УДК 343.98.068:004

ПРОБЛЕМНЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАССЛЕДОВАНИИ УГОЛОВНЫХ ДЕЛ

Э.А. Ли

Раскрываются возможности совершенствования защиты компьютерной информации для информационного обеспечения в уголовном процессе.

Ключевые слова: компьютерные технологии; компьютерная информация; информационная безопасность.

PROBLEMATIC ASPECTS OF INFORMATION SECURITY IN THE INVESTIGATION OF CRIMINAL CASES

E.A. Li

The paper describes the possibility of improving the protection of computer information systems for information assurance in the criminal process.

Keywords: computer technology; computer information; information security.

Наличие относительно высокого процента числа нераскрытых преступлений – это, прежде всего, неудовлетворительная работа следователей, в особенности, связанный с этим недостаточный уровень знаний и умений пользоваться современными достижениями компьютерных технологий.

Безусловно, можно согласиться с позицией Ю.В. Кореневского, с точки зрения которого "не вызывает сомнений, что всегда будут преступления, раскрыть которые не удалось, несмотря на добросовестную, умелую, порой самоотверженную работу оперативников и следователей. Если не считаться с этим, мы получим (и уже получаем) результат, прямо противоположный ожидаемому" [1, с. 57]. В этой связи считаем вполне очевидным, что проблема результативности деятельности по раскрытию и расследованию преступлений не зависит только от вопросов, связанных с эффективностью организации и осуществлением процесса расследования. Как представляется, эта проблема носит сложный, многофакторный характер, на что совершенно верно обратил внимание А.И. Трусов, с точки зрения которого существует целое множество факторов, которые могут как способствовать, так и препятствовать установлению истины по уголовному делу [2, с. 6, 7].

В специальной литературе приводятся различные точки зрения по поводу состава и содержания различных факторов, мешающих оптимальному протеканию информационных процессов в ходе расследования преступлений. К их числу А.В. Лапин, например, относит:

- *технический* – необходимость применения технических средств для обнаружения, изъятия и фиксации информации;
- *социальный* – необходимость преодоления антисоциальных установок заинтересованных лиц;
- *терминологический* – наличие специальных терминов, непонятных участникам расследования и следователю;
- *языковой* – препятствие информационному общению из-за языковых различий;
- *гносеологический* – недостаток профессиональных знаний, опыта следователя и др. [3, с. 24].

По мнению А.М. Кустова, вся совокупность факторов, определяющих возможность получения информации о механизме преступления, может быть поделена на две основные группы: объективные и субъективные [4, с. 234–235].

Конечно, перечень факторов, определяющих информационную составляющую эффективности предварительного следствия, не является исчерпывающим и может быть дополнен. Данный вопрос не является целью настоящей статьи. Однако

проведенный анализ факторов негативного воздействия на деятельность по раскрытию и расследованию преступлений, носящих информационный характер, подтверждает тот вывод, что эти факторы могут носить как субъективный, так и объективный характер.

Следует отметить, что в правовой литературе встречаются различные подходы к определению понятия "противодействие расследованию преступлений". Так, например, ряд авторов под противодействием расследованию понимают умышленную деятельность с целью воспрепятствования решению задач расследования и в конечном счете установлению истины по уголовному делу [5, с. 129].

За последние десятилетия преступная деятельность стала более профессиональной и организованной, произошел раздел сфер влияния, налаживаются и углубляются связи с международными преступными сообществами. В отличие от правоохранительных органов, преступные формирования располагают практически неограниченными финансовыми ресурсами и не связаны никакими ограничениями закона, что позволяет им выстраивать свою, достаточно эффективную, систему противодействия органам правопорядка при осуществлении ими своих полномочий в сфере уголовного судопроизводства, используя при этом новейшие технические средства и информационные технологии [6, с. 11].

В этой связи вполне объяснимо то, что в настоящее время деятельность правоохранительных органов по раскрытию и расследованию преступлений осуществляется в условиях усиливающегося информационно-технического противодействия со стороны преступных формирований, "...современные криминальные формирования активно используют технические, в особенности радиоэлектронные, средства для планирования, подготовки конкретных противоправных действий. Ситуация осложняется тем, что в открытой печати, на информационных стендах, в рекламах различных фирм и т. п. публикуется множество объявлений о продаже "техники безопасности" (по сути дела, спецтехники, предназначенной для скрытого добывания информации)" [7, с. 361].

В настоящее время преступными сообществами используются специальные технические средства для организации каналов получения разведывательной информации, по которым идет утечка сведений о наличии, а в отдельных случаях и о ходе оперативных проверок в отношении членов организованных преступных сообществ и планируемых органами внутренних дел в отношении них операциях. В этих целях ими осуществляется прослушивание рабочих радиочастот органов внутренних дел, перехват радио- и телефонных переговоров оперативно-следственных групп при их выезде на места происшествий, прослушивание служебных и домашних телефонов оперативных и следственных работников с целью получения значимой информации, ведение наблюдения за свидетелями, потерпевшими, экспертами с целью сбора компрометирующих материалов, фиксация их контактов, установление места жительства и т. п.

Исходя из сказанного, полагаем вполне очевидным то обстоятельство, что практические проявления рассмотренных факторов негативного воздействия на процесс предварительного расследования не только затрудняют его осуществление и снижают эффективность расследования, но и зачастую представляют собой непосредственные угрозы деятельности по раскрытию и расследованию преступлений в информационном плане, угрозы, предопределяющие необходимость принятия комплекса действенных мер по обеспечению информационной безопасности этой деятельности.

Если посмотреть на эту проблему несколько шире, то, в сущности, как верно заметил Н.В. Щедрин, "история человека есть история обеспечения его безопасности. От примитивной палки – до компьютерной защиты, от мистического табу – до философски и юридически обоснованных систем коллективной безопасности" [8, с. 67]. Безопасность – это неотъемлемая характеристика прогресса, а понятие безопасности является одним из ключевых при исследовании вопросов оптимизации человеческой деятельности, в том числе и деятельности по борьбе с преступностью.

На протяжении столетий понятие безопасности неоднократно наполнялось разным содержанием и, соответственно, пониманием его смысла. Так, в древности понимание безопасности не выходило за рамки обыденного представления и трактовалось как отсутствие опасности или зла для человека. В таком житейском значении термин "безопасность" употреблялся, например, еще древнегреческим философом Платоном [9, с. 107].

Однако, несмотря на то что в настоящее время существует уже достаточно большое количество исследований по проблемам безопасности, приходится констатировать, что в отечественной науке налицо проблемы с неопределенностью понятий "безопасность" и "информационная безопасность".

Следует согласиться с мнением А.Н. Григорьева [10, с. 15], что обеспечение информационной безопасности деятельности по раскрытию и расследованию преступлений с содержательной точки зрения представляет собой процесс создания таких

“благоприятных” условий осуществления расследования уголовного дела, при которых обеспечивается достижение его целей в информационном плане, т. е. формируется достоверный и достаточный массив доказательственной информации по расследуемому преступлению и обеспечивается соответствующей информационной защитой с помощью как технических, так и программных средств.

Необходимость реализации отмеченного предопределяет то, что важнейшими задачами, стоящими в ходе предварительного следствия перед субъектами деятельности по раскрытию и расследованию преступлений, помимо прочих, являются выявление и блокирование потенциальных информационных угроз, а также предотвращение и минимизация информационных потерь [11, с. 60].

Исходя из изложенного полагаем, что под информационной безопасностью предварительного расследования преступлений следует понимать такую совокупность условий его осуществления, при которой потенциально опасные информационные угрозы деятельности по раскрытию и расследованию преступлений либо предупреждались, либо сводились к уровню, обеспечивающему достижение целей этой деятельности.

Таким образом, мы приходим к выводу, что защита компьютерной информации является неотъемлемой составной частью информационного обеспечения безопасности при расследовании преступлений, определяющей не только успешное осуществление информационных процессов, но и создание оптимальных условий для эффективного использования компьютерной информации в целях раскрытия и расследования преступлений.

Перечислим некоторые из применяемых способов защиты компьютерной информации.

1. Физические способы защиты компьютерной информации в своей основе предполагают создание различных физических препятствий, которые максимально ограничили бы доступ посторонних лиц к техническим средствам хранения криминалистически значимой информации (серверам, персональным компьютерам, рабочим станциям и т. д.) с использованием технических средств, таких как замки и решетки на дверях и окнах, устройства охранной сигнализации, камеры слежения. Также могут быть использованы специальные электронные системы допуска в рабочие кабинеты и комнаты, в которых находятся средства хранения компьютерной информации, с использованием электронных ключей, дающих доступ только ограниченному кругу лиц.

2. Организационные способы защиты компьютерной информации включают в себя меры по организации соответствующего режима секретности, пропускного и внутреннего режима в следственном и оперативно-розыскном подразделениях. В данном случае речь идет о разработанном порядке работы с компьютерной информацией, которая имеет криминалистическое значение и правила получения, передачи, хранения и использования рассматриваемой информации. Для минимизации случаев утери компьютерной информации следует рассмотреть вопрос о наличии в штате правоохранительных структур инженеров-компьютерщиков, которые, наряду с функциями по администрированию локальных сетей, также занимались бы и вопросами профилактики и настройки персональных компьютеров следователей и оперативных работников, технической помощи следователям по компьютерному моделированию, а также выстраиванием всей системы защиты компьютерной информации.

3. Программные способы защиты компьютерной информации являются средством защиты информации, находящейся в компьютере посредством использования специальных компьютерных программ, которые могут подразделяться на программы для обнаружения и удаления мониторинговых программных продуктов (программ-шпионов) и на программы специализированных систем защиты. Как видно из изложенного выше, программные средства защиты очень важны с учетом того, что часто преступники, не имея физического доступа к компьютерному оборудованию следователя, пытаются установить такой доступ через использование программ-шпионов.

4. Биометрическая технология – наиболее продвинутое из последних достижений в области идентификации и контроля доступа к информации. Как показали результаты аналитического исследования современного состояния и перспектив развития рынка биометрических средств защиты информации, в развитии индустрии безопасности сегодня обозначился новый этап. На общем фоне стабилизировавшегося рынка наиболее динамично продолжают развиваться современные системы идентификации личности и защиты информации, в том числе и компьютерной. Особое внимание привлекают к себе биометрические средства защиты информации (БСЗИ), что объясняется их высокой надежностью идентификации и достигнутым в последнее время значительным снижением их стоимости.

Наибольшее применение в настоящее время нашли биометрические системы защиты информации, использующие идентификацию личности по отпечатку пальца. Сочетание биометрического

сканирования отпечатка пальца и ввод PIN-кода суммарно повышают эффективность защиты доступа к компьютерной информации. При совпадении введенного PIN-кода с кодом, зашифрованным в системе и совпадении предъявляемого и контрольного отпечатков, терминал подает сигнал на запуск автоматизированной системы или отдельных ее функций или открывает доступ к определенной информации.

5. Криптографические способы защиты информации путем шифрования необходимо применять в особенности при пересылке криминалистически важной компьютерной информации. Криптографические способы защиты используют методы шифровки информации, которые кодируют информацию таким образом, чтобы ее содержание было доступно только при предъявлении некоторой специфической информации (ключа). Шифрование может осуществляться автоматически, с помощью специальных аппаратных средств (шифраторов) или специального программного обеспечения. Криптографическим шифрованием называется процесс замены и/или перестановки тех или иных символов исходного сообщения (исходной информации) по специальному алгоритму в соответствии с заданным ключом (своего рода паролем). Причем, что немаловажно, одному и тому же символу исходного сообщения, который может встречаться там сколько угодно раз, всегда соответствуют различные и случайные символы шифровки. Иначе сам процесс назывался бы просто кодированием и не представлял бы никакого интереса для науки криптологии. Одной из популярных программ является программа PGP (Pretty Good Privacu), основанная на самых надежных алгоритмах шифрования. Ее производитель PGP Inc. достиг высокой надежности и предотвращения от несанкционированного перехвата ключей для расшифровки.

Учитывая, что в практике деятельности правоохранительных органов Кыргызской Республики описанные выше физические и организационные способы защиты компьютерной информации функционируют, но при этом не могут в условиях все возрастающего противодействия расследованию преступлений обеспечивать безопасность от утечки компьютерной информации, актуальным становится внедрить дополнительно в обязательном порядке и такие современные способы защиты компьютерной информации, как: программные; биометрические; криптографические.

Таким образом, отечественный и зарубежный опыт защиты информации показывает, что комплексная система мер защиты компьютерной информации на досудебной стадии уголовного процесса, включающая такие современные способы защиты компьютерной информации, как программные, биометрические и криптографические, а именно их алгоритмическое сочетание, может привести к наиболее надежной защите компьютерной информации за счет достижения синергетического эффекта.

Литература

1. *Кореневский Ю.В.* Актуальные проблемы доказывания в уголовном процессе / Ю.В. Кореневский // Государство и право. 1999. № 2.
2. *Трусов А.И.* Проблемы надежности процессуального доказывания / А.И. Трусов // Проблемы надежности доказывания в советском уголовном процессе: тез. выступлений на семинаре, проведенном ВНИИ МВД СССР, совместно с ин-том Прокуратуры СССР 13 апреля 1983 г. М.: ВНИИ МВД СССР, 1984.
3. *Лапин А.В.* Теория информации и некоторые вопросы расследования преступлений / А.В. Лапин // Вестник Белорус. ун-та им. В.И. Ленина. 1987. Сер. 3.
4. *Кустов А.М.* Криминалистика и механизм преступления: цикл лекций / А.М. Кустов. М.: Изд-во Моск. псих. соц. ин-та, 2002.
5. Криминалистическое обеспечение деятельности криминальной милиции и органов предварительного расследования / под ред. проф. Т.В. Аверьяновой и проф. Р.С. Белкина. М.: Новый юрист, 1997.
6. Специальная техника и информационная безопасность: учеб. / под ред. В.И. Кирилина: в 2 т. Т. 1. М.: Академия управления МВД России, 2000.
7. Основы оперативно-розыскной деятельности: учеб. / под ред. В.Б. Рушайло. СПб.: Лань, 2000.
8. *Щедрин Н.В.* Введение в правовую теорию мер безопасности / Н.В. Щедрин. Красноярск: Изд-во Красноярск. гос. ун-та, 1999.
9. *Таранов П.С.* Мудрость трех тысячелетий / П.С. Таранов. М.: ООО “Изд-во АСТ”, 1999.
10. *Григорьев А.Н.* Теоретические аспекты информации и ее защиты в предварительном расследовании преступлений: автореф. дис. ... канд. юрид. наук / А.Н. Григорьев. Калининград, 2002.
11. *Камалова Г.Г.* Криминалистическое содержание и сущность защиты информации в деятельности по выявлению и раскрытию преступлений: дис. … канд. юрид. наук / Г.Г. Камалова. Ижевск, 2002.