УДК 002.001;002:001.8

С.В. Скрыль, Е.Б. Белов, Р.В. Мещеряков

Структурирование описания противоправных действий в сфере компьютерной информации как методологическая основа их криминалистического исследования

Обосновывается структурирование описания противоправных действий в сфере компьютерной информации как инструмент криминалистического исследования подобного рода действий.
Формулируются принципы структурирования.

В соответствии с принципами системного анализа и существующими взглядами на проблему криминалистического исследования противоправных действий в информационной сфере, такого рода исследование проводится с использованием сценарных описаний, отражающих различные аспекты этих действий как объекта идентификации [1].

В этих целях возможно использование известных структурных методологий [2].

Структурным анализом принято называть метод исследования системы, который начинается с ее общего обзора и затем детализируется, приобретая иерархическую структуру со все большим числом уровней. Структурирование по отношению к формальным методам описания архитектуры сложных систем и процессов их функционирования является методологией, которая позволяет понизить сложность описания.

Как инструмент описания исследуемого объекта структурирование может быть выполнено на основе:

- дедуктивного подхода (переход от общего к частному), осуществляемого путем расчленения и группировки частей описываемого объекта, начиная с рассмотрения его как единого целого;
- индуктивного подхода (переход от частного к общему), осуществляемого путем сбора элементов описываемого объекта и композиции в соответствии с их взаимоотношениями в древовидную структуру, которая заканчивается целостным описанием объекта.

Учитывая то обстоятельство, что индуктивный подход не исключает пропуска отдельных элементов или связей, а также неадекватной их оценки не с системных позиций, представляется целесообразным в качестве инструмента для исследования противоправных действий в сфере компьютерной информации использовать дедуктивный подход.

Вместе с тем, методы декомпозиции, которые уже достаточно хорошо разработаны для формализованных структур, для таких трудно формализуемых процессов, как противоправные действия в сфере компьютерной информации, могут иметь эвристическую форму.

Принимая во внимание целевую направленность противоправных действий в отношении информации компьютерных систем при их исследовании методами структурного анализа декомпозиции подлежит предметная целевая функция [3]. Это приводит к необходимости в процессе декомпозиции выделять функционально специализированные элементы. При этом специфицируемые в результате декомпозиции функции и логические связи исследуемых процессов формируют описание их функциональной структуры, что в свою очередь, является функциональным представлением их как объекта исследования.

Структура объекта исследования, представленная в терминах такого описания, является его структурным базисом.

Структурированное описание противоправных действий в сфере компьютерной информации в интересах их выявления должно обеспечивать:

- полноту отображения всех существенных элементов и атрибутов таких действий и их взаимосвязей;
- возможность воспроизведения всех значимых характеристик противоправных действий;
- унифицированность описания структуры и взаимосвязей между элементами на любом уровне ее детализации;
- гибкость, позволяющую объединять элементы в структуры и заменять эти элементы и их совокупности.

Несмотря на то, что структурным методологиям свойственен ряд недостатков, накладывающих определенные ограничения на их применение: сложность понимания, большая трудоемкость в использовании, они все же дают возможность предоставить достаточный инструментарий для описания процессов такого уровня сложности как противоправные действия в сфере компьютерной информации.

Функциональное описание подобного рода противоправных действий основываются на двух основных принципах.

1. Рассмотрение функций должно осуществляться сверху-вниз.

2. Степень детализации функционального описания считается достаточной, если вариант функциональной декомпозиции дает однозначное соответствие между противоправным действием и его исполнителем.

В соответствии ***с первым принципом*** информация, получаемая об особенностях противоправных действий в сфере компьютерной информации иерархически распределяется по уровням, постепенно детализируясь. Таким образом, обеспечивается представление информации и ее уточнение приемлемым объемом новых данных.

Основной характеристикой противоправных действий в сфере компьютерной информации является характеристика степени достижения злоумышленниками поставленных целей в результате выполнения некоторой целевой вредоносной функции. Это означает, что степень достижения целей в результате подобного рода противоправных действий допускает функциональное представление, а сами функции можно представить в виде вредоносных воздействий.

Очевидно, что целевая функция, реализуемая злоумышленниками, зависит от ряда внутренних и внешних по отношению к его действиям факторов, а также входных данных и выходных результатов. Допустимость функционального представления противоправных действий в сфере компьютерной информации, в свою очередь предполагает представление их в виде множества вредоносных воздействий, последовательная реализация которых и составляет целевую функцию.

Представление целевой функции в виде упорядоченных последовательностей вредоносных воздействий составляет процесс ее декомпозиции. Естественно, что каждое вредоносное воздействие обеспечивается некоторым механизмом, связанным в общей функциональной реализации целевой функции с другими механизмами. Поэтому множества вредоносных воздействий и механизмов образуют декомпозиционный структурный базис описания противоправных действий в сфере компьютерной информации.

Для адекватного представления реальных вредоносных воздействий на информацию компьютерных систем процесс декомпозиции должен включать выявление и описание не только функциональных, но и информационных связей между компонентами, составляющими декомпозиционный структурный базис описания противоправных действий в отношении информационных ресурсов таких систем.

В соответствии ***со вторым принципом*** устанавливается необходимая степень детализации функционального описания исследуемых противоправных действий.

В этой связи хотелось бы отметить, что уже имеющийся опыт функциональной декомпозиции противоправных действий в информационной сфере базируется лишь на интуитивном (экспертном) обосновании необходимого уровня детализации исследуемых процессов. Однако, подобный подход не позволяет произвести исследования процессов такого уровня сложности как противоправные действия в отношении информации компьютерных систем.

Вместе с тем, исследование механизмов вредоносных воздействий на защищенные информационные системы в интересах выявления противоправных действий в сфере компьютерной информации с позиций методологии системного анализа позволило обосновать необходимую степень детализации функционального описания, базируясь на эвристических правилах, в соответствии с которыми детализация описания считается достаточной, если вариант функциональной декомпозиции:

– определяет исполнителя подобного рода действий – непосредственно злоумышленник, вредоносная программа, специальное аппаратное средство;

– обеспечивает достоверное описание функциональных связей и логической структуры информации;

– формирует криминалистически значимый набор признаков.

Применение структурированного описания противоправных действий при проведении компьютерно-технических экспертиз позволяет выделить несколько этапов, важных для сохранения доказательной базы и сокращения времени проведения экспертиз.

Очевидно, что применение в практической работы экспертных учреждений сопряжено с рядом трудностей. В первую очередь это квалификация эксперта, для использования предложенного метода необходимо обладать знаниями и навыками в области системного анализа, иметь опыт построения декомпозиционного структурного базиса, а также выделения функций при исследовании представленных объектов экспертизы.

Вместе с тем можно предложить создание формализованной модели совершения противоправных действий, а также формальных методов ее исследования. Основой модели совершения противоправных действий в сфере компьютерной информации может являться модель нарушителя информационной системы. В свою очередь эксперт-криминалист будет выступать в роли аудитора, проводящего аттестацию.

Разработанный подход был апробирован при проведении компьютерно-технических экспертиз в Центре технологий безопасности ТУСУРа. Полученные результаты показали повышение эффективности работы эксперта: сокращение времени на проведение экспертизы, полнота описания функций, прав, исследовательских действий, а также выводов.

Например, при выявлении факта неправомерного доступа к компьютерной информации прежде всего необходимо выделить цель получения данной информации злоумышленником. При построении дерева целей злоумышленника можно выделить некоторые задачи, которые злоумышленник решал

при организации доступа. По полученным сведениям можно построить функцию, описывающую действия злоумышленника.

С другой стороны, детализация описания действий, проводимым злоумышленником при неправомерном доступе к информации позволяет представить следственным органам и суду доказательную базу в виде некоторой последовательности этапов (шагов) во времени.

На основании изложенного можно сделать вывод о том, что структурный анализ является эффективным методом исследования механизмов вредоносного воздействия на компьютерные системы в интересах выявления противоправных действий в сфере компьютерной информации. За счет универсальности структурного анализа как метода исследования подобного рода противоправных действий обеспечивается решение ряда важных задач организационно-правового обеспечения защиты компьютерной информации.

Литература

1. Правовое обеспечение информационной безопасности: учебник для высших учебных заведений МВД России / В.А. Минаев, А.П. Фисун, С.В. Скрыль, С.В. Дворянкин, М.М. Никитин, Н.С. Хохлов - М.: Маросейка, 2008. – 368 с.

2. Карпычев В.Ю. Концептуальное проектирование информационных систем: учебное пособие – М.: ГУ НПО «Спецтехника и связь» МВД России, 2002. – 132 с.

3. Скрыль С.В. Методологические принципы моделирования угроз информационному обеспечению органов внутренних дел / С.В. Скрыль, О.Б. Рощин // Современные проблемы борьбы с преступностью: Материалы Международной научно-практической конференции. - Воронеж: Воронежский институт МВД России, 2006. - С. 6 - 10.

Скрыль Сергей Васильевич
Воронежский институт МВД России

Белов Евгений Борисович
ИКСИ, 93 106 09

Мещеряков Роман Валерьевич
ГОУ ВПО Томский государственный университет систем управления и радиоэлектроники
К.т.н., доцент кафедры комплексной информационной безопасности электронно-вычислительных систем
Эл. почта: mrv@keva.tusur.ru.

K.S. Skryl, E.B. Belov, R.V. Mescheryakov

Description of iliegal actions structurization in sphere of the computer information as their criminal research methodological basis

Proves structurization of the description of illegal actions in sphere of the computer information as the tool crimina researches of a similar sort of actions. Principles of structurization are formulated.