Хлус, А. М. Тенденции развития методического обеспечения расследования преступлений против критической информационной инфраструктуры / А. М. Хлус // Актуальные проблемы развития российского законодательства и практика его применения : сборник научных статей по результатам Всероссийской науч.-практ. конф. с международным участием «Актуальные проблемы развития российского законодательства и практика его применения», 15 – 16 ноября 2022 г. [Электронное издание] / под общ. ред. К. Г. Дедюхина; под науч. ред. И. И. Аминова, А. А. Николаевой; Ижевский институт (филиал) ВГУЮ (РПА Минюста России). – Ижевск: Ижевский институт (филиал) ВГУЮ (РПА Минюста России), 2022. – Электрон., текстовые данные (3 643 КБ). – 1 электр. опт. диск (CD-ROM). – С. 1397–1406.

ТЕНДЕНЦИИ РАЗВИТИЯ МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ПРОТИВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

TRENDS IN THE DEVELOPMENT OF METHODOLOGICAL SUPPORT FOR THE INVESTIGATION OF CRIMES AGAINST CRITICAL INFORMATION INFRASTRUCTURE

Хлус Александр Михайлович,
доцент, кандидат юридических наук,
Белорусский государственный университет, город Минск,
доцент кафедры криминалистики
E-mail: hlus.home@mail.ru

Аннотация: Проведенный анализ криминалистической характеристики неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации позволил автору сделать вывод, что содержание данной научной категории не дает полного криминалистического представления об этом виде преступлений и не может служить надёжной основой для построения методики их расследования. В основу совершенствования криминалистической характеристики должны быть положены сведения о типичных элементах материальной структуры рассматриваемого вида преступлений.

Ключевые слова: уголовное право; критическая информационная инфраструктура; компьютерная информация; криминалистика; криминалистическая характеристика; материальная структура преступления.

Abstract: The analysis of the forensic characteristics of unlawful impact on the critical information infrastructure of the Russian Federation allowed the author to conclude that the content of this scientific category does not provide a complete forensic understanding of this type of crime and cannot serve as a reliable basis for constructing a methodology for their investigation. The basis for improving the forensic characteristics should be based on information about the typical elements of the material structure of the type of crime in question.

Keywords: criminal law; critical information infrastructure; computer information; criminalistics; forensic characteristics; the material structure of the crime.

В последнее время увеличилось количество компьютерных атак на информационные инфраструктуры государственных органов и иных организаций. В связи с этим уголовный кодекс Российской Федерации (далее УК РФ) в главе 28 «Преступления в сфере компьютерной информации» дополнен специальной статьей 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации». Данной нормой криминализирован ряд деяний. Во-первых, речь идет о преступлениях, связанных с созданием, распространением и (или) использованием компьютерных программ либо иной информации, предназначенных для воздействия на критическую информационную инфраструктуру (далее КИИ), в том числе для уничтожения, блокирования, модификации, копирования информации. Во-вторых, криминализирован неправомерный доступ к охраняемой компьютерной информации, связанный с причинением вреда КИИ Российской Федерации. Неправомерный доступ также может быть осуществлен с использованием компьютерных программ либо иной компьютерной информации. В-третьих, уголовная ответственность по указанной статье наступает и за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации,

содержащейся в КИИ, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к КИИ Российской Федерации, либо правил доступа к ним при условии причинения вреда КИИ Российской Федерации.

Криминализация указанных деяний обусловлена Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» № 187-ФЗ от 26 июля 2017 (далее ФЗ «О безопасности КИИ») [5], принятие которого вызвано всплеском кибератак с одновременным распространением компьютерных вирусов, поразивших информационную инфраструктуру многих государственных органов и учреждений, и крупных российских фирм («Сбербанк», «Роснефть» и др.).

Действующее законодательство Республики Беларусь также предусматривает меры противодействия злоумышленникам в сфере информационных технологий. Постановлением Совета Безопасности Республики Беларусь в 2019 г. утверждена Концепция информационной безопасности Республики Беларусь [6]. Согласно п. 8 данной концепции информационная инфраструктура представлена как «совокупность технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации». Информационная инфраструктура наряду с информацией, легальными субъектами, осуществляющими ее сбор, формирование, распространение и использование является элементом информационной сферы, представляющей криминальный интерес. В уголовном кодексе Республики Беларусь (далее УК) [8] криминализированы деяния, совершаемые в информационной сфере. Они обобщены в главе 31 «Преступления против компьютерной безопасности». В ней предусмотрена ответственность за следующие деяния: «Несанкционированный доступ к компьютерной информации» (ст. 349 УК), «Уничтожение, блокировка и модификация компьютерной информации» (ст. 350 УК), «Неправомерное завладение компьютерной информацией» (ст. 352 УК), «Разработка, использование, распространение либо сбыт вредоносных компьютерных

программ или специальных программных или аппаратных средств» (ст. 354 УК), «Нарушение правил эксплуатации компьютерной системы или сети» (ст. 355 УК).

Имеющиеся расхождения в наименовании глав и конструкций соответствующих им норм уголовных кодексов Российской Федерации и Республики Беларусь не свидетельствует о различии сущностной направленности на противодействие преступлениям, совершаемым в информационной сфере. Отсутствие в белорусском законодательстве понятия «критическая информационная инфраструктура» также не препятствует активному противодействию преступлениям, посягающим на нее. По мнению российских ученых понятие «критическая» имеет отношение к «инфраструктуре, которая при выведении из строя или разрушении приведет к катастрофическому и далеко идущему ущербу» [7, с. 101–102].

Условиями эффективной борьбы с преступлениями, совершаемыми в информационной сфере, является четкая формулировка предписаний, содержащихся в уголовной статье и наличие соответствующей методики их расследования. По мнению ученых, низкая эффективность борьбы с преступлениями, предусмотренными ст. 274.1 УК РФ, обусловлена неопределенностью содержащихся в ней предписаний [3]. Что касается методических рекомендаций по расследованию, то следует отметить их недостаточную разработанность, учитывая специфику сферы совершения преступлений данного вида.

По сложившей традиции формирование криминалистических методик основывается на криминалистической характеристике преступлений определенного вида или группы. Для объективного криминалистического описания криминального деяния, т. е. его характеристики необходимо опираться на эмпирические данные, полученные в ходе изучения по возможности значительного количества расследованных уголовных дел. Практика расследования уголовных дел по ст. 274.1 УК РФ «крайне мала» [1, с. 59]. В Беларуси, несмотря на тенденцию роста преступлений, совершаемых в

информационной сфере, количество раскрытых и расследованных аналогичных уголовных дел также не велико. Все это результат сложности выявления и расследования преступлений данной категории.

Отсутствие достаточной эмпирической базы не позволяет в полной мере представить криминалистическую характеристику преступления, предусмотренного ст. 274.1 УК РФ. Тем не менее, о комплексной характеристике данного преступного деяния речь идет в статье Ф. А. Голубева. Несмотря на название статьи, где указано на криминалистическую характеристику расследования [1, с. 50], автор дает описание отдельным, криминалистически значимым элементам. В их числе названы субъекты КИИ и преступления, объект и предмет преступления, и его последствия, связанные с причинением вреда КИИ. Кроме того, Ф. А. Голубев рассматривает объективную и субъективную стороны деяния. Он также указал на необходимость изучения обстановки совершения данных преступлений, которой является «недостаточная информационная и иная защита объектов КИИ РФ», а ее установление «важно для их предупреждения и профилактики» [1, с. 59].

В качестве субъектов КИИ названы государственные органы и учреждения, юридические лица и индивидуальные предприниматели, владеющие на законном основании информационными системами или автоматизированными системами управления, информационно-телекоммуникационными сетями в различных сферах деятельности. К этим сферам, определенным ст. 2 ФЗ «О безопасности КИИ», относятся, например, здравоохранение, энергетика, наука, оборонная, горнодобывающая, химическая промышленность и др. В процессе следственной деятельности решение вопроса о том, относится ли данный субъект к субъектам КИИ возможно на основании изучения различных документов. Такими документами являются, например, общероссийский классификатор видов экономической деятельности, лицензии на деятельность, определенную классификатором и др.

Субъект и объект преступления в криминалистической характеристике представлены с позиции уголовного права. Субъект – это «вменяемое физическое лицо, которое достигло 16 летнего возраста», а объектом являются «общественные отношения, складывающиеся при обеспечении нормальной работы, функционирования электронных вычислительных машин, сетей и систем электронных вычислительных машин, которые относятся к объектам КИИ Российской Федерации» [1, с. 53–55].

В качестве предмета преступлений, предусмотренных ст. 274.1 УК РФ, автор рассматриваемой криминалистической характеристики называет «технические средства, которые используются для хранения, обработки и передачи компьютерной информации (ЭВМ, сети и системы ЭВМ, носители информации), которая относится к КИИ Российской Федерации» [1, с. 55].

Анализ криминалистической характеристики преступления, предусмотренного ст. 274.1 УК РФ, позволяет сделать вывод, что ее содержание преимущественно наполнено сведениями из специального закона о безопасности КИИ и уголовного права и в меньшей степени она отражает собственно криминалистические данные. Такой подход к описанию преступления не обеспечивает представление о нем с позиций криминалистической науки и не способствует определению направлений поиска следов в практической деятельности по расследованию.

Нам представляется, что в основу разработки криминалистической характеристики любого криминального деяния должны быть положены сведения о его материальных составляющих. Именно они дают возможность познать преступление в процессе его расследования, основываясь на следовой картине, ими отражаемой.

Данная идея базируется на криминалистическом учении о материальной структуре преступления [2]. В ее основе представление о том, что система преступления состоит из ряда материальных элементов, вступающих во взаимосвязь в момент его совершения.

Учитывая положения упомянутого учения, рассмотрим материальные составляющие анализируемого преступления. В его материальной структуре можно выделить следующие материальные составляющие: субъект, совершающий преступное деяние, объект и предмет преступного посягательства, средства совершения преступления.

Субъектом данного, в равной степени, как и любого другого преступления, является человек, реализующий преступный замысел индивидуально либо в составе группы, т. е. деяние совершается несколькими лицами. Особенность субъекта рассматриваемого преступления в наличии у него специальных знаний в области компьютерной техники и информационных технологий. В преступной системе субъект вступает во взаимодействие с иными структурными элементами, оставляя на них следы преступных действий. Эти следы могут быть обнаружены на средствах, которые использовались для воздействия на КИИ, в информационных системах, подвергшихся воздействию. Следует иметь в виду, что средства воздействия на КИИ отражают следы-действия (применение вредоносной программы) и материальные следы использования средства.

Субъекты неправомерного воздействия на КИИ подразделяются на две группы: внешние по отношению к объекту посягательства и внутренние, на которых возложены обязанности по соблюдению правил обслуживания объекта КИИ (ч. 3 ст. 274.1 УК РФ).

Объектом преступного посягательства с позиции криминалистики следует считать материальную систему, на которую направлены преступные действия субъекта.

Основываясь на учении о материальной структуре, учитывая положения ФЗ «О безопасности КИИ», формирующего понимание критической информационной инфраструктуры, в качестве объектов посягательства можно представить информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления. Данные «системы» и «сети» представляют собой непосредственный объект

преступного посягательства. Но в широком понимании объектом для рассматриваемых преступлений являются организации, которым причиняется имущественный и иной вред, т. е. те «субъекты критической информационной инфраструктуры», структурным звеном которых выступают указанные «системы» и «сети». На данные «системы» и «сети» оказывается неправомерное воздействие, в результате которого образуются следы. Криминалистическое исследование следовой информации, отраженной на объекте посягательства, обеспечивает познание иных, неизвестных элементов материальной структуры.

В тесной связи с объектом находится предмет преступного посягательства, в качестве которого нами понимается такой материальный элемент преступной системы, определяющий целевую направленность деяния. На основе анализа ч. 1 и 2 ст. 274.1 УК РФ можно сделать вывод, что предметом преступного посягательства выступает информация, которая в результате неправомерного воздействия на КИИ может быть уничтожена, заблокирована, модифицирована или скопирована либо использована злоумышленником.

Неправомерное воздействие на КИИ предполагает обязательное использование средств совершения преступления. В их качестве надо понимать материальные системы, обеспечивающие неправомерное воздействие на объект и достижение цели доступа к компьютерной информации. Под доступом к информации «понимается проникновение в ее источник с использованием средств (вещественных и интеллектуальных) компьютерной техники» [4]. Средствами неправомерного воздействия на КИИ являются компьютерные программы либо иная компьютерная информация (ч. 1 ст. 274.1 УК РФ), а также компьютерная и иная техника, обеспечивающая неправомерный доступ к охраняемой компьютерной информации (ч. 2 ст. 274.1 УК РФ).

Выделение элементов материальной структуры рассматриваемого преступления не является самоцелью и не противопоставляется учению о криминалистической характеристике. Для формирования теоретической основы построения частной методики расследования необходимо, по нашему мнению,

первоначально рассмотреть типичные элементы материальной структуры преступления, которые затем подлежат описанию (характеристике) в аспекте криминалистически значимой для расследования информации. Такое сочетание двух различных по своей сути криминалистических научных категорий можно представить в виде «криминалистической характеристики материальной структуры преступлений».

На основе выше рассмотренного для обсуждения предлагаются следующие выводы:

Во-первых, криминалистическая характеристика неправомерного воздействия на КИИ не дает полного представления о данном виде преступлений и не может служить надёжной основой для построения методики его расследования, и, соответственно, для методического обеспечения следственной деятельности.

Во-вторых, в основу криминалистической характеристики неправомерного воздействия на КИИ должны быть положены сведения о типичных элементах материальной структуры данного вида преступлений.

Список литературы

1. Голубев Ф. А. Криминалистическая характеристика расследования неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации // Право и политика. 2020. № 10. С. 50–59. DOI: 10.7246/2454-0706.2020.10.33985. URL: https://nbpublish.com/library_read_artikle.php?id=33985 (дата обращения: 06.11.2022).

2. Гучок А. Е. Основы криминалистического учения о материальной структуре преступления. Минск: Тесей, 2012. 228 с.

3. Кругликов Л. Л., Соловьев О. Г., Бражник С. Д. Ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274. 1 УК РФ) в системе экономической и информационной безопасности / URL: https://j.uniyar.ac.ru/index.php/vyrgu/artikle/view/894 (дата обращения: 03.11.2022].

4. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации / URL: https://www.consultant.ru/dokument/cons_doc_law_16181/2e

91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100027 (дата обращения: 06.11.2022).

5. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26 июля 2017. № 187-ФЗ / URL: https://www.consultant.ru/dokument/cons_doc_LAW_220885/c5051782233acca771e9adb35b47d3fb82c9ff1c/ (дата обращения: 06.11.2022).

6. О Концепции информационной безопасности Республики Беларусь : утв. Постановлением Совета Безопасности Республики Беларусь 18 марта 2019 № 1 / URL: https://pravo.by/ dokument/?guid=12551&p0=P219s0001&p1=1 (дата обращения: 06.11.2022).

7. Трунцевский Ю. В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. 2019. № 5. С. 99–106.

8. Уголовный кодекс Республики Беларусь от 9 июля 1999 г. № 275-З / URL: https://pravo.by/ dokument/?guid=3871&p0=hk9900275 (дата обращения: 05.11.2022).