УДК 002.001;002:001.8

О.С. Авсентьев, В.В. Александров, Г.И. Рябинин, К.С. Скрыль, Р. В. Мещеряков

Принципы моделирования механизмов воздействия вредоносных программ на защищенные информационные системы в интересах оценки угроз их безопасности

Формулируются принципы решения задачи моделирования механизмов воздействия вредоносных программ на защищенные информационные системы в интересах оценки угроз безопасности их информационным ресурсам. Приводится формальная ее постановка и пути решения.

Анализ стратегий несанкционированного воздействия на информацию в защищенных информационных системах, реализуемых с использованием вредоносных программ, позволяет установить закономерность между функциональным обликом вредоносных программ и этапами воздействия на защищенные информационные системы, в рамках которых эти программы используются [1]. Это позволяет математически описать последовательность противоправных действий в отношении защищенной информационной системы, совершаемых с использованием вредоносных программ, и оценить уровень угрозы безопасности системе в зависимости от этапа воздействия. При этом описание этапов воздействия на защищенные информационные системы может быть получено лишь в результате структурного синтеза обобщенной функциональной модели противоправных действий, совершаемых с использованием вредоносных программ.

Это позволяет сформулировать принципы моделирования механизмов воздействия вредоносных программ на защищенные информационные системы в интересах оценки угроз их безопасности. С этой целью определим ряд рабочих гипотез.

Основополагающими гипотезами при решении данной задачи являются **гипотеза об идентифицируемости воздействия вредоносных программ на защищенные информационные системы** и **гипотеза о многоэтапности совершения противоправных действий в отношении защищенных информационных систем, совершаемых с использованием вредоносных программ**.

В соответствии с первой гипотезой, несмотря на применяемые вредоносными программами технологии обеспечения активности и живучести, существуют способы идентификации их воздействия. Это дает возможность поставить в соответствие воздействиям вредоносных программ идентифицирующие признаки, что, в свою очередь, позволяет использовать эти признаки в качестве исходных данных для моделирования механизмов воздействия вредоносных программ на защищенные информационные системы в интересах оценки угроз их безопасности.

В соответствии со второй гипотезой вредоносные программы реализуют свои функции в рамках многоэтапных стратегий противоправных действий. Многоэтапность этих стратегий обусловлена необходимостью преодоления (вскрытия) защитных механизмов защищенных информационных систем.

Из приведенных гипотез вытекают основные принципы моделирования механизмов воздействия вредоносных программ на защищенные информационные системы в интересах оценки угроз их безопасности.

Принцип синтезируемости описания противоправных действий, совершаемых с использованием вредоносных программ, предполагает в качестве основы для формирования описаний подобного рода действий их структурный синтез.

Логически вытекающий из данного принципа **принцип функционального представления противоправных действий, совершаемых с использованием вредоносных программ,** приводит к необходимости использования методов функционального моделирования для формирования описаний подобного рода действий.

В соответствии с **принципом поэтапной обобщаемости признаков противоправных действий, совершаемых с использованием вредоносных программ,** оценка угроз воздействия таких программ должна осуществляться с учетом многоэтапности стратегий подобного рода действий.

Принцип многоуровневости функционального синтеза описаний противоправных действий, совершаемых с использованием вредоносных программ, предполагает наличие нескольких уровней функционального облика подобного рода действий.

С целью решения задачи моделирования механизмов воздействия вредоносных программ на защищенные информационные системы в интересах оценки угроз их безопасности определим соответствующий показатель.

В качестве основы для конструирования показателя возможностей оценки угроз безопасности защищенным информационным системам на основе моделирования механизмов воздействия вредоносных программ на их информационные ресурсы заданной номенклатурой M моделей условимся использовать вероятность P такой оценки, как вероятность события, при котором моделируемые противоправные действия, совершаемые с использованием вредоносных программ, из их множества D однозначно идентифицируют степень угрозы безопасности защищенной информационной системе. При этом множество D будет считаться полным, если каждому его элементу d_i, $i = 1, 2, ..., |D|$ будет соответствовать признак противоправных действий a_j, $j = 1, 2, ..., |A|$ из их множества A.

Оценка уровня U такой угрозы считается реализованной заданной номенклатурой M моделей, если с вероятностью P обеспечивается участие каждого признака противоправных действий a_j, $j = 1, 2, ..., |A|$ в формировании значения U.

С учетом изложенного, задача моделирования механизмов воздействия вредоносных программ на защищенные информационные системы в интересах оценки угроз их безопасности в содержательном плане формулируется следующим образом.

Применительно к возможностям воздействия вредоносных программ на защищенные информационные системы и номенклатуре моделей, описывающих противоправные действия, совершаемые с использованием вредоносных программ, разработаны алгоритмы оценки безопасности этих систем на основе моделирования подобного рода воздействий.

С целью формализации задачи и способов ее решения, в соответствии со сформулированной содержательной постановкой, обозначим через $R(M)$ набор правил оценки угрозы безопасности защищенной информационной системе заданной номенклатурой M моделей. При этом обеспечиваются возможности оценки угроз $P(R)$. Тогда задачу моделирования механизмов воздействия вредоносных программ на защищенные информационные системы в интересах оценки угроз их безопасности можно рассматривать как задачу отыскания набора правил R, максимизирующего возможности P оценки угроз информационной безопасности при номенклатуре m моделей не превышающей заданной M.

Это позволяет формально постановку задачи представить в виде

$$R = \arg \max_{m \le M} P(R).$$

Сформулированную задачу моделирования механизмов воздействия вредоносных программ на защищенные информационные системы в интересах оценки угроз их безопасности целесообразно решать путем представления в виде следующих основных последовательно решаемых задач:

– структуризация описаний противоправных действий, совершаемых с использованием вредоносных программ;

– унификация методов моделирования механизмов воздействия вредоносных программ на защищенные информационные системы в интересах оценки угроз их безопасности с целью получения номенклатуры моделей, не превышающей заданной;

– проведения экспериментов по оценке возможности оценки угроз безопасности защищенным информационным системам.

Разработанная методика оценки может быть применена к этапам аудита информационных систем:

1) описание объекта исследования;

2) идентификация угроз информационной безопасности;

3) прогнозирование поведения объекта исследования в условиях воздействия угроз информационной безопасности;

4) степень невыполнения требований информационной безопасности;

5) формирование требований (контрмер) по увеличению уровня защищенности;

6) проверка эффективности введённых контрмер;

7) оценка затрат на информационную безопасность к степени защищенности информационной системы.

В общем случае модель может быть применена к элементарным действиям, классифицируемым как противоправные на каждом этапе аудита. Однако не все параметры моделей могут быть учтены на этапе проектирования систем, что затрудняет анализ моделей.

Предлагается использовать многоуровневое представление для поэтапного моделирования не только противоправных действий, но и собственно деятельности информационной системы и программного обеспечения в частности. Перспективным представляется формирование типовых моделей механизмов вредоносных программ, а также методов противодействия.

Литература

1. Моделирование как методология криминалистического исследования в сфере компьютерной информации / С.В. Скрыль, В.А. Минаев и др. // Безопасность информационных технологий. – М.: МИФИ, 2005. – № 1. – С. 57–61.

Авсентьев Олег Сергеевич
Александров Виталий Витальевич
Рябинин Геннадий Иванович
Скрыль Сергей Васильевич
Воронежский институт МВД России

Роман Валерьевич Мещеряков
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.

O.S. Avsentyev, V.V. Aleksandrov, G.I. Ryabinin, K.S. Skryl, R.V. Mescheryakov

Principles of influence mechanisms modelling nocuous programs on the protected information systems in interests of threats estimation of their safety

Principles of the problem decision of influence mechanisms modelling nocuous programs on the protected information systems in interests of an estimation of safety threats to their information resources are formulated. Its formal statement and ways of the decision is resulted.