид. наук. М., 2006. С. 16.

КИБЕРПРЕСТУПНОСТЬ: ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ ОЦЕНКИ И ОРГАНИЗАЦИИ ПРОТИВОДЕЙСТВИЯ

А.В. Рыженкова, Юго-Западный государственный университет
Я.П. Ряполова, к.ю.н., доцент кафедры уголовного процесса и криминалистики Юго-Западного государственного университета

Парадокс развития человечества заключается в том, что во все исторические периоды люди накапливали, передавали, запоминали и использовали информацию, общались посредством нее. Процесс информатизации, по своей природе, непрерывно охватывает все сферы жизни: в политической регулирует отношения национальной безопасности, международные конфликты; в социальной повышает уровень здравоохранения и образование; в экономической борется с безработицей, управляет финансовой деятельностью государства; в духовной же способствует межличностному общению, окультуриванию индивидов. В современном мире, где такие понятия как глобализация, всеобщая интеграция и бурное развитие компьютерных технологий, неразрывно сосуществуют в обществе, на рубеже xx века, с момента создания первой ЭВМ, появилось понятие «киберпреступность». С 1990 года всемирная паутина интернета стала распространяться по планете с огромной скоростью.

Жизнь большинства современных людей незаметно все более и более переходит в виртуальную реальность. Социальные сети дают широкие возможности для новых знакомств, для общения с людьми из других стран, с которыми можно обмениваться культурным, историческим опытом, учить иностранные языки, в конце концов, из интернета, мы регулярно черпаем множество интересующей нас информации и новостей. Ежегодно число киберпреступлений растет, а способы и методы их совершения становятся более профессиональными, вследствие чего несут угрозы не только гражданам и юридическим лицам, но также опасны для отдельных государств и для мирового сообщества в целом. Даже несколько хорошо обученных преступников могут поставить в опасность все мировое сообщество, а субъектный состав жертв достаточно разноплановый: от среднестатистического гражданина до государства в лице его государственных органов в целом. Специалисты в области информационной безопасности отмечают буквально лавинообразный

рост киберпреступности, причем связанный не только с внешними атаками, но и с внутренними факторами, поэтому в связи с такой неспокойной виртуальной обстановкой, в обиход входит термин «кибертеррор».

Согласно ежегодному докладу Центра по борьбе с преступлениями в сети Интернет (ICCC), совокупный ущерб от киберпреступлений в 2015 г. достиг уровня 495,3 млн. долларов, а средний ущерб в расчете на одно преступление составил 6700 долларов [2, с. 134]. По данным некоторых научных деятелей, ущерб от мировой киберпреступности в 2016 году составил приблизительно 600 миллиардов долларов, что составляет процент мирового ВВП. В то время, как раскрывается менее 3-4 % киберпреступлений, их размах ежедневно увеличивается. По оценкам Сбербанка, в 2017 году ущерб мировой экономики от участившихся кибератак может перевалить за 1 трлн. долларов, а через три года - вырасти до 2 трлн долларов, в свою очередь, моровой оборот наркоторговли составляет 500 млрд. долларов в год [2, с.351].

Киберпреступность - это одна из главных проблем 21 века, которая имеет ряд своих особенностей. Например, максимальная скрытность деяний, которая заключается в анонимности любых действий, в использовании анонимайзеров. Также к особенностям данного феномена относят гигантские расстояния между жертвой и преступником и нестандартность действий преступников, ведь киберпреступления и их последствия невозможно предугадать (хакеры могут разрабатывать программы, которые без помощи создателя могут снимать деньги с банковских карт). Конечно, правоохранительные органы, в лице спецслужб, могут определить местонахождения преступника по его IP- адресу, однако же, при использовании человеком специальных шифровальных программ, это сделать практически невозможно.

На сегодняшний день есть страны - лидеры по числу кибератак, это Китай, Россия и США. Так как представленные страны имеют достаточно большую территорию, зачастую невозможно достаточно эффективно скоординировать действия спецслужб через пределы юрисдикций государственных границ и через многообразие законодательной базы стран. Думается, что только на основе межгосударственного сотрудничества, возможно создание новых, специфических механизмов выявления киберпреступности, ее расследования и пресечения. Скорее всего, этими новыми

механизмами должны стать новейшие компьютерные технологии, которые будут устойчивыми к кибератакам. В настоящее время, в большинстве стран (в том числе и в России) нет законодательства, которое бы регулировало борьбу с информационными преступлениями и отвечало бы современным реалиям правоприменения.

Глава 28 УК РФ посвящена преступлениям в сфере компьютерной информации. Составы данных преступлений носят материальный характер и предполагают наступление таких последствий как: уничтожение информации, ее блокирование, переработка, внесение изменений, перенос информации на другой электронный носитель. Все это впоследствии должно привести к нарушению работы компьютера или отельных его программ. Субъективная сторона всегда характеризуется умышленной формой вины, то есть преступник знает, какие последствия в дальнейшем должны наступить и все- таки сознательно идет на преступление. Что же касается санкций за данное деяние, то они альтернативно предусматривают штрафы, исправительные работы и лишение свободы, это зависит от характера совершенного преступления и его последствий. Однако, ни в кодексе, ни в комментариях к нему, ни в какой либо иной законодательной базе РФ, применение электронных информационно-коммуникационных способов и средств сбора, накопления и распространения электронной информации широкого отражения не получили. Также в УК не отражены такие понятия как фишинг, скимминг и прочие важные термины в области киберпреступлений. Первое - это вид интернет - мошенничества, целью которого является получение доступа к средствам аутентификации клиента, конфиденциальным данным пользователей — логинам и паролям учетной записи. Второе понятие включает в себя вид мошенничества, в ходе которого злоумышленником производится скрытая от держателя банковской карты операция с использованием самой карты, ее реквизитов. Иными словами, скиммер это определенная накладка, которая при установлении на картоприемник, может считывать с банковской карты любую информацию. Так, в 2011 году с данным явлением столкнулись многие клиенты банка «ВТБ-24», а в дальнейшем жертвами скримминга стали клиенты «Альфа - банка». С электронных карт обладателей были списаны денежные средства, и данная операция в 2011 году коснулась более 75% работников «2ГИС», у которых зарплата перечислялась на карты «ВТБ-24» [1, с. 35].

Некоторые специалисты спецслужб считают необходимым и возможным внесение исправлений в Уголовный кодекс РФ с целью ввести отдельный состав об уголовной ответственности за проведение DDoS-атак. Данные хакерские атаки ставят перед собой цель создать для компьютерной системы такие условия, при которых пользователи не смогут получить доступа к серверам, то есть доступ к сайтам и к любой информации будет затруднен. Такие атаки являются вредоносными и несут серьезную опасность для эффективной работы с электронной инфраструктурой, поэтому следует считать разумным введение и ужесточение санкций за создание такого плана вредоносных программ.

С каждым годом профессионализм хакеров возрастает и киберпреступления становятся серьезной проблемой государственной важности. Киберпреступность превратилась в некий выгодный, циничный, скрытный бизнес, доходы от которого превышают доходы от торговли оружием или наркотиками [1, с. 67]. По данным Group-IB, финансовые показатели оборота мирового рынка компьютерной преступности в 2012 году составили 12,5 млрд. долларов, для сравнения, к 2015 году показатели возросли более чем в 2 раза. На долю русских хакеров пришлось 4,5 млрд. долларов, из них 2,3 млрд. долларов составляют доходы от киберпреступлений, совершенных непосредственно на территории Российской Федерации. Это такие преступления как спам, обналичивание денежных средств, хищение электронных денег и другое. В расследовании возникают проблемы обнаружения и предотвращения информации о совершенном преступлении, так как многие предприятия и организации не заинтересованы в огласке данного события и в потере репутации и клиентской базы, поэтому проблема сокрытия фактов - важнейшая проблема на сегодняшний день.

Необходимо отметить, что важнейшим фактором стремительной эволюции и развития преступлений в области информационных технологий является несовершенная юридическая база в сфере преследования хакеров в правовом поле, потому как в уголовном и уголовно - процессуальном кодексе нет квалификации и составов киберпреступлений. Это дает преступникам ощущение своеобразной защищенности и безнаказанности. Так как на сегодняшний день судебная и правоприменительная практика не достаточно широка и совершенна, подобные инциденты зачастую скрываются, и это дополнительно стимулирует совершения такого рода преступлений.

Чтобы предупреждать кибератаки, а впоследствии и совершения киберпреступлений, правоохранительным органам и спецслужбам необходимо расширять теоретические и практические знания в области разбора, реагирование и предотвращения инцидентов в области информационной безопасности, этим должны заниматься высококвалифицированные специалисты.

Существует система основных этапов расследования киберпреступлений: для начала спецслужбами должен быть установлен факт неправомерного доступа и проникновения в чужую компьютерную систему, далее специалисты должны установить время совершения преступления, способ несанкционированного доступа к сети, установить круг подозреваемых и определить их виновность, цели и мотивы, далее требуется заняться сбором доказательной базы и выявить обстоятельства, способствующие преступлению. Последним этапом считается факт установления вредных последствий и разработка и предоставление рекомендаций по минимизации рисков.

Естественно, рядовые сотрудники полиции по своему роду деятельности не обладают должными знаниями в сфере компьютерных технологий, поэтому не имеют возможности и навыков для борьбы с киберпреступниками. Поэтому для борьбы с преступлениями в IT-сфере, было создано специальное подразделение МВД «Отдел К». В число его задач входит: обнаружение проникновения в компьютерные базы и списание средств с банковских карточек пользователей, борьба с нарушением авторских прав, борьба с распространением порнографии в интернете и через съемные носители. Но полную информацию об этом подразделении обычным гражданам найти невозможно, потому что многие данные засекречены. Однако есть сведения о том, что в нём трудятся бывшие «хакеры», которые решили встать на сторону закона и помогать властям бороться с такими же, как они [3, с. 57].

Чем же обусловлены сложности расследования? Одна из сложностей заключается в определение состава, места и времени преступления, к тому же вычислить преступника зачастую тоже бывает максимально сложно. Ряд исследователей определили круг причин, из-за которых раскрыть киберпреступления намного сложнее, чем преступления реальные, а не виртуальные. Довольно часто спецслужбы оказываются в ситуации, когда даже факт совершения преступления остается незамеченным, его сложно установить. Преступник может получать любую, скрытую интересующую его

информацию и об это не узнают, по крайней мере, пока не обнаружат утечку информации, здесь стоит говорить о латентности преступных деяний.

Также преступления в сети могут быть крайне масштабными. Условный студент, хорошо разбирающийся в программах и имеющий навыки в хакерской деятельности, может взломать базу данных, проникнуть в секретные архивы и ведь совершение данного деяния подвластно одному человеку.

Среди причин, обуславливающих сложности расследования, выделяют транснациональную составляющую. Она проявляется в том, преступник и потерпевший могут находиться в разных точках мира и в данном аспекте глобализация рассматривается как отрицательный фактор, который несет лишь отрицательное влияние. Хакеры, как правило, обладают достаточно высоким интеллектом, их действия и ходы зачастую невозможно предугадать, поэтому стоит говорить, в определенной стезе, об их высокой образованности.

На практике в уголовных делах обязательным этапом следствия является составление сотрудником правоохранительного органа при помощи и участии психолога приблизительного образа преступника, и зачастую данные фотороботы оказываются верными по характеристикам потерпевшего. Что же касается ситуаций с киберпреступлениями, то нарушителям может быть абсолютно любой человек, которого никак нельзя охарактеризовать по гендерному признаку, описать его черты лица, манеру поведения, одежду и прочее.

На сегодняшний день, существует важная проблема, напрямую связанная с эффективностью расследования и доведению до суда дел о киберпреступлениях. Это общественное мнение, которое не думает о серьезных последствиях данной категории преступлений, потому что люди уверены, что компьютерные преступники, даже если расследование доведено до конца и вынесен приговор суда, отделываются легкими наказаниями, зачастую - условными приговорами. Отсюда возникает понятие правового нигилизма и у преступников и у потерпевших, так как первые осознают свою относительную безнаказанность, а вторые даже не хотят обращаться в правоохранительные органы, дабы заявить о несанкционированном деянии, будучи уверенными, что должного и разумного наказания для преступников они не добьются. И на самом деле такое поведение потерпевших обоснованно, ведь в современном обществе практически

отсутствует законодательная база, которая бы регулировала процессуальные действия по киберпреступлениям.

Подводя итог вышеизложенному, хочется отметить, что социум еще не привык и не успел подготовиться к такого рода преступлениям как киберпреступления, ведь это относительно новый вид незаконных деяний. Думается, что необходимо дополнительное обучение всех категорий юристов современным информационным технологиям не только как продвинутых пользователей офисных программ, а как лиц, осведомленных в стандартах и новациях IT в целом, особенно осведомленных в юридических аспектах обеспечения функционирования IT. Чтобы бороться с киберпреступлениями, нужно создавать и совершенствовать эффективную и грамотную законодательную базу, ведь именно правильно применяя закон, можно вынести справедливое решение.

Список использованных источников и литературы

1. Клаверов В.Б. Современная киберпреступность. Характеристика и подробный анализ. – М: Саарбрюккен: Саарбрюккен: LAP LAMBERT Academic Publishing, 2012. – 92 с.

2. Злоченко Я.М. Методика расследования. – М: LAP Lambert Academic Publishing, 2012. - 632 с.

3. Сотов, А.И. Компьютерная информация под защитой. Правовое криминалистическое обеспечение безопасности компьютерной информации : монография / А.И. Сотов. — М. : Издательство «Русайнс», 2015. – 204 с.

КИБЕРПРЕСТУПНОСТЬ В СОВРЕМЕННОМ МИРЕ: ПОНЯТИЕ И ПРОБЛЕМЫ РАССЛЕДОВАНИЯ

Я.П. Ряполова, к.ю.н., доцент кафедры уголовного процесса и криминалистики Юго-Западного государственного университета

В XXI веке технологии стремительно развиваются и выходят на более высокий уровень. В связи с этим появляются новые виды преступлений, именуемые «киберпреступлениями». Не существует однозначного определения данного понятия. Во многих источниках под киберпреступлениями понимают: «компьютерные преступления», «преступления в сфере высоких технологий», «информационные преступления», собственно «киберпреступления», «преступления в сфере безопасности обращения компьютерной информации», «преступления в сфере компьютерной информации» и т.д. Данный перечень весьма широк, но общее определение киберпреступности закреплено в Конвенции о преступности в сфере компьютерной информации ETS № 185 Совета Европы от 23.11.2001 г. [1, с. 187].

Киберпреступность в узком смысле – это противоправные деяния, совершаемые посредством электронных операций, с нарушением обеспечения безопасности компьютерных систем и обрабатываемых ими данных. К данному определению относят компьютерные преступления.

Киберпреступность в широком смысле – любые противоправные деяния, совершаемые посредствам или связанные с компьютерами, компьютерными сетями или системами, включая незаконное предложение и владение или распространение информации посредством компьютерных сетей или систем. К данному определению относят преступления, связанные с компьютерами.

Киберпреступность является проблемой не только в Российской Федерации, это общепризнанная проблема мирового сообщества. Сейчас, когда огромная часть жизни личности, общества и государства механизирована, степень вреда от данных преступлений значительно возросла. Но расследование таких преступлений является весьма затруднительным по ряду причин: во-первых, сеть интернета является мировой, что приводит к тому, что расследование таких преступлений происходит на международном уровне, нежели в пределах конкретного государства, так как такие киберпреступность охватывает весь мир и лица, совершившие преступления, могут находиться в

разных точках земного шара, что приводит к проблеме их задержания и привлечения к ответственности за совершенные деяния. К тому же возникает проблема назначения компьютерно-технической экспертизы в отношении серверов, которые находятся на территории другого государства, откуда было совершено преступление.

Упомянутая Конвенция определила основные направления в борьбе с преступностью в сфере высоких технологий. В первую очередь, должно быть произойти согласование государствами-участниками национальных уголовно-правовых норм, связанных с преступлениями в киберпространстве, разработка процессуального законодательства, необходимого для расследования таких преступлений и судебного преследования лиц, их совершивших, а также сбора доказательств, находящихся в электронной форме; обеспечение быстрого и эффективного режима международного сотрудничества в данной области [2, с. 94]. То есть выдвинуты реальные задачи для реализации на уровне национального законодательства, которые необходимы для эффективной борьбы с такого рода преступлениями. Конвенция была подписана Российской Федерацией, однако не была ратифицирована. Но на ее основании можно составить определенную стратегию в развитии борьбы с киберпреступностью в рамках нашего государства.

В рамках ООН был рассмотрен вопрос о преступлениях в сфере компьютерных технологий в рамках проекта конвенции «О сотрудничестве в сфере противодействия информационной преступности». Было принято решение о том, что национальное законодательство государств-участников нуждается в обновлении в соответствии с появлением такого преступления. Также было сказано о том, что расследование данных преступлений требует определенных знаний в IT-сфере, к тому же следователям, если говорить непосредственно о РФ, следует выработать новую тактику борьбы с преступлениями такого рода. Ввиду этого, 24 июля 2013г. Президентом Российской Федерации утверждены Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года [3, с. 13]. Российская Федерация делает определенные шаги для борьбы с киберпреступностью на национальном уровне, однако на это потребуется несколько лет.

Следует, однако, учитывать разницу между понятием «преступления в сфере компьютерной информации» и «преступления,

совершаемые с использованием высоких технологий». Ответственность за первые предусмотрена главой 28 УК РФ, которая содержит три состава – неправомерный доступ к компьютерной информации (ст. 272); создание, использование и распространение вредоносных компьютерных программ (ст. 273); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274). Понятие «преступления, совершаемые с использованием высоких технологий» – собирательное, употребляется в тех случаях, когда для совершения традиционных преступлений используются информационные технологии. Ответственность за деяния такого рода предусматривается статьями из различных глав УК РФ, например, 159.3 (мошенничество с использованием платежных карт), 159.6 (мошенничество в сфере компьютерной информации), 146 (нарушение авторских и смежных прав при незаконном использовании программных продуктов), 187 (изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов с использованием средств компьютерной техники) и т.п.

Выделяют также ряд и других проблем, связанных с расследованием киберпреступлений. Высокая латентность преступлений в сети интернет, сложность сбора доказательств и появление так называемого «виртуального» или «информационного следа», однако в криминалистике существуют споры относительно существования и признания такого следа как доказательства, отсутствие судебной и следственной практики – все это является проблемой для раскрытия преступлений в сфере информационных технологий. Еще одной проблемой является высокая квалификация преступников, которые не оставляют после себя практически никаких следов, порой жертва такого преступления даже не подозревает о совершении такового. Факт совершения преступления обнаруживается ими многим позже. К тому же необходимо сказать, что большинство киберпреступников, хакеров продолжают развивать свою деятельность, зная о том, что в законодательстве существуют определенные пробелы, с помощью которых можно предпринимать попытки обходить законы и избегать ответственности [4, с. 161]. Так же следует отметить такую проблему как неопределенный круг потерпевших при совершении данного преступления. Не всегда можно четко определить круг лиц, которые стали жертвами

киберпреступлений ввиду того, что многие граждане не афишируют того факта, что стали жертвами преступления. Еще одной проблемой можно считать постоянное перемещение преступника по территории как одного, так и многих государств, в то же время как отследить его след крайне необходимо для следствия и привлечения лица к ответственности.

Круг проблем весьма широк и разнообразен как с точки зрения национального права, так и с точки зрения международного права. Вместе с тем необходимо полностью создать базу расследования таких преступлений на уровне следователей и дознавателей. Сотрудники оперативных подразделений органов внутренних дел не имеют достаточных знаний в этой области, что приводит к утрате следов совершения хищений, к неэффективному использованию оперативно значимой информации, полученной в ходе проведения оперативно-технических мероприятий [5, с. 44]. Деятельность экспертно-криминалистических подразделений МВД РФ не отвечает требованиям в расследовании такого рода преступлений, так как сроки проведения экспертизы, касающихся информационных технологий, являются достаточно длинными. Все эти обстоятельства находятся в прямой и непосредственной связи с результатами деятельности органов предварительного следствия в системе МВД России.

Также говоря о киберпреступности, необходимо учитывать степень незащищенности данных правоохранительных органов, которые так же могут подвергнуться атаке хакеров. Важнейшим аспектом внедрения информационных технологий становится построение на их основе деятельности правоохранительных структур. В ситуации, когда преступные сообщества располагают современной техникой, привлекают к работе высококвалифицированных хакеров, неизмеримо повышаются требования к защите служебной информации. Необходимость защиты от посягательств, а также своевременной реакции оперативного восстановления данных побуждают создавать специальные отделы, занимающиеся вопросами информационной безопасности и защиты информации. [6, с. 15]. В ряде зарубежных стран созданы специальные отделы для борьбы с киберпреступностью, созданием и методикой расследования таких преступлений и пресечения их, что, впрочем, является достаточно трудным, учитывая специфику данного преступления.

Следует отметить позицию А. Г. Волеводза, который считает, что расследование преступлений в информационных сетях обычно

требует быстрого анализа и сохранения компьютерных данных, которые очень уязвимы по своей природе и могут быть быстро уничтожены. В этой ситуации традиционные механизмы взаимной правовой помощи и принцип суверенитета, одним из проявлений которого является то, что только правоохранительные органы государства могут проводить следственные действия на его территории, требуют множество формальных согласований, делая расследования транснациональных киберпреступлений проблематичным [7, с. 228-229]. Именно поэтому Россия так и не ратифицировала Европейскую конвенцию, ссылаясь на то, что «Конвенция предусматривает возможность, не ставя в известность то или иное государство, правоохранительным органам другого государства иметь доступ к ресурсам, размещенным в сетях общего пользования этого государства», что нарушает вышеуказанные принципы.

Однако исследования, проведенные как отечественными, так и зарубежными специалистами, показали, что процесс сдерживания преступности имеет две стороны. Во-первых, потенциальные преступники должны быть убеждены в том, что их обязательно обнаружат, т.е. необходим определенный уровень подготовки правоохранительных органов, чтобы непосредственно привлечь виновное лицо к ответственности независимо от его местоположения и усилий, приложенных для сокрытия своих данных.

Во-вторых, они должны быть убеждены, что наказание будет непременно суровым, то есть требуется реформация уголовного законодательства в отношении преступлений в сети интернет, а также совместная работа государств по данному вопросу, дабы правосудие восторжествовало.

Для эффективной работы в данной сфере необходимо сделать достаточно, чтобы успешно бороться с киберпреступностью. В первую очередь, это должно проводиться не только на уровне отдельного государства, но и всего мирового сообщества. Новые технологии позволяют правоохранительным органам заниматься успешной совместной борьбой с преступностью в международном масштабе, позволяя найти взаимоприемлемые подходы к сложнейшему вопросу территориальной подсудности, который является ключевым в борьбе с киберпреступностью.

Подводя итог всему сказанному, следует еще раз подчеркнуть, что киберпреступность это преступление глобального характера, но

вместе с тем оно достаточно новое. Преступники в данной области постоянно совершенствуются, ввиду чего всему мировому сообществу следует совершенствовать расследование таких преступлений, то же самое следует сделать и на национальном уровне, так как непосредственно в Российской Федерации пока не выработан механизм расследования преступлений в сфере компьютерных технологий и недостаточно отлажен. Существует много факторов, которые следует учесть и устранить, таких, как, например, отсутствие у следователя или дознавателя соответствующих знаний в данной теме, или продолжительность экспертиз. Также следует заполнить пробелы в законодательстве, дабы исключить возможные будущие преступления. Необходимо создать такой механизм, который успешно бы боролся с таким видом преступлений. И найти ту самую грань в работе с мировым сообществом, чтобы борьба с такими преступлениями была успешной.

Список использованных источников и литературы

1. Романенко А.С. Некоторые аспекты борьбы с киберпреступностью // Актуальные проблемы права, экономики и управления. 2015. №11. – С. 187-188.

2. Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт: монография. – М., 2004. – 185 с.

3. Шевко Н.Р. Особенности раскрытия и расследования киберпреступлений: проблемы и пути решения // Ученые записки Казанского юридического института МВД России. 2016. №1 (1). – С.13-16

4. Зверянская Л.П. Дискуссионные проблемы выявления и предупреждения киберпреступлений // Гуманитарные, социально-экономические и общественные науки. 2015. №8. С.160-161.

5. Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. №24. – С.45-55

6. Згадзай О. Э. Предупреждение киберпреступности. Проблемы и решения // Вестник Казанского юридического института МВД России. 2011. №6. – С.12-17

7. Волеводз А. Г. Правовые основы новых направлений международного сотрудничества в сфере уголовного процесса: дис. … на соискание ученой степени доктора юридических наук. 2016. – 426 с.

Научное издание

**УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ
И КРИМИНАЛИСТИЧЕСКИЕ ЧТЕНИЯ
НА АЛТАЕ**

ВЫПУСК XIV
Проблемы противодействие киберпреступности
уголовно-процессуальными, криминалистическими
и оперативно-розыскными средствами

Сборник научных статей

Статьи публикуются в авторской редакции

Подписано в печать 2017 г.
Объем уч.-изд. л. Формат 60х84/16. Бумага офсетная.
Тираж 100 экз. Заказ №