

происшествия при расследовании компьютерных преступлений невозможно или осмотр будет неэффективен. В связи с этим следует учесть некоторые моменты при проведении предварительных исследований, в результате которых устанавливаются все элементы места происшествия и все места нахождения следов преступления и таким образом обеспечивается быстрое и полное собирание всех следов.

Так, в первую очередь следователь должен принять предупредительные меры, которые обеспечат целостность доказательств в среде компьютерной техники, а именно:

обеспечить охрану территории производства осмотра, на которой находятся средства компьютерной техники;

удалить людей от оборудования и источников питания;

убедиться, что ни при каких обстоятельствах компьютер не будет включен;

убедиться, что компьютер отключен (некоторые экранные заставки создают впечатление, что компьютер отключен).

На рабочем этапе осмотра специалист осуществляет помощь следователю:

выявляет специальные средства уничтожения информации в компьютере при несанкционированном доступе к нему;

устанавливает необходимый пароль доступа к информации;

разрабатывает правила использования пароля с тем, чтобы посторонние действия и нарушения этих правил не привели к уничтожению файлов.

Также во время осмотра может возникнуть необходимость получения первоначальных сведений от отдельных лиц об определенных фактах или событиях. Роль специалиста сводится к обеспечению общения путем разъяснения, толкования и верного использования специальной компьютерной терминологии. Также специалист помогает следователю:

точнее и полнее понять опрашиваемого, который использует в речи специальные термины;

немедленно прекратить дачу заведомо ложных показаний, касающихся специальных вопросов, сообщение которых рассчитано на неосведомленность следователя;

получить начальные сведения ориентирующего характера, необходимые для организации поиска и задержания подозреваемых, пресечения преступления или минимизации негативных последствий его совершения;

получить сведения и материалы, необходимые для назначения соответствующих экспертиз;

определить способ совершения преступных действий и механизм преступления.

Таким образом, существуют определенные трудности, связанные с надлежащим техническим обеспечением расследования преступлений против информационной безопасности, а также в подготовке квалифицированных специалистов в данной области. Для решения вышеуказанных проблем необходимо отслеживать тенденции в развитии информационных технологий с последующим применением их в методических рекомендациях для наиболее эффективного расследования преступлений против информационной безопасности.

УДК 343.985.7

С.А. Шаронов

ОПРЕДЕЛЕНИЕ ПОНЯТИЯ ВРЕДОНОСНОЙ КОМПЬЮТЕРНОЙ ПРОГРАММЫ: УГОЛОВНО-ПРАВОВЫЕ И ТЕХНИЧЕСКИЕ АСПЕКТЫ

Одним из приоритетных направлений государственной политики в области обеспечения информационной безопасности является совершенствование правовых мер защиты компьютерной информации. При этом эффективность правовых норм во многом зависит от точного и единообразного определения терминов, используемых в конкретной сфере деятельности. Чтобы должным образом работал механизм ответственности за противоправные действия с вредоносными программами, необходимо дать однозначное определение понятия вредоносной компьютерной программы. Между тем анализ действующего законодательства и научных взглядов свидетельствует об отсутствии единых подходов в данном вопросе.

В ст. 354 Уголовного кодекса Республики Беларусь предусматривается ответственность за разработку, использование либо распространение вредоносных компьютерных программ. Исходя из диспозиции данной статьи к вредоносным относятся программы, предназначенные для несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, а также специальные вирусные программы. Согласно Комментарию к УК Республики Беларусь под редакцией А.В. Баркова и В.М. Хомича под вредоносными предлагается понимать две разновидности программ:

специально разработанные или видоизмененные компьютерные программы, которые в процессе своего действия не предполагают ни предварительного уведомления собственника, владельца, пользователя о характере действий таких программ, ни получения их санкции на

уничтожение, блокирование, модификацию либо копирование информации, хранящейся в компьютерной системе, сети или на машинных носителях;

специальные вирусные программы, деятельность которых связана с их свойством самовоспроизводиться, самопроизвольно присоединяться к другим программам и при запуске последних приводить без ведома и санкции добросовестных пользователей к аналогичным и иным вредным последствиям.

В то же время в техническом нормативном правовом акте – Государственном стандарте Республики Беларусь СТБ 34.101.8–2006 (далее – Госстандарт) установлено, что вредоносной программой является программный код (исполняемый или интерпретируемый), обладающий свойством несанкционированного воздействия на объект информационных технологий. Под объектом информационных технологий понимается комплекс технических и программных средств, предназначенных для выполнения функций сбора, обработки, хранения, передачи и использования данных. Его элементами являются оперативная память, энергонезависимая память, файлы данных и системное программное обеспечение.

Приведенные определения свидетельствуют о неоднозначности трактовки понятия вредоносной программы. В частности, исходя из Госстандарта компьютерная программа, предназначенная для любого несанкционированного воздействия на объект информационных технологий, должна признаваться вредоносной. Следовательно, несанкционированный доступ, осуществляемый с нарушением системы защиты, также может являться одним из видов вредоносного воздействия, а программа, специально предназначенная для получения несанкционированного доступа, должна относиться к категории вредоносных программ.

Между тем приведенное утверждение противоречит ст. 354 УК, согласно которой программа, предназначенная для получения несанкционированного доступа к компьютерной системе, сети или машинным носителям информации, вредоносной не является. В этой связи органы предварительного следствия рассматривают использование указанной программы как способ совершения несанкционированного доступа к компьютерной информации и квалифицируют такие действия только по ст. 349 УК.

С другой стороны, вредоносность использования программ, специально предназначенных для несанкционированного доступа к защищенным информационным ресурсам, сомнений не вызывает. В качестве примера таких действий можно привести материалы уголовного дела

№ 06018000064 (рассмотрено судом Борисовского р-на Минской обл.), согласно которым житель Борисова с использованием компьютерных программ, в том числе программы «Woron Scan v.1.09», осуществлял несанкционированный доступ к информации, хранящейся на машинных носителях – модулях подлинности абонентов (сим-картах) операторов сотовой связи Республики Беларусь. Эти действия сопровождались нарушением установленной производителем сим-карт программной и аппаратной системы защиты указанной информации.

Из материалов уголовного дела № 05016000245 (рассмотрено судом Солигорского р-на Минской обл.) следует, что житель Солигорска использовал компьютерные программы (в том числе программу «bdw.c») с целью несанкционированного доступа к информации, хранящейся в компьютерной системе компании «Niconica Inc.» (Канада).

Кроме того, некоторое отличие вышеуказанных определений вредоносной программы наблюдается и в объекте посягательства, на который направлено их действие. В частности, исходя из норм Госстандарта несанкционированное воздействие вредоносной компьютерной программы может быть направлено как на программные, так и на технические средства. Например, на интернет-сайте «Лаборатории Касперского» имеются сведения о компьютерном вирусе, которому дано название «Чернобыль», способном повреждать аппаратную часть компьютера. В уголовном праве идет речь о возможности несанкционированных действий вредоносной программы исключительно в отношении информации, хранящейся в компьютерной системе, сети или на машинных носителях информации.

Не вполне однозначным также является определение вирусной компьютерной программы. Как отмечено ранее, в уголовном праве под специальной вирусной понимается программа, деятельность которой связана со свойством самовоспроизводиться, самопроизвольно присоединяться к другим программам и при запуске последних приводить без ведома и санкции добросовестных пользователей к вредоносным последствиям. Однако под данное определение не попадают программы, выделяемые специалистами в отдельную категорию «сетевых червей». В частности, Ф.С. Воройский высказывает мнение, что «сетевые черви» – программы, которые, распространяясь по сети, не изменяют файлы, а проникают в память компьютера, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Хотя их и называют вирусами, таковыми они не являются. Е.В. Старостина утверждает, что компьютерные «черви» по характеру схожи с компьютерными вирусами. Отличие состоит в том, что «червь» – самостоятельная программа.

В то же время согласно Госстандарту компьютерный вирус – тип вредоносной программы, обладающий способностью создавать свои копии и внедрять их в элементы объекта информационной технологии (т. е. в файлы данных, системное программное обеспечение, оперативную и энергонезависимую память), при этом копии сохраняют свойства компьютерного вируса. Исходя из данного определения программу «сетевые черви» можно отнести к вирусным компьютерным программам.

Приведенные несоответствия в понятийном аппарате негативно влияют на комплексное обеспечение информационной безопасности и могут создать проблемы при расследовании уголовных дел о преступлениях, связанных с использованием вредоносных компьютерных программ. В этой связи представляется целесообразным выработать общеобязательное, единое для всех сфер деятельности определение понятия вредоносной программы, которое позволит объективно и единообразно оценивать действия по использованию программ в неправомерных целях.

СВЕДЕНИЯ ОБ АВТОРАХ

Анищенко Инесса Алексеевна – начальник кафедры криминалистических экспертиз следственно-экспертного факультета Академии МВД Республики Беларусь, кандидат юридических наук, доцент.

Асаёнок Борис Валерьевич – профессор кафедры правового обеспечения деятельности органов пограничной службы Института пограничной службы Республики Беларусь, кандидат юридических наук, доцент.

Ахраменко Татьяна Викторовна – преподаватель кафедры криминалистических экспертиз следственно-экспертного факультета Академии МВД Республики Беларусь.

Борисенко Николай Александрович – адъюнкт научно-педагогического факультета Академии МВД Республики Беларусь.

Боровик Петр Леонидович – старший преподаватель кафедры правовой информатики Академии МВД Республики Беларусь.

Быстриков Алексей Михайлович – курсант Института пограничной службы Республики Беларусь.

Водолазов Артемий Владимирович – заведующий научно-исследовательским сектором технических исследований документов Центра судебных экспертиз и криминалистики Министерства юстиции Республики Беларусь.

Волкова Анна Геннадьевна – старший преподаватель кафедры общей и юридической психологии Калужского государственного университета им. К.Э. Циолковского, кандидат психологических наук.

Галезник Марина Владимировна – доцент кафедры криминалистики Академии МВД Республики Беларусь, кандидат юридических наук, доцент.

Горошко Елена Юрьевна – старший преподаватель кафедры криминалистических экспертиз следственно-экспертного факультета Академии МВД Республики Беларусь, кандидат юридических наук.

Григоревич Василий Леонидович – доцент кафедры криминалистики Академии МВД Республики Беларусь, кандидат юридических наук, доцент.

Гридюшко Павел Владимирович – заместитель начальника кафедры расследования преступлений следственно-экспертного факультета Академии МВД Республики Беларусь, кандидат юридических наук, доцент.

Гриневич Виктория Викторовна – слушатель магистратуры факультета заочного обучения, преподаватель кафедры расследования преступлений следственно-экспертного факультета Академии МВД Республики Беларусь.

Гусенцов Александр Олегович – преподаватель кафедры криминалистики Академии МВД Республики Беларусь.

Гуца Юрий Анатольевич – адъюнкт научно-педагогического факультета Академии МВД Республики Беларусь.

Дмитриева Татьяна Федоровна – преподаватель кафедры уголовного права и уголовного процесса Витебского государственного университета им. П.М. Машерова.

Енгальчев Вали Фатехович – профессор кафедры общей и юридической психологии Калужского государственного университета им. К.Э. Циолковского, доктор психологических наук, профессор.