УДК 621.3 УДК 343

В. Е РОГ
старший преподаватель кафедри информационных технологий и кибербезопасности ХНУВД
О.П. МЕЛАЩЕНКО
старший преподаватель кафедри информационных технологий и кибербезопасности ХНУВД
Denys Lebediev
manager of Risk and Compliance Group InfoReach, Inc

СЛЕДООБРАЗОВАНИЕ ПРИ НЕПРАВОМЕРНОМ ДОСТУПЕ К КОМПЬЮТЕРНОЙ СИСТЕМЕ ИЛИ СЕТИ

В данное время разработки ученых и инженеров - программистов ведут общество к новому качественному витку развития информационных услуг, а также определяют и обеспечивают основу его существования в информационном поле. Глобальные информационные сети и системы являются технологической основой всеобщего обмена информации. Таким образом, информационные ресурсы представляют огромную ценность, а несанкционированный доступ к этим ресурсам может привести к глобальным катастрофам если не будет достаточной защиты данных ресурсов. Данная ситуация может привести к не поправимым последствиям или, в условиях конкуренции, изменить ситуацию в пользу того, кто первый получил доступ к информации.

Пагубные последствия неправомерного доступа к компьютерной системе могут заключаться в хищении денежных средств или материальных ценностей, завладении компьютерными программами, а также информацией путем изъятия машинных носителей либо копирования. Это может быть также незаконное изменение, уничтожение, блокирование информации, выведение из строя компьютерного оборудования, внедрение в компьютерную систему компьютерного вируса, заведомо ложных данных и др.

Также можно отметить, что традиционная классификация следов совершения тех или иных преступлений не охватывает те ее виды, которые

возникли при появлении новых видов преступлений.

Таким образом, к киберпреступлению может быть отнесено любое преступление, совершенное в электронной среде. Преступление, совершенное в киберпространстве - это противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также другие противоправные общественно опасные действия, совершенные с помощью компьютеров, комп'ютерних сетей и программ.

Механизм следообразования - это своего рода форма протекания процесса в результате которого образуется след-отображение.

В результате чего можно сделать вывод, что основой процесса следообразования в компьютерной системе и главным следообразующим фактором является совокупность взаимодействующих программ и их настроек, которые существовали на момент совершения расследуемого события. Поскольку программа оставляет следы только тогда, когда она находится в активном состоянии, то есть выполняется в оперативной памяти компьютера, а выполнение программы является некоторым процессом, то программа является следообразующим процессом.

Основой любого криминалистического исследования, в том числе и выполняемого специалистом при расследовании преступлений в компьютерной сфере является исследование процесса следообразования. Важным вопросом в этой области является вопрос о природе следов в компьютерной системе, и ряд связанных с ним вопросов, в частности, являющихся объектами взаимодействия в компьютерных системах, свойства присущи этим объектам и их признаки находят свое отражение в следах, связанных с событием преступления.

При рассмотрении преступлений в сфере компьютерной информации мы сталкиваемся с особой группой следов - «виртуальными следами», т.е. следами, которые остаются в памяти технических устройств, в электронном поле, на

носителях информации. К таким следам можно отнести файлы, магнитные носители, информация, передаваемая в эфире посредством магнитной волны.

Получаемые «виртуальные следы» не надежны, так как их можно неправильно считать. Таким образом, можно представить «виртуальный след» как любое изменение состояния киберпространства, связанное с событием и зафиксированное в виде компьютерной информации на материальном носителе.

С технической точки зрения обнаружение и фиксация «виртуальных» следов проводится с использованием широкого спектра програмно-технических средств.

Таким образом, можно сделать вывод, что основой процесса следообразования в компьютерной системе и главным следообразующим фактором является совокупность взаимодействующих программ которые существовали на момент совершения расследуемого события. Поскольку программа оставляет след только в активном состоянии, а выполнение программы это некоторый процесс, то программу можно считать следообразующим процессом.