М.Ш. Махтаев[1]
И.Е. Лебедь[2]

КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Статья посвящена освещению вопросов криминалистического обеспечения предупреждения преступлений в сфере компьютерной информации, обосновывается положение о том, что обстоятельства, способствующие совершению и сокрытию компьютерных преступлений, устанавливаются по результатам тщательного анализа всех материалов расследования конкретного преступления в указанной сфере, оперативных данных и другой имеющейся информации, а также путем анализа ранее расследовавшихся уголовных дел по аналогичным преступлениям или преступлениям, совершенным в данной организации, районе.

Ключевые слова: *криминалистическое предупреждение преступлений, компьютерные преступления, предупреждение компьютерных преступлений, защита компьютерных систем, преступление, причины и условия, способствующие совершению преступлений (обстоятельства, способствующие совершению преступлений), вредоносные программы, компьютерная информация, сеть ЭВМ, система ЭВМ, правила эксплуатации ЭВМ.*

M.Sh. Makhtaev,
I.E. Lebed

CRIMINOLOGICAL ASPECTS OF WARNING CRIMES IN THE COMPUTER INFORMATION

The article is dedicated to the illumination of questions of the criminological guarantee of warning crimes in computer information. The position about the fact that the circumstances, which facilitate accomplishment and concealment of computer crimes, are set to the results of the thorough analysis of all materials of the concrete crime investigation, operational data and of other existing information, and also via earlier investigated criminal cases analysis for analogous crimes, or crimes perfected in this organization, as well as in region as a whole.

Keywords: *criminological warning of crimes, computer crimes, warning computer crimes, protection of computer systems, crime, reasons and the conditions, which facilitate the accomplishment of crimes (circumstances, which facilitate the accomplishment of crimes), malicious software, computer information, computer Networks, computer system, operating instructions of computers.*

В решение задач предупреждения преступлений и локализации причин, их порождающих, определяющий вклад вносит комплексное изучение проблемы предупреждения правонарушений рядом общественных и юридических наук, вследствие чего следует считать общепризнанным междисциплинарный подход к решению данной проблемы, что особенно актуально на современном этапе развития юридических наук.

Высказывается мнение, что проблема предупреждения преступлений целиком относится к криминологии, а ее включение в предмет криминалистики необоснованно расширяет, размывает его четкие рамки. Даже если ограничить предмет криминалистики раскрытием преступлений, предупреждение и в этом случае будет относиться к задачам криминалистики, поскольку преступление нельзя считать полностью раскрытым, пока не выяснены все обстоятельства, подлежащие доказыванию по уголовному делу (ст. 73 УПК РФ), в том числе и обстоятельства, способствующие совершению преступления.

Исследуя проблему предупреждения преступлений, криминалисты, криминологи и процессуалисты должны объяснить, что́ именно следует понимать под причинами и условиями, способствующими совершению преступлений, в каких пределах и какими методами они должны выявляться следователем или оперативным работником, какие меры и как именно должны ими приниматься для их устранения.

[1] Доктор юридических наук, заведующий кафедрой уголовно-правовых дисциплин юридического факультета НОУ ВПО «Российский новый университет».

[2] Аспирант НОУ ВПО «Российский новый университет».

Разработка тактически и методически продуманных решений задач выявления причин и условий, способствующих совершению и сокрытию преступлений, и применения специфических мер их предупреждения и пресечения практически всегда были целью науки криминалистики, начиная с первых лет ее существования.

Общим вопросам криминалистического предупреждения преступлений были посвящены работы Р.С. Белкина, Н.П. Яблокова, И.Я. Фридмана, Г.Г. Зуйкова, В.А. Ледащева, В.В. Вандышева, В.С. Зеленецкого, В.Ф. Зудина, М.Ш. Махтаева, В.П. Колмакова и других ученых. В криминалистической литературе все большее распространение получает идея дальнейшего развития частной криминалистической теории предупреждения преступлений. Окончательное формирование данной частной теории еще далеко от своего завершения, но основные ее положения уже раскрыты в ряде научных работ [1, гл. 6; 2, гл. 57].

Существо мер по предотвращению (предупреждению) или пресечению преступлений состоит в том, чтобы при готовящемся правонарушении удержать от преступления лицо, намеревающееся его совершить, а также не допустить совершения преступления или покушения на него. Когда же преступная деятельность уже вылилась в совершение преступления, меры пресечения должны обеспечить прекращение указанной деятельности на любой ее стадии. В ходе начавшегося расследования следователь пресекает преступную деятельность разными средствами, например путем задержания и избрания меры пресечения для подозреваемых или обвиняемых или посредством изъятия орудий преступления в ходе отдельных следственных действий (обыске, выемке).

С учетом соответствующих норм уголовно-процессуального законодательства, выделяют ряд конкретных задач криминалистического предупреждения преступлений, решаемых специфическими методами криминалистики:

• разработка методов и приемов выявления причин и условий, способствующих совершению преступлений с учетом их криминологических и криминалистических особенностей;

• выделение объектов криминалистико-профилактического изучения и воздействия;

• выявление и исследование особенностей типичных следственных ситуаций профилактического характера, складывающихся при расследовании, и выработка на их основе главных направлений криминалистической деятельности по предупреждению преступлений;

• определение примерного комплекса профилактических мер, наиболее действенных в каждой из выделенных ситуаций и показ особенностей их реализации;

• разработка мер пресечения начавшегося и предупреждения готовящегося преступления [3, с. 110].

В криминалистическом обеспечении предупреждения преступлений определенное место занимает разработка средств, приемов и методов предупреждения преступлений в сфере компьютерной информации, в целом, и связанных с созданием, использованием и распространением вредоносных программ, в частности. Некоторые криминалистические аспекты предупреждения преступлений в указанной сфере деятельности затрагивались в работах В.В. Крылова, Н.Г. Шурухнова, М.Ш. Махтаева, В.Б. Вехова, В.Ю. Рогозина, В.Д. Курушнина, Ю.В. Гаврилина, Л.Н. Соловьева и других авторов [4; 5; 6].

Однако нельзя сказать, что процесс разработки вопросов предупреждения преступлений рассматриваемой категории окончен. Эти преступления продолжают развиваться, расширяются возможности, совершенствуются орудия и средства их совершения, возникают новые и видоизменяются старые способы совершения преступлений, а это, в свою очередь, требует постановки и разрешения новых задач предупреждения преступлений в сфере компьютерной информации.

Статья 73 УПК РФ требует от следователя, органа дознания, прокуратуры, суда выявлять обстоятельства, способствовавшие совершению преступления. Установив их, указанные в законе субъекты обязаны принять специальные меры к их устранению, с тем чтобы предупредить совершение аналогичных или иных преступлений.

Задача выявления указанных причин и условий ставится в законе не случайно, так как нередко преступления являются следствием комплекса причин и условий, часто *образующих сложные причинно-следственные цепи*. Исходя из того, что объектом криминалистического познания причинных связей в ходе расследования, прежде всего, является характер различного рода временных, динамических и иных видов связи отдельных этапов, обстоятельств, факторов самого события преступления, характеризующих механизм расследуемого преступления, криминалистов, в отличие от представителей других наук криминального цикла, интересуют все звенья причинно-следственного ряда. Выявление же на практике расследования различных преступлений всех звеньев указанного ряда крайне затруднено.

Преступления, связанные с созданием, использованием и распространением вредоносных программ и наступлением в результате этого вредных

последствий, зачастую могут являться следствием нескольких различных причин. Как правило, это результат сложного причинно-следственного взаимодействия, в котором наряду с техническими, организационными и иными обстоятельствами наличествуют такие элементы, как сформировавшееся с годами неверное представление о вредоносных программах, устаревшие взгляды на проблему компьютерных преступлений в целом, непонимание общественной опасности последних. Кроме того, в эту систему нередко вливаются и различные посторонние факторы, существенным образом изменяющие направление и характер действия отдельных элементов причинной цепи. Разбираться во всех звеньях причинно-следственного ряда по таким уголовным делам, как и в других случаях, необходимо, исходя из конкретной сложившейся ситуации, в зависимости от особенностей расследуемого преступления: путем следственных действий, путем моделирования с использованием логических приемов мышления.

Помимо этого следователем, оперативным работником и другими субъектами, участвующими в расследовании, могут использоваться и другие специальные криминалистические средства. Одним из таких средств является криминалистическое прогнозирование. Используя всю имеющуюся в распоряжении следователя информацию, включая материалы служебного расследования и материалы, полученные из оперативных подразделений, средствами криминалистического прогнозирования могут быть выявлены дополнительные потенциальные источники и направления, угрожающие безопасности компьютерных систем. В ходе криминалистического прогнозирования могут решаться и более сложные проблемы. Например, речь может идти о прогнозировании новых способов совершения преступлений и формирования новых предупредительных мер, направленных на их локализацию, что особенно важно для преступлений рассматриваемой категории.

Отсутствие достаточной практики расследования преступлений рассматриваемой категории и, как следствие этого, надлежащим образом разработанной методики их расследования приводит к трудностям в установлении всех обстоятельств, подлежащих доказыванию, в том числе и обстоятельств, способствующих совершению этой группы преступлений.

Анализ имеющейся на сегодняшний день практики показывает, что обстоятельства, способствующие совершению преступлений в сфере компьютерной информации, можно разделить на три группы:

1) обстоятельства, способствующие неправомерному доступу к компьютерной информации;

2) обстоятельства, способствующие непосредственно созданию, использованию и распространению вредоносных программ для ЭВМ;

3) обстоятельства (причины и условия), способствующие нарушению правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Обстоятельства, способствующие неправомерному доступу к компьютерной информации, преимущественно состоят в следующем.

1. Отсутствие единой политики безопасности в организации.

2. Отсутствие в организации (подразделении) реально действующих правил эксплуатации средств компьютерной техники.

3. Недостаточное кадровое и материально-техническое обеспечение служб при проведении обслуживания технических систем.

4. Недостаточное кадровое и материально-техническое обеспечение служб безопасности и кадровых служб организаций, учреждений, предприятий.

5. Приобретение и использование несертифицированного, контрафактного программного обеспечения.

6. Приобретение и эксплуатация несертифицированных ЭВМ и других средств компьютерной техники.

7. Незащищенность коммуникационных каналов и других элементов компьютерных систем.

8. Неэффективность избранных собственником методов защиты компьютерной информации от несанкционированного доступа.

9. Отсутствие плановости и тщательности в проверке сетей и систем на наличие несанкционированного доступа.

10. Отсутствие должного контроля при приобретении, техническом обслуживании и эксплуатации в рамках структурного подразделения организации программных и аппаратно-технических средств компьютерной техники.

11. Отсутствие проверок на изменение конфигурации и программного обеспечения после технического обслуживания и эксплуатации компьютерных систем.

12. Нарушение правил администрирования систем и сетей ЭВМ (незаконная передача паролей, нарушение установленных правил их изменения, необоснованное повышение уровня доступа, неконтролируемые сеансы работы, неконтролируемый выход во внешние сети и т.д.).

13. Отсутствие или недостаточная разъяснительная работа в организации.

Обстоятельства, способствующие непосредственно созданию, использованию и распро-

странению вредоносных программ для ЭВМ, не вошедшие в группу обстоятельств, способствующих неправомерному доступу, следующие.

1. Нарушение установленных технических и организационных правил по обеспечению защиты компьютерной информации от вредоносных программ.

2. Отсутствие необходимых программных и аппаратно-технических средств защиты компьютерной информации, обеспечивающих защиту от внедрения и функционирования вредоносных программ.

3. Отсутствие специалистов по противодействию вредоносным программам.

4. Нарушение порядка резервирования компьютерной информации, включая используемое программное обеспечение.

5. Отсутствие надлежащего порядка использования и утилизации резервных копий данных и программного обеспечения.

6. Отсутствие надлежащего порядка хранения машинных носителей информации.

7. Использование случайных машинных носителей информации.

8. Использование непосредственными пользователями программных средств, не предназначенных для обеспечения деятельности организации.

9. Использование устаревшего или поврежденного программного обеспечения.

10. Неконтролируемый обмен через глобальные и иные информационные сети электронными письмами.

11. Неконтролируемое использование Интернета, получение непроверенных файлов данных и программного обеспечения.

12. Ограниченный обмен текущей информации о существующих вредоносных программах и признаках их внедрения и функционирования.

Обстоятельства (причины и условия), способствующие нарушению правил эксплуатации ЭВМ, системы ЭВМ или их сети, выявляются путем изучения как общего состояния охраны информационной безопасности в определенной системе или сети, так и факторов, непосредственно обусловивших расследуемое событие. Основные из этих обстоятельств были перечислены среди обстоятельств, способствовавших неправомерному доступу к компьютерной информации и созданию, использованию и распространению вредоносных программ.

Успешность выявления указанных обстоятельств зависит от систематичности соответствующих действий следователя, что обеспечивается целенаправленным планированием расследования.

Обстоятельства, способствовавшие преступлению, должны устанавливаться в ходе всего расследования. Поэтому уже при составлении плана первоначальных следственных действий предусматриваются действия, прямо относящиеся к решению этого вопроса. Например, проверяя версию о возможности внедрения вредоносной программы посторонним лицом, в плане указываются действия по выяснению наличия, состава и режима работы структурного подразделения и охраны организации, состоянию технических средств обеспечения безопасности компьютерных систем и помещений, порядок внесения изменений в программное обеспечение и т.д.

Перечисленные обстоятельства устанавливаются по результатам тщательного **анализа всех материалов конкретного уголовного дела, оперативных данных и другой имеющейся информации**, а также путем анализа ранее расследовавшихся уголовных дел по аналогичным преступлениям или преступлениям, совершенным в данной организации, районе и т.д.

Важную информацию об обстоятельствах, способствовавших преступлению, можно получить путем следственного осмотра. Так, осматривая место совершения неправомерного доступа к компьютерной системе, следователь может отметить возможность беспрепятственного доступа в помещение, что создает удобные условия для осуществления не только преступлений рассматриваемой категории, но и других, напрямую не связанных с воздействием на компьютерную информацию, например хищений. В ходе осмотра могут быть выявлены и другие обстоятельства, прямо или косвенно влияющие на совершение рассматриваемой категории преступлений. В ряде случаев отсутствие обязательного пломбирования (опечатывания) корпусов ЭВМ, закрытия и опечатывания хранилищ машинных носителей информации, выявленные в ходе осмотра, а также их небрежное хранение могут свидетельствовать о ненадлежащей охране машинных носителей информации. Отсутствие во многих случаях защитных корпусов на ЭВМ и другом электротехническом оборудовании, ненадлежащие условия его эксплуатации, повреждение электропроводки хотя напрямую могут быть и не связаны с совершенным преступлением, но они являются явным нарушением требований охраны труда, пожарной безопасности, что требует обязательного устранения и не может быть обойдено вниманием следователя.

Немаловажным является и проведение последовательного изучения различных документов, относящихся к вопросам организации взаимодей-

ствия с компьютерной информацией, компьютерными системами и их защиты (различных правил, инструкций, положений). Особое значение могут иметь материалы ведомственного (служебного) расследования.

В ходе осмотра ЭВМ может быть выявлено отсутствие средств, обеспечивающих разграничение доступа к определенному программному обеспечению и данным, отсутствие специальных программ, предназначенных для борьбы с вредоносными программами, непроведение или несистематичность проведения контроля программных средств, небрежность хранения компьютерной информации на машинном носителе, наличие случайного программного обеспечения и т.д. Все это может и не быть связано с совершенным преступлением, но может привести к нарушению целостности информации или ее конфиденциальности, а также может быть связано с нарушением авторских прав на используемое программное обеспечение. При осмотре сетей ЭВМ может быть выявлена возможность несанкционированного подключения к компьютерной сети, неконтролируемого внешнего доступа в локальную компьютерную сеть, отсутствие систем разграничения доступа, неконтролируемое число пользователей и т.д.

При осмотре документов может быть выявлена небрежность оформления, несоблюдение установленных правил их оборота и хранения, что позволило преступнику завладеть информацией, относящейся к компьютерным системам, выяснить характер обрабатываемой информации, получить имена и пароли законных пользователей, исходных текстов программного обеспечения и другую информацию и создать благоприятные условия для совершения самого преступления.

Эффективным средством выявления указанных обстоятельств может стать обыск жилища или рабочего места лица, подозреваемого в совершении преступления. Так, обнаруженные в ходе обыска вредоносные программы, их исходные тексты, информация, относящаяся к определенным компьютерным системам, может свидетельствовать о подготовке или совершении ряда других преступлений. Обнаруженные машинные носители с указанными программами могут позволить выявить место их приобретения, всю цепочку, ведущую от создателя через посредников к лицу, их использовавшему, что позволяет пресечь их дальнейшее распространение.

Путем допроса (опроса) подозреваемых, потерпевших и свидетелей следователь и оперативный работник получают сведения, значимые как для профилактики преступлений, так и для анализа личности виновных, формы и содержания их антиобщественной установки. Путем допроса становится возможным не только выявить конкретные обстоятельства, способствовавшие совершению расследуемого преступления, но и определить, в какой мере они способствуют новым преступлениям.

При допросе подозреваемого должны быть выяснены обстоятельства формирования у него умысла, с чем это связано, каким мотивом он руководствовался. Подробно выясняются те обстоятельства, которые облегчили ему совершение преступной акции, каким образом ему стало известно об этих обстоятельствах и как именно он их использовал.

Круг свидетелей, который должен быть опрошен, зависит от характера обстоятельств, способствовавших преступлению. В нашем случае это работники, осуществляющие взаимодействие с компьютерной информацией (операторы, ремонтники, администраторы сетей и т.д.), лица, обеспечивающие безопасность компьютерных систем и помещений, а также работники бухгалтерии, кадровых служб и т.д.

В ходе всех этих следственных и розыскных действий следователем могут быть использованы самые разнообразные индивидуально-воспитательные и иные методы, направленные на перестройку психологии личности, психологического микроклимата в малой социальной группе, изменение условий жизни и труда, в которых живет и действует личность, функционирует малая социальная группа.

Следственный эксперимент позволяет получить сведения о способе преступления и способствующих его совершению обстоятельствах: о недостатках программных и аппаратно-технических средств, используемых преступником, путях использования уязвимых мест в охране объектов, в том или ином технологическом процессе обработки информации, контроле за процессами хранения, обработки и передачи информации и т.п.

При проведении следственного эксперимента желательно участие специалиста.

Вопросы о способствовавших рассматриваемому преступлению обстоятельствах целесообразно ставить при проведении компьютерно-технической экспертизы. В ходе последней могут быть выявлены причины сбоев в работе ЭВМ, уничтожения или модификации информации и другие. Результатом экспертизы может стать и выяснение вопроса, не является ли причиной таких последствий вредоносная программа. Вопрос об обстоятельствах, способствовавших преступлению, может быть поставлен перед экспертом в прямой форме, но о них можно судить и по отве-

там на другие вопросы. Подобные обстоятельства могут быть установлены экспертом и по собственной инициативе. В этом случае эксперт сообщает о них в своем заключении.

Кроме установления обстоятельств совершения преступлений в сфере компьютерной информации в криминалистике разработаны и иные средства, позволяющие обеспечить эффективность предупредительных мер и защиту объектов, на которых используются компьютерные системы, от иных преступных посягательств, которые могут быть совершены в случае неустранения выявленных недостатков в сфере обеспечения безопасности компьютерной информации.

Сведения о начавшемся или готовящемся преступлении поступают к следователю в процессе расследования уголовного дела либо к оперативным работникам в процессе оперативно-розыскной деятельности. В качестве профилактических мер в данных случаях могут применяться средства процессуального и непроцессуального воздействия (задержание с поличным, изменение характера режима охраны, системы контроля и т.д.).

В настоящее время существуют различные технико-криминалистические средства и методы, которые не менее эффективно могут быть использованы в предупреждении преступлений. Разработка и применение соответствующих технических приемов и средств защиты осуществляются с привлечением специалистов технического профиля. При этом одни технические приемы и средства используются с целью пресечения реально подготовленной к началу или уже начатой преступной деятельности (различного рода сигнализационные и блокирующие устройства, приемы и средства распознавания модификации и подмены программных средств и др.), другие направлены на затруднение совершения преступлений (приемы и средства защиты программ и данных, средства, препятствующие подбору идентификационных данных законных пользователей, различные технические устройства аутентификации пользователей и др.), третьи – для быстрого обнаружения виновных и объектов преступных посягательств (различные программные ловушки, программы контроля доступа и т.д.).

Статья 158 УПК РФ регламентирует порядок внесения следователем представлений в соответствующую организацию или соответствующему должностному лицу о принятии мер по устранению указанных обстоятельств или других нарушений закона. Меры по представлению должны быть приняты не позднее чем в месячный срок со дня его вынесения, и о результатах сообщено лицу, направившему представление с указанием, какие и кем конкретно приняты меры.

Это не весь спектр возможных профилактических мер, которые могут быть проведены самим следователем и другими участниками расследования либо по их поручению. Конкретные профилактические методы и средства должны выбираться в зависимости от обстоятельств конкретного уголовного дела, наличествующих сил и средств для их осуществления.

Лишь комплексное и целенаправленное проведение следователем, оперативными работниками мероприятий, направленных на предотвращение совершения преступлений и пресечение совершаемых, может позволить правоохранительным органам достигнуть успеха в деле предупреждения преступлений в целом и преступлений в сфере компьютерной информации в частности.

Литература

1. *Махтаев, М.Ш.* Основы теории криминалистического предупреждения преступлений: монография. – М.: Раритет, 2001; Криминалистика : учебник. / отв. ред. Н.П. Яблоков. – М. : Юристъ, 2001. – Глава 6;

2. *Аверьянова, Т.В., Белкин, Р.С.*, *Корухов, Ю.Г.*, *Россинская, Е.Р.* Криминалистика : учебник для вузов, 1999. – Глава 57.

3. Криминалистика : учебник / отв. ред. Н.П. Яблоков, 2001.

4. *Вехов, В.Б.* Компьютерные преступления : способы совершения и раскрытия / под ред. акад. Б.П. Смагоринского. – М. : Право и Закон, 1996.

5. *Крылов, В.В.* Расследование преступления в сфере информации. – М. : Издательство «Городец».

6. *Курушин, В.Д., Минаев, В.А.* Компьютерные преступления и информационная безопасность. – М. : Новый Юрист, 1998.