

Некоторые проблемы расследования нелегального негласного получения информации при помощи специальных технических средств

Научный руководитель – Неретина Надежда Сергеевна

Саркисян А.А.¹, Юдина О.В.¹

1 - Московский государственный юридический университет имени О.Е. Кутафина (МГЮА),
Институт судебных экспертиз, Москва, Россия

В настоящее время информация играет главную роль в жизни общества, и как никогда справедлив принцип «кто владеет информацией, владеет миром». Благодаря научному прогрессу за последние годы появилось большое количество технических средств, предназначенных для быстрого обмена большими объемами данных, которые стали использоваться для совершения преступлений, в этой связи за последние годы возникла проблема негласного получения информации. Под негласным получением информации можно понимать скрытное получение данных, представляющих интерес для решения определенных задач. Негласное получение информации может иметь как легальное основание, например, при производстве оперативно-розыскной деятельности, так и нелегальное, например, если доступ к информации пытаются заполучить с целью последующего шантажа или «кражи личности», незаконного использования персональных данных для получения материальной выгоды. Основной проблемой при расследовании подобных преступлений является постоянное повышение уровня квалификации субъектов киберпреступлений.

Понятие «специального технического средства» в законе отсутствует. Однако Конституционный Суд Российской Федерации в своем Постановлении от 31 марта 2011 г. N 3-П отнес к техническим средствам для негласного получения информации специальные технические средства, предназначенные (разработанные, приспособленные, запрограммированные) именно для целей негласного (т.е. тайного, неочевидного, скрытного) получения информации [2]. В части восьмой статьи 6 Федерального закона "Об оперативно-розыскной деятельности" указано, что Правительство РФ устанавливает те виды специальных технических средств, предназначенных для негласного получения информации, которые могут использоваться в процессе осуществления оперативно-розыскной деятельности [3]. Одним из методов негласного получения информации является использование специальных закладных устройств, замаскированных различными способами. Закладные устройства в зависимости от вида и особенностей информации, на перехват которой они направлены, могут подразделяться на акустические, телефонные и аппаратные закладки, а также на закладные телевизионные системы [4]. Отдельно от устройств также следует выделить программно-технические средства получения доступа к информации.

Специальные технические средства в зависимости от способа получения доступа к информации можно подразделить на средства контактного, бесконтактного и внутреннего действия. Например, процедура кейлоггинга, а именно перехвата информации о действиях пользователя компьютера путем регистрации сведений о нажатии клавиш на клавиатуре и компьютерной мыши, может производиться путем применения как программно-технических, так и аппаратных или акустических закладок. В первом случае способ получения доступа к информации будет внутренним, во втором - контактным, а в третьем - бесконтактным. Следовательно, возникает проблема расширения способов нелегального получения информации.

Вследствие специфики способа совершения преступления преступник попытается добиться максимальной скрытности закладки, так как чем дольше он останется незамеченным, тем больше информации можно получить. Камуфляж подбирается в зависимости от

вида устройства. Соответственно большинство материальных средств маскируются под объекты из привычной обстановки лица, в отношении которого совершается сбор информации. Программно-технические средства способны самостоятельно мимикрировать под ту среду, в которой они функционируют, следовательно, их обнаружение сводится к минимуму.

Найти такие устройства без применения специальных приборов практически невозможно, так как по внешнему виду они ничем не отличаются от предметов обстановки, их можно обнаружить только с помощью просвечивания рентгеновскими лучами [1]. Обнаружение закладок возможно с помощью различных сканеров, так как это действующие устройства, излучающие сигнал определенной частоты, но следует заметить, что существуют устройства, способные накапливать информацию достаточно долгий срок и с большой скоростью ее передавать. В свою очередь, это порождает еще одну проблему, - обнаружения устройств нелегального получения информации.

Последние годы получило распространение использование слабых мест технологий облачных хранилищ и беспроводных сетей с целью доступа к большому объему данных. Основной проблемой при расследовании неправомерного доступа к компьютерной информации при помощи этих средств, является зачастую либо полное отсутствие следов преступлений, либо их умышленное изменение субъектом преступления.

В процессе ускорения развития информационно-коммуникационных технологий возникает ряд проблем, связанных с обеспечением защиты данных. С каждым годом расширяется круг методов и средств, которые могут применяться субъектами киберпреступлений. В этой связи возникает необходимость формирования и развития направления цифровой криминалистики, в рамках которой будут разрабатываться основные вопросы расследования преступлений в области информационно-коммуникационных технологий.

Источники и литература

- 1) Коротыч Д.И. Лабораторный стенд для анализа демаскирующих признаков закладных устройств // Гаудеамус. 2013. №2 (22). С. 163-165.
- 2) Постановление Конституционного Суда РФ от 31.03.2011 N 3-П - «По делу о проверке конституционности части третьей статьи 138 Уголовного кодекса РФ в связи с жалобами граждан С.В. Капорина, И.В. Коршуна и других» // СПС Консультант-Плюс.
- 3) Федеральный закон от 12.08.1995 N 144-ФЗ (ред. от 06.07.2016) «Об оперативно-розыскной деятельности» // СПС КонсультантПлюс
- 4) Хорев А.А. Классификация электронных устройств перехвата информации // Спец-техника и связь. 2009. №1. С.46-49.