DOI 10.12851/EESJ201606C04ART06

Artur S. Stepanov,
Masters student,
Crimean Law Institute (branch)
Russian Academy of General Prosecutor's Office

Fundamental Criminalistics Technique and Tactics of Crime Investigation in Sphere of Computer Information

Key words: information, computer technology, crimes in the sphere of computer information, computer crimes.

Annotation: the article contains the author's suggestions on technique and tactics of investigation and disclosing of crimes in the sphere of computer information in order to optimize this process.

В современном обществе при стремительном развитии научно-технического прогресса уделяется особое внимание совершенствованию компьютерных технологий, это связано с возрастающей ролью информации. Существует разветвленная система общественных отношений, предметом которых является информация, хранящаяся, циркулирующая и обрабатываемая как в отдельных компьютерах, так и информационно-коммуникационных сетях. Одним из следствий такой массовой компьютеризации явились преступления в сфере компьютерной информации. С каждым годом частота преступлений в компьютерной сфере и объем наносимого ими ущерба значительно увеличиваются. Основная причина этому – высокая доходность такого противозаконного бизнеса и недоработки в законодательстве и судовой практике Российской Федерации.

Преступления, совершаемые с использованием компьютерных средств и систем, называются компьютерными преступлениями. Это определение рассматривают не только в уголовно-правовом аспекте, а и в криминалистическом, поскольку оно связано не с квалификацией, а именно со способом совершения и сокрытия преступления и, следовательно, с методикой его раскрытия и расследования (1, p. 68).

Рассмотрим основные особенности тактики следственных действий при расследовании компьютерных преступлений. Можно выделить следующие типичные следственные ситуации.

Компьютерное преступление произошло:

в условиях очевидности — характер и его обстоятельства известны (например, какой вирус и каким способом введен в компьютерную сеть) и выявлены потерпевшим собственными силами, преступник известен и задержан (явился с повинной);

известен способ совершения, но механизм преступления в полном объеме неясен (например, произошел несанкционированный доступ к файлам законного пользователя через Интернет, через слабые места в защите компьютерной системы), преступник известен, но скрылся;

налицо только преступный результат (например, дезорганизация компьютерной сети банка), механизм преступления и преступник неизвестны.

В первом случае необходимо установить, имелась ли причинно-следственная связь между несанкционированным проникновением в компьютерную систему и наступившими последствиями, определить размеры ущерба.

Во втором случае первоочередной задачей наряду с указанным выше являются розыск и задержание преступника.

В третьей ситуации необходимо установить механизм преступления (2, p. 23).

Далее рассмотрим особенности тактики следственных действии, направленных на собирание компьютерной информации.

Перед началом обыска принимаются меры к предотвращению повреждения или уничтожения информации:

осуществляется контроль за бесперебойным электроснабжением информационно-коммуникационного комплекса в момент осмотра;

удаляются все посторонние лица с территории, на которой производится осмотр, и прекращается доступ на нее;

оставшиеся на территории лица лишаются доступа к средствам вычислительной техники и к источникам электропитания;

эвакуируются находящиеся на объекте взрывчатые, легковоспламеняющиеся, едкие вещества, посторонние источники излучения и другие предметы и аппаратура, способные привести к аварии ЭВМ.

Собирание криминалистически значимой информации в вычислительной сети имеет свои особенности. В первую очередь необходимо установить общее количество компьютеров и их распределение по другим помещениям, а также количество и тип используемых серверов и рабочих мест. Далее важно выяснить тип используемой сетевой операционной системы и состав прикладного программного обеспечения, используемого в вычислительной сети. Следует также установить факт наличия резервных копий данных и места их хранения. Особое внимание должно уделяться выявлению выхода в другие, в том числе и глобальные, сети; установлению возможностей использования коммуникационных средств для связи с удаленными пользователями, другими организациями (фирмами), частными лицами.

В это же время определяются принятые в организации мероприятия по защите информации и наличие выхода в Интернет. В случае использования телефонной линии для связи с другими сетями обеспечить отключение телефона; по возможности удалить из помещения все взрывчатые, едкие и легковоспламеняющиеся материалы.

Завершающим этапом осмотра, обыска или выемки по делам, сопряженным с использованием компьютерных технологий, являются фиксация и изъятие компьютерных средств. От того, как произведены изъятие, транспортировка и хранение этих объектов, часто зависит их доказательственное значение. Все изъятые системные блоки и другие устройства должны быть упакованы и опечатаны таким образом, чтобы исключить возможность их повреждения, включения в сеть и разборки. В протоколе

должны быть точно отражены место, время и внешний вид изымаемых предметов и документов. При изъятии компьютеров и носителей данных их следует упаковывать и опечатывать.

При допросах подозреваемых и обвиняемых необходимо учитывать данные криминалистической характеристики о личности предполагаемого преступника.

Выполнение подобных задач требует высокой квалификации специалистов – владение методиками и процедурами сбора и представления доказательств, их подачи в компетентные инстанции, знание законодательных нормативов и тонкостей для формирования понятного состава обвинения.

References:

1. *Manoilo AV. State information policy in special circumstances: Monography. Mosocw, 2010; 388.*
2. *Vekhov VB. Computer modeling in the investigation of crimes in the sphere of computer information: manual, VB. Vekhov, SA. Kovalev; ed. ScD, professor BP. Smagorinsky. Volgograd, 2014; 77.*
3. *The Criminal Code of the Russian Federation; dated June 13, 1996; N 63-FZ. (Art. 274 of the Criminal Code)*
4. *Criminal Procedure Code of the Russian Federation of December 18, 2001; N 174-FZ.*