Д. А. Илюшин, **А. И. Моисеев**, **М. Н. Осипов**, **В. П. Цветов** (Самара, УСТМ ГУВД по СО, СамГУ). **Об инструментальных средствах для обеспечения функций оперативно-разыскных мероприятий при расследовании компьютерных преступлений.**

Одной из главных проблем на этапе проведения оперативно-разыскных мероприятий, связанных с компьютерными преступлениями, является нехватка мобильных и относительно простых программно-аппаратных средств, предназначенных для сбора и анализа машиночитаемых данных.

Состав и функциональность подобных средств определяются спецификой совершаемых компьютерных преступлений, среди которых наиболее распространены следующие: преступления, связанные с нарушением авторских прав на программные продукты и данные; преступления, связанные с созданием и распространением вредоносных программ; мошенничества с электронными картами; неправомерный доступ к системам хранения, обработки и передачи данных.

В части расследования сетевых инцидентов основные оперативно-разыскные функции реализуются средствами СОРМ-2, которые позволяют вести исчерпывающий протокол сетевых событий, начиная со сбора статистических сведений о соединениях и заканчивая полной информацией о циркулирующих данных. Однако в большинстве случаев полный объем функций, предоставляемый СОРМ-2, является избыточным, вдобавок, они предназначены только для анализа сетевых взаимодействий.

По этой причине становится актуальной задача разработки комплекса инструментальных средств, сочетающего в себе как элементы СОРМ-2, так и дополнительные специализированные компоненты, предназначенные для автоматического сбора и анализа данных по наиболее распространенным видам компьютерных преступлений.

Разрабатываемый авторами комплекс должен реализовывать следующую минимальную функциональность: сканирование параметров операционной системы и программных прошивок; определение лицензионности программного обеспечения; выявление вредоносных программ и средств преодоления систем защиты; быстрый поиск и обработка фрагментов данных; обнаружение скрытых и зашифрованных данных; дешифрование данных; мониторинг, протоколирование, фильтрация и блокирование предопределенных сетевых событий; обеспечение достоверности собранных данных и их защиту от модификации.

Работы по проектированию комплекса находятся на стадии составления технического задания.