УГОЛОВНОЕ ПРАВО, КРИМИНАЛИСТИКА И КРИМИНОЛОГИЯ

УДК 343.97:004 DOI: 10.15507/VMU.024.201403.042

СПОСОБЫ СОКРЫТИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

П. В. Малышкин

В статье указывается на то, что успех расследования преступлений, совершенных с применением информационных компьютерных технологий, зависит от успеха преодоления противодействия этому расследованию. При этом необходимо отметить, что преимущественное использование преступных инсценировок не предполагает того, что другие способы сокрытия преступлений, при совершении которых применялись информационные компьютерные технологии, не применяются. Не менее распространенными в последнее время стали отвлекающие от совершенного преступления хакерские атаки. Кроме этого, одной из разновидностей противодействия расследованию указанных преступлений является имитация технического сбоя. Информационные технологии развиваются, а вместе с ними совершенствуются и способы сокрытия преступлений, совершенных с применением этих технологий. Самым распространенным способом сокрытия данных преступлений является преступная инсценировка, которая подробно анализируется в статье. Одной из основных особенностей преступлений, совершенных с применением информационных компьютерных технологий, является то, что способ и механизм их совершения, как правило, предполагает включение действий, направленных на сокрытие совершаемого преступления. Преступник в этом случае стремится к тому, чтобы совершенное им преступление не было выявлено. Кроме этого, рассматриваются и другие способы сокрытия преступлений, совершенных с применением информационных компьютерных технологий.

Ключевые слова: противодействия расследованию преступлений, преступление, совершенное с применением информационных компьютерных технологий, сокрытие преступления, преступная инсценировка.

MEASURES OF CRIME CONCEALING WITH USE OF INFORMATION TECHNOLOGIES

P. V. Malyshkin

The article reveals the importance of effectiveness of countermeasures against resistance to investigation. It should be noted that dominating usage of criminal staging does not assume non-application of other concealing measures with use of information technologies. They are in use too, but much more seldom than staging. Besides, hacker attacks, made for distracting from a committed crime, obtain currency. One of countermeasures against investigation is concealing measures with use of information technologies, such as imitation of technical malfunction. Information technologies develop, and so do the concealing measures. One of peculiarities of computer crimes is the fact that the way and the mechanism of committing of it usually includes actions, aimed at concealing of the crime, in the first instance, hiding of a fact of a crime. The article also deals with other concealing measures with use of information technologies.

Keywords: resistance to crime investigations, crimes committed with the use of information technologies, ways of concealing crimes, criminal staging.

В настоящее время имеются все основания полагать, что значительная часть преступлений, совершенных с применением информационных компьютерных технологий, остается нераскрытой вследствие высокой эффективности оказанного расследованию информационно-технологического противодействия. Таким образом, «главной проблемой в борьбе с преступлениями в сфере компьютерной информации является то, что выявляется их правоохранительными органами гораздо меньше, чем совершается» [4, с. 172]. Это является справедливым не только по отношению к преступлениям в сфере компьютерной информации, но и ко всем преступлениям, при совершении которых используются компьютерные технологии.

Одной из основных особенностей таких преступлений является то, что способ и механизм их совершения, как правило, уже на начальном этапе предполагает включение действий, направленных на сокрытие. В этом случае преступник стремится прежде всего к тому, чтобы совершенные им противоправные действия не были обнаружены. Для этих целей, как правило, используются достаточно сложные, с технической точки зрения, средства, которые чаще всего представляют собой новейшее программное обеспечение. Сложность этих средств является залогом того, что преступление не будет замечено правоохранительными органами. Справедливо отмечается, что «наиболее частым способом инсценировки является то, что преступник использует технические возможности компьютерных сетей и специальные программы для того, чтобы при обнаружении преступления следы, оставленные в сети, указывали не на него (или, точнее, его компьютер), а на совершенно другое лицо, которое может и не подозревать о совершении этого преступления» [3, с. 90]. В этом случае преступник достигает прежде всего анонимности, что обеспечивает безнаказанность и возможность в последующем совершать аналогичные действия. Очевидно, что длительное их совершение ведет к тому, что преступники улучшают применяемые ими способы и средства. Таким образом, постепенно достигается настолько высокий уровень преступлений, что их обнаружение становится для правоохранительных органов более проблематичным. Очевидно, именно в этом отчасти кроется причина высокой латентности преступлений, совершенных с применением информационных компьютерных технологий.

Для того чтобы скрыть свою личность, преступник прибегает к специальным программам, созданным с учетом принципа так называемой «луковичной маршрутизации» (tor), используемой для передачи информации в глобальной сети Интернет. Данная технология позволяет сохранять анонимность при посещении сайтов, публикации материалов, отправке сообщений благодаря созданию сети маршрутизаторов (серверов-«посредников»), через которые устанавливается соединение. Учитывая, что таких «посредников» много и значительная их часть находится за пределами одного государства, то правоохранительным службам этого государства бывает сложно установить как потребителя информации с того или иного сайта, так и того, кто ее на нем оставил. Отметим, что устанавливаемая цепочка связи шифруется. Все это делает установление личности того, кто использует подобную программу, почти невозможным.

Существует другие способы обеспечения анонимности в глобальной сети. Например, с помощью веб-прокси, суть которых состоит в том, что услуга анонимности предоставляется определенными веб-сайтами. Еще один способ предполагает заражение вирусом соответствующего сайта или адреса электронной почты конкретного пользователя и позволяет добиться сразу двух целей: преступного результата и сохранения анонимности. Необходимо отметить, что действия, направленные на

сокрытие преступлений с применением информационных компьютерных технологий, не ограничиваются названными способами. Информационные технологии постоянно развиваются, а вместе с ними совершенствуются способы сокрытия подобных преступлений. Более того, бурное развитие этих технологий способствует появлению принципиально новых способов. Именно поэтому в настоящее время не представляется возможным составить их исчерпывающий перечень.

Одним из распространенных методов сокрытия преступлений, совершенных с применением информационных компьютерных технологий, является имитация технического сбоя, который, как правило, связан с перебоями в энергоснабжении или несовместимостью программного обеспечения. В последнем случае они могут приводить к завершению работы программ, «зависанию» компьютера и даже утрате части информации. Имитация такой несовместимости иногда используется преступниками для уничтожения определенных сведений или «взлома» защиты с целью совершения противоправных действий. Существуют и другие виды сокрытия преступлений. Их выбор во многом зависит от особенностей совершенного деяния, или используемого программного обеспечения, или от особенностей (прежде всего интеллектуальных) того лица, которое планирует и организует сокрытие.

Одной из разновидностей сокрытия преступлений является преступная инсценировка. В. И. Фадеев определяет ее как «деятельность субъекта преступления по сокрытию (видоизменению) совершенного преступления (аморального поступка) и (или) совершению преступления, характеризующаяся умышленным созданием ложной субъектной, предметной, пространственной, временной, информационной, следовой обстановки, скрывающей умысел и цели преступника» [6, с. 26]. Сопоставление данного определения с практикой расследования преступлений, совершенных с применением информационных компьютерных технологий, заставляет усомниться в возможности распространения данного определения на рассматриваемую область. Прежде всего, возникает сомнение, что преступная инсценировка является результатом деятельности только субъекта преступления. Анализ практики расследования позволяет утверждать, что не только субъекты преступления участвуют в преступных инсценировках; к ним могут привлекаться лица, не подозревающие о том, что было совершено преступление. Так, преступник (преступники) может привлекать программистов к тому, чтобы модернизировать то или иное программное обеспечение, согласно конкретным нуждам потребителя. При этом перед специалистами могут быть поставлены такие задачи по улучшению программного обеспечения, выполнение которых позволит не только успешно совершить преступление, но и инсценировать его. Например, известно, что программное обеспечение анонимности в настоящее время используется для того, чтобы преодолевать цензуру в Интернете. Отметим, что оно способно не только обеспечить анонимность, но и преодолеть блокировку отдельных сайтов.

Умелая модификация соответствующих программ способна привести к тому, что они смогут преодолевать защиту отдельных сайтов, банковских счетов и т. д. При этом такое преодоление, как правило, инсценирует источник, из которого была произведена атака. Очевидно, что программист в данном случае не является субъектом преступления, однако именно благодаря его участию преступная инсценировка стала возможной, поэтому его деятельность по модификации программного обеспечения также следует рассматривать причастной к преступлению.

Не менее распространенными в последнее время стали отвлекающие хакерские атаки. Как правило, они проводятся достаточно организованно, но при этом

многие их участники не знают истинных целей организаторов этих атак и руководствуются не стремлением добиться какого-либо преступного результата, а своего рода «спортивным» интересом, возможностью продемонстрировать силу своего интеллекта. Однако именно они способствуют преступной инсценировке. В последнее время достаточно распространенными стали преступления по хищению средств с банковских счетов. Достаточно часто их скрывают именно с помощью хакерской атаки.

Существуют и другие случаи, когда то или иное лицо, не являясь субъектом преступления, участвует (часто не осознавая этого) в совершении преступной инсценировки. Так, учитывая, что социальная среда благоволит киберпреступникам, находится немало пользователей компьютерных сетей, которые готовы бескорыстно содействовать этим преступникам в инсценировке или любом другом способе сокрытия совершенного ими преступления. Отчасти это объясняется тем, что внутри различных категорий компьютерных пользователей наблюдается солидарность, проявляющаяся в готовности помочь другому такому же пользователю в трудную для него минуту, не разбираясь при этом в сути тех причин, по которым эти трудности возникли. Главным для них в этом случае является осознание того, что киберпреступник – пользователь, относящийся к аналогичной категории. При этом такие лица могут не иметь личного знакомства с преступником и, соответственно, не знать о его преступных намерениях. Очевидно, что они также не являются субъектами преступления, однако их роль в инсценировке может быть значительной.

Все виды преступной инсценировки во многом обусловлены спецификой отношений, возникающих между пользователями глобальных сетей и далеко не всегда основанных на корысти. К сожалению, такая среда часто используется как для совершения преступлений с применением высоких технологий, так и для их сокрытия. По этой причине нельзя ограничивать круг лиц, которые могут быть причастными к инсценировке только субъектами преступления. В связи с этим мы считаем, что определение инсценировки, данное Р. С. Белкиным, в большей мере отображает реалии совершения преступлений с применением информационных компьютерных технологий. Так, он писал, что инсценировка преступлений – это «создание обстановки, не соответствующей фактически происшедшему на этом месте событию; может дополняться ложным поведением и ложными сообщениями» [1, с. 83]. При этом ученый отмечал, что все инсцинировки классифицируются «по субъекту – совершаемые преступником(ами) или иными лицами» [Там же]. Очевидно, Р. С. Белкин не считал правильным ограничивать понятие инсценировок только теми из них, которые совершены субъектами преступления.

Такой подход мы считаем наиболее целесообразным. Р. С. Белкин также полагал, что инсценировка относится к смешанным способам сокрытия преступлений: «Смешанные способы сокрытия преступления представлены в следственной практике различными инсценировками или, по старой терминологии, различными видами симуляции обстоятельств преступления» [2, с. 368]. При этом справедливо замечание о том, что в «инсценировках могут присутствовать элементы и фальсификации, и утаивания, и уничтожения, и маскировки» [5, с. 374].

Применение конкретного способа сокрытия зависит от вида соответствующего преступления. Таким образом, совершение определенного вида преступления позволяет с высокой степенью вероятности предположить примененным способ его сокрытия, то есть в какой-то степени способ сокрытия и конкретный вид преступления идентифицируют друг друга. Следует отметить, что среди способов сокрытия преступлений, совершенных с применением инфор-

мационных компьютерных технологий, наиболее распространенным является преступная инсценировка, поскольку эффективность других не настолько высока. Так, например, утаивание, уничтожение или маскировку информации достаточно легко обнаружить с помощью соответствующих программ. Кроме того, преступления, при совершении которых применяются информационные компьютерные технологии, в силу своих особенностей предполагают преимущественное использование преступных инсценировок, поскольку они позволяют как сохранить анонимность, так и достигнуть преступного результата. При этом совершение преступной инсценировки предполагается преступниками уже на стадии планирования преступления.

Отдельные действия, составляющие преступление, могут быть не только элементами данного преступления, но и одновременно являться частью системы, составляющей инсценировку. Особенностью в этом случае является то, что если нет возможности создания инсценировки, то преступник может отказаться от совершения соответствующего преступления. Таким образом, возможность создания преступной инсценировки является одним из условий совершения преступлений, в которых применяются информационные компьютерные технологии.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. **Белкин, Р. С.** Криминалистическая энциклопедия / Р. С. Белкин. – Москва : БЕК, 1997 . – С. 83.

2. **Белкин, Р. С.** Курс криминалистики : в 3 т. : Криминалистические средства, приемы и рекомендации / Р. С. Белкин. – Москва : Юристъ, 1997. – Т. 3. – С. 368.

3. **Косынкин, А. А.** Преодоление противодействия расследованию преступлений в сфере компьютерной информации / А. А. Косынкин. – Москва : Юрлитинформ, 2013. – С. 90.

4. **Подольный, Н. А.** Проблемы оптимизации расследования преступлений в сфере компьютерной информации / Н. А. Подольный // Раскрытие и расследование преступлений, сопряженных с использованием средств вычислительной техники, проблемы, тенденции, перспективы. – Москва : МАКС Пресс, 2005. – С. 172.

5. **Подольный, Н. А.** Теоретические и практические основы раскрытия и расследования преступлений, совершенных молодежными организованными группировками : дис. на соиск. учен. степ. д-ра юрид. наук / Н. А. Подольный. – Москва, 2007. – С. 374.

6. **Фадеев, В. И.** Расследование криминальных инсценировок / В. И. Фадеев. – Москва : Норма, 2007. – С. 26.

Поступила 11.03.2014 г.

Об авторе:

Малышкин Павел Викторович, доцент кафедры правоведения Ковылкинского филиала ФГБОУ ВПО «Мордовский государственный университет им. Н. П. Огарёва» (Россия, г. Ковылкино, ул. Желябова, д. 26), кандидат юридических наук, kriminalistika kaf_upkk@mail.ru

Для цитирования: Малышкин, П. В. Способы сокрытия преступлений, совершаемых с применением информационных компьютерных технологий / П. В. Малышкин. – Вестник Мордовского университета. – 2014. – № 4. – С. 42–47. DOI: 10.15507/VMU.024.201403.042

REFERENCES

1. Belkin R. S. Kriminalisticheskaja jenciklopedija [Criminalistic encyclopedia]. Moscow, BEK Publ., 1997, p. 83.

2. Belkin R. S. Kurs kriminalistiki: v 3 t.: Kriminalisticheskie sredstva, priemy i rekomendacii [Criminalistics course in 3 volumes: criminalistics measures, techniques and recommendations]. Moscow, Jurist Publ., 1997, vol. 3, 368 p.

3. Kosynkin A. A. Preodolenie protivodejstvija rassledovaniju prestuplenij v sfere komp'juternoj informacii [Surmounting the resistance to investigation in computer crimes]. Moscow, Jurlitinform Publ., 2013, 90 p.

4. Podol'nyj H. A. Problemy optimizacii rassledovanija prestuplenij v sfere komp'juternoj informacii. Raskrytie i rassledovanie prestuplenij, soprjazhennyh s ispol'zovaniem sredstv vychislitel'noj tehniki, problemy, tendencii, perspektivy [Issues of optimization of computer crimes investigation. Computer crimes investigation: problems, tendencies, prospects]. Moscow, MAKS Press Publ., 2005, 172 p.

5. Podol'nyj N. A. Teoreticheskie i prakticheskie osnovy raskrytija i rassledovanija prestuplenij, sovershennyh molodezhnymi organizovannymi gruppirovkami: dis. na soisk. uchen. step. d-ra jurid. Nauk [Theoretical and practical principles of investigation of crimes, committed by youth criminal groups: Doc. Jur. Sci. diss.]. Moscow, 2007, 374 p.

6. Fadeev V. I. Rassledovanie kriminal'nyh inscenirovok [Investigation of criminal stagings]. Moscow, Norma Publ., 2007, 26 p.

About the author:

Malyshkin Pavel Viktorovich, Associate professor of Law chair, Ogarev Mordovia State University, Kovylkino campus (Russia, Kovylkino, 26 Zheljabova Str.), Candidate of Sciences (PhD) degree holder in Law, kriminalistika_kaf_upkk@mail.ru

For citation: Malyshkin P. V. Sposoby sokrytija prestuplenij, sovershaemyh s primeneniem informacionnyh komp'juternyh tehnologij [Measures of crime concealing with use of information technologies]. *Vestnik Mordovskogo Universiteta* – Mordovia University Bulletin, 2014, no. 4, pp. 42–47. DOI: 10.15507/VMU.024.201403.042