он может рассматриваться преимущественно как следообразующий элемент. В качестве следовоспринимающего элемента его можно рассматривать по отношению только к средству совершения преступления.

Объектом преступного посягательства является компьютерная система, сети или машинные носители информации.

Средством совершения преступления являются компьютерная техника, программные (аппаратные) средства, обеспечивающие доступ к защищенной компьютерной системе или сети, вредоносные программы.

Предметом преступного посягательства являются компьютерная информация (программа). В качестве предмета может выступать также компьютерное оборудование, компьютерная система, сеть или машинный носитель информации.

Выделение элементов криминалистической структуры преступлений против информационной безопасности, а затем их анализ обеспечивают наиболее полное и объективное познание конкретного преступления.

При развитии следственной ситуации, когда субъект преступления не известен, познание его и других элементов структуры конкретного преступления против информационной безопасности начинается с исследования объекта посягательства. Исследование компьютерной системы, сети или машинных носителей информации посредством изучения следов преступления позволяет выявить особенности обстановки преступного посягательства и установить конкретный способ совершения преступления.

Система следов, отразившихся на объекте преступного посягательства от иных структурных элементов преступления, образует так называемую следовую картину, сведения о которой являются элементом криминалистической характеристики [6, с. 237]. Анализ специфики формирования следовой картины при совершении преступлений против информационной безопасности позволяет сделать вывод, что в качестве следов могут выступать: изменения исходной информации на магнитных и оптических носителях; следы уничтожения или блокирования информации; следы опосредованного доступа к ней с помощью глобальных или локальных компьютерных сетей [6, с. 247]. Нетрадиционный характер этих следов привел к предложению ввести понятие «виртуальный след», под которым понимается «зафиксированный компьютерной системой на цифровом материальном носителе результат отражения реального физического процесса или действия иной компьютерной системы, связанный с преступлением (имеющий уголовно-релевантное значение), в виде цифрового образа формальной (математической) модели этого процесса» [7, с. 59].

На основе изучения следовой картины конкретного преступления выявляется связь между способом совершения преступления, свойствами субъекта посягательства и обстановкой, в которой совершено преступное деяние данным способом.

Сведения о способе и обстановке совершения преступления образуют информационную основу криминалистической характеристики преступлений против информационной безопасности. Их использование при исследовании объекта преступного посягательства позволяет следователю выдвинуть наиболее вероятную версию о субъекте преступного посягательства. Так, например, для крэкеров характерно использование способов, направленных на получение несанкционированного доступа к компьютерной информации [6, с. 238]. Для таких субъектов преступного посягательства основной задачей является взлом компьютерной системы с целью получения несанкционированного доступа к чужой информации.

1. Белкин Р.С. Курс криминалистики. В 3 т. Т. 3. Криминалистические средства. Приемы и рекомендации. М., 1997.

2. Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М. : НОРМА, 2001.

3. Криминалистика : учеб. пособие для вузов / А.В. Дулов [и др.] ; под общ. ред. А.В. Дулова. Минск : НКФ «Экоперспектива», 1996.

4. Гучок А.Е. Криминалистическая структура преступлений. Минск : БГУ, 2007.

5. Мухин Г.Н. Научно-методические и дидактические аспекты методики расследования преступлений, совершаемых организованными преступными формированиями // Проблемы раскрытия и расследования преступлений, совершаемых организ. Группами : сб. науч. тр. / под общ. ред. Н.И. Николайчика [и др.]. Минск, 2000.

6. Криминалистика : учебник. В 3 ч. Ч. 3. Криминалистическая методика / под ред. Г.Н. Мухина ; М-во внутрен. дел Респ. Беларусь, учреждение образования «Акад. М-ва внутрен. дел Респ. Беларусь». 2-е изд., испр. Минск : Акад. МВД, 2010.

7. Ищенко Е.П. Об актуальных проблемах технико-криминалистического обеспечения расследования преступлений // Актуал. проблемы соврем. криминалистики и судеб. экспертизы : материалы Междунар. науч.-практ. конф., посвящ. 35-летию со дня образования кафедры криминалистики Акад. МВД Респ. Беларусь (Минск, 3 июня 2011 г.) / М-во внутр. дел Респ. Беларусь, учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь» ; редкол.: Н.И. Порубов [и др.]. Минск : Акад. МВД, 2011.

УДК 004.3:34

В.Б. Шабанов, А.Н. Лепёхин

НЕКОТОРЫЕ СВОЙСТВА ИНФОРМАЦИИ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ ЕЕ ЗАЩИТЫ

Развитие информационно-коммуникационных технологий ведет к трансформации содержания основных категорий в сфере информационных правоотношений. Нормативные правовые акты, регулирующие данную сферу общественной жизни, в настоящее время динамично развиваются. Примером тому может служить совершенствование отраслевого законода-

тельства Республики Беларусь. В целях регулирования правоотношений в последнее время были приняты несколько законодательных актов, таких, как закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации», которым определены основные категории и их легальное закрепление, перечень субъектов, участвующих в информационных правоотношениях и их права и обязанности. Кроме того, указаны вопросы, связанные с защитой информации, целями и мерами такой защиты. Также данным законом определено, что правовой режим отдельных видов информации регулируется соответствующим законодательством. И одним из таких законов, регулирующих вопросы обращения информации ограниченного распространения, является закон Республики Беларусь от 19 июля 2010 г. № 170-З «О государственных секретах». В данном нормативном правовом акте комплексно отражены вопросы, связанные с основными положениями в сфере государственных секретов, полномочиями государственных органов в данной сфере, порядком отнесения сведений к государственным секретам, засекречиванием и рассекречиванием сведений, а также с установленным порядком допуска и доступа к государственным секретам.

Нисколько не умаляя значение данных нормативных правовых актов для регулирования информационных правоотношений, отметив их комплексный характер, восполняющий пробелы в правовом регулировании данной сферы общественных отношений, считаем необходимым обратить внимание на следующие обстоятельства.

В соответствии с законом Республики Беларусь «Об информации, информатизации и защите информации» под информацией понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их предоставления. Этим же законом определено, что понимается под конфиденциальностью информации, а также права и обязанности субъектов информационных отношений, направленные на реализацию требований конфиденциальности информации. Кроме того, законом установлено, что понимается под защитой информации: комплекс правовых, организационных и технических мер, направленных на целостность (неизменность), конфиденциальность, доступность и сохранность информации, т. е. определен комплекс мер, направленных на обеспечение основных свойств информации. Также в законе раскрыто содержание этих мер.

Очевидно, что соблюдение собственником или владельцем информации указанных требований по защите информации, является достаточно сложной и экономически затратной процедурой. Более того, законом Республики Беларусь «О государственных секретах» определен перечень сведений, которые относятся к государственным секретам, категории государственных секретов (государственной тайны и служебной тайны), порядок отнесения сведений к государственным секретам и достаточно важный аспект – срок засекречивания и порядок рассекречивания сведений. Также законом установлены следующие сроки засекречивания: для государственной тайны – до 30 лет, для служебной тайны – до 10 лет. При этом срок исчисляется с даты засекречивания.

Очевидно, что такие меры имеют объективный и необходимый характер и направлены на обеспечение интересов государства, его национальной безопасности, а также защиту прав и законных интересов граждан. Вместе с тем реализация в установленном порядке указанного выше комплекса мер по защите информации является достаточно экономически затратным мероприятием. Более того, такие меры должны осуществляться в течение достаточно длительного периода (не менее 10 и 30 лет соответственно). В этой связи закономерно возникает вопрос о достаточно взвешенном подходе к отнесению сведений к государственным секретам. Указанная необходимость обусловлена в первую очередь тем, что в настоящее время информационные процессы приобретают гиперболизированный характер и объемы информации постоянно растут. Исходя из этого полагаем необходимым обратить внимание на появление и нормативное закрепление такой новой характеристики, как жизненный цикл информации (ее актуальность), под которым считаем возможным понимать период, в течение которого информация отвечает требованиям потребителя информации в удовлетворении его нужд.

Таким образом, с учетом увеличения объемов информации, достаточно быстрой утраты ее смысловой ценности считаем возможным ставить вопрос о законодательном закреплении свойств информации в соответствующем нормативном акте и корректировке сроков отнесения сведения к государственным секретам и установленного порядка рассекречивания секретных сведений.

УДК 343

С.А. Шарапов

О ВРЕДОНОСНОСТИ ВИРУСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ

В Республике Беларусь вирусные компьютерные программы отнесены к категории вредоносных. Ответственность за разработку и заведомое использование специальных вирусных программ, а также за распространение носителей с ними предусмотрена ст. 354 УК Республики Беларусь. Таким образом, для привлечения лица к уголовной ответственности достаточно, чтобы разработанная, используемая или распространяемая им компьютерная программа обладала свойством «вирусности», т. е. способностью к самовоспроизведению, самопроизвольному присоединению к другим файлам. В обоснование такой позиции можно привести доводы специалистов о том, что безобидных вирусов не существует, компьютерные вирусы –