

МЕТОДИКА СИСТЕМНОГО АНАЛИЗА ДЕСТАБИЛИЗИРУЮЩИХ ПРОГРАММНЫХ ВОЗДЕЙСТВИЙ

В.И. Батищев, А.В. Дорфман

Самарский государственный технический университет
443100, г. Самара, ул. Молодогвардейская, 244
E-mail: vib@list.ru

Проведен анализ базовых методик системного анализа. На их основе разработана новая методика системного анализа дестабилизирующих программных воздействий, в которой выделены этапы моделирования проблемы и выработки решения проблемы, предусмотрена итеративность, обеспечивающая нахождение оптимального решения проблемы.

Ключевые слова: компьютерные вирусы, дестабилизирующие программные воздействия, методика системного анализа, математическое и системное моделирование.

Для функционирования программных систем управления и обработки информации большую угрозу представляют компьютерные вирусы, троянские программы, другие виды вредоносных программ, а также программные ошибки и уязвимости, которые были объединены авторами под общим термином – дестабилизирующие программные воздействия (ДПВ).

Наибольшие научные и практические результаты достигнуты в области компьютерной вирусологии, занимающейся изучением вредоносных программ и включающей четыре направления: экспериментальные исследования экземпляров вирусов, разработка методов их анализа, разработка средств защиты и теоретические исследования, посвященные созданию математических моделей вирусов и выявлению с их помощью обобщенных свойств вирусов.

В области исследования ошибок и уязвимостей существует ряд методов для их выявления, часть из которых основана на распознавании сигнатур ошибок при анализе исходных текстов, другая часть работает с бинарным кодом без исходных текстов и основана на генерации случайных входов для программной системы с целью вызвать в ней ошибку – фаззинг.

Сообщения об успешных атаках компьютерных вирусов и атаках, основанных на уязвимостях, свидетельствуют о недостаточной эффективности современных средств распознавания ДПВ. Истоки данной неэффективности лежат в ряде проблем, причем основной следует признать отсутствие системных исследований дестабилизирующих программных воздействий.

Поэтому была поставлена задача системного анализа дестабилизирующих программных воздействий [1, 2]. Вследствие отсутствия методик системного анализа в данной предметной области было решено провести анализ базовых, так сказать, пионерских методик системного анализа [3-8], затем выбрать среди них подходящую или синтезировать новую методику системного анализа ДПВ.

Виталий Иванович Батищев (д.т.н., профессор), заведующий кафедрой «Информационные технологии».

Антон Владимирович Дорфман (к.т.н., доцент), доцент кафедры «Электронные системы и информационная безопасность».

В исследовании Э. Квейда [1] предложена методика системного анализа для военных решений (табл. 1). Она содержит пять этапов, изложенных в довольно общих формулировках.

Таблица 1

Методика системного анализа Э. Квейда

1	Постановка задачи	Определение существа проблемы, выявление целей и определение границ задачи
2	Поиск	Сбор необходимых сведений, определение альтернативных средств достижения поставленных целей
3	Толкование	Построение модели и ее использование для исследования результатов применения альтернативных средств, обычно путем оценки их стоимости и характеристик
4	Рекомендация	Определение предпочтительной альтернативы или курса действий, что может представлять собой сочетание характерных свойств рассмотренных альтернатив или их модификаций, необходимых для учета факторов, не принятых во внимание на ранних этапах исследования
5	Подтверждение	Экспериментальная проверка рекомендации

В этапе 4 методики заложена важная особенность – возможность синтеза собственного решения на основе выгодных свойств альтернатив.

В работе С. Оптнера [4] и вступительной статье С.П. Никанорова «Системный анализ: этап развития методологии решения проблем в США» к этой работе представлены две методики (табл. 2).

Этапы 1, 2, 3 данных методик похожи и, по сути, являются детализацией этапа 1 методики Э. Квейда. Никаноров отдельно выделяет этап 4 – определение критериев и укрупняет этапы 11, 12 С. Оптнера в свой этап 12. В остальном этапы обеих методик практически идентичны, и часть из них является детализацией этапов методики Э. Квейда. Следует отметить первую часть этапа 4 от С. Оптнера – вскрытие структуры системы и этап 13, позволяющий оценить результаты реализации решения.

Работа С. Янга [5] описывает системный анализ как методологию совершенствования организации и представляет методику, состоящую из следующих десяти этапов: определение целей организации, выявление проблем в процессе достижения этих целей, исследование проблем и постановка диагноза, поиск решения проблемы, оценка всех альтернатив и выбор наилучшей из них, согласование решений в организации, утверждение решения, подготовка к вводу решения в действие, управление применением решения, проверка эффективности решения. По данной методике можно сделать вывод, что если не учитывать ее специфику, ее этапы уже встречались в рассмотренных ранее методиках.

В работе Н.П. Федоренко [6] приводится методика, состоящая из восьми этапов: формулирование проблемы, определение целей, сбор информации, разработка максимального количества альтернатив, отбор альтернатив, построение модели в виде уравнений, программ или сценария, оценка затрат, испытание чувствительности решения (параметрическое исследование). Новшеством здесь является последний пункт. Кроме того, необходимо отметить этап построения модели, который встречался только у Квейда.

Методики системного анализа С. Оптнера и С. П. Никанорова

<i>По С. Оптнеру</i>	<i>По С.П. Никанорову</i>
Идентификация симптомов	Обнаружение проблемы
Определение актуальности проблемы	Оценка актуальности проблемы
Определение цели	Определение цели и принуждающих связей
Вскрытие структуры системы и ее дефектных элементов	Определение критериев
Определение структуры возможностей	Определение дефектных элементов существующей системы, ограничивающих получение заданного выхода, оценка веса их влияния на определяемые критериями выходы системы
Нахождение альтернатив	Определение структуры для построения набора альтернатив
Оценка альтернатив	Построение набора альтернатив
Выбор альтернативы	Оценка альтернатив
Составление решения	Выбор альтернатив для реализации
Признание решения коллективом исполнителей и руководителей	Определение процесса реализации
Запуск процесса реализации решения	Согласование найденного решения
Управление процессом реализации решения	Реализация решения
Оценка реализации и ее последствий	Оценка результатов реализации решения

В работе [5] представлена методика системного анализа, применяемая при отраслевом планировании и содержащая семь этапов: постановка задачи, исследование, анализ, предварительное суждение, подтверждение, окончательное суждение, реализация принятого решения. Отметим, что в ней появились зачатки итеративности, полезное свойство, которое можно использовать.

В исследовании Ю.И. Черняка [8] обобщены результаты предыдущих работ [3-7] и представлена проработанная и подробная методика системного анализа, применяемая при управлении в экономической отрасли (табл. 3).

Данную методику отличает от предыдущих ее детальная проработка, однако она имеет свою специфичную область применения.

Таблица 3

Методика системного анализа Ю.И. Черняка

Анализ проблемы	Существует ли проблема? Точное формулирование проблемы Анализ логической структуры проблемы Развитие проблемы (в прошлом и будущем) Внешние связи проблемы (с другими проблемами) Принципиальная разрешимость проблемы
-----------------	---

Определение системы	Спецификация задачи Определение позиции наблюдателя Определение объекта Выделение элементов (определение границ разбиения системы) Определение подсистем Определение среды
Анализ структуры системы	Определение уровней иерархии (в больших системах) Определение аспектов и языков (в сложной системе) Определение процессов-функций (в динамической системе) Определение и спецификация процессов управления и каналов информации (в кибернетических системах) Спецификация подсистем Спецификация процессов (функций) текущей деятельности (рутинных) и развития (целевых)
Формирование общей цели и критерия системы	Определение целей-требований надсистемы Определение целей и ограничений среды Формулирование общей цели Определение критерия Декомпозиция целей и критериев по подсистемам Композиция общего критерия и критериев подсистем
Декомпозиция цели, выявление потребности в ресурсах и процессах	Формулирование целей верхнего ранга Формулирование целей текущих процессов Формулирование целей эффективности Формулирование целей развития Формулирование внешних целей и ограничений Выявление потребностей в ресурсах и процессах
Выявление ресурсов и процессов, композиция целей	Оценка существующей технологии и мощностей Оценка современного состояния ресурсов Оценка реализуемых и запланированных проектов Оценка возможностей взаимодействия с другими системами Оценка социальных факторов Композиция целей
Прогноз и анализ будущих условий	Анализ устойчивых тенденций развития системы Прогноз развития и изменения среды Предсказание появления новых факторов, оказывающих сильное влияние на развитие системы Анализ ресурсов будущего Комплексный анализ взаимодействия факторов будущего развития Анализ возможных сдвигов целей и критериев
Оценка целей и средств	Вычисление оценок по критерию Оценка взаимодействия целей Оценка относительной важности целей Оценка дефицитности и стоимости ресурсов Оценка влияния внешних факторов Вычисление комплексных расчетных оценок
Отбор вариантов	Анализ целей на совместимость и входимость Проверка целей на полноту Отсечение избыточных целей Планирование вариантов достижения отдельных целей Оценка и сравнение вариантов Совмещение комплекса взаимосвязанных вариантов
Диагноз существующей системы	Моделирование технологического и экономического процесса Расчет потенциальной и фактической мощности

	Анализ потерь мощности Выявление недостатков организации производства и управления Выявление и анализ мероприятий по совершенствованию организации
Построение комплексной программы развития	Формулирование мероприятий, проектов и программ Определение очередности целей и мероприятий по их достижению Распределение сфер деятельности Распределение сфер компетенции Разработка комплексного плана мероприятий в рамках ограничений по ресурсам во времени Распределение по ответственным организациям, руководителям и исполнителям
Проектирование организации для достижения целей	Назначение целей организации Формулирование функций организации Проектирование организационной структуры Проектирование информационных механизмов Проектирование режимов работы Проектирование механизмов материального и морального стимулирования

Анализ базовых методик позволил выявить, что во всех них в той или иной форме представлены этапы выявления проблемы, постановки целей, нахождения альтернатив, оценки и выбора альтернатив, реализации решения. В некоторых также есть этап оценки эффективности решений. Поскольку в методиках не ясна взаимосвязь между этапами, в частности возможность возвращаться к предыдущим этапам, то отсутствует итеративность. Также не является ясным, что делать, если нет альтернатив или существующие альтернативы не устраивают, что имеет место в нашем случае. В целом можно отметить, что ни одна из рассмотренных методик не пригодна для системного анализа ДПВ. Поэтому было решено разработать новую авторскую методику на основе синтеза лучших особенностей проанализированных.

В системном смысле о компьютерных вирусах (вредоносных программах) можно сделать следующие выводы. Вирус является искусственной технической системой, созданной без использования аппарата математического моделирования на основе интуиции и опыта конкретного автора. При этом в нее закладываются некоторые свойства адаптивности, поскольку ее дальнейшее функционирование происходит без какого-либо вмешательства со стороны разработчика.

Разработанная методика системного анализа дестабилизирующих программных воздействий представлена на рисунке.

Преимуществом данной методики является то, что она вобрала в себя все лучшее от проанализированных. Выделены этапы моделирования проблемы и выработки ее решения, существует итеративность, которая гарантирует нахождение оптимального решения. Помимо этого введено экспериментальное исследование, в процессе которого анализируются экземпляры ДПВ с целью выявления закономерностей их функционирования.

В соответствии с предложенной методикой был проведен системный анализ компьютерных вирусов. На этапе 1 в качестве проблемы выбраны компьютерные вирусы и проведен анализ их влияния на программные средства промышленного применения. Целью исследования выбрано создание новой информационной технологии – нового способа распознавания компьютерных вирусов. В соответствии



Методика системного анализа дестабилизирующих программных воздействий

с этапом 2 проведено экспериментальное исследование компьютерных вирусов, на основе которого на этапе 3 выявлены компоненты системы, реализованы ее декомпозиция, системная модель состава вируса и функциональная классификация вирусов. Существующие способы распознавания компьютерных вирусов проанализированы на основе декомпозиции системы «компьютерный вирус» на этапе 4, и проведенная оценка альтернатив выявила, что существующие способы распознавания не удовлетворяют поставленной цели. Исходя из выявленных системных свойств вирусов и поставленных задач исследования на этапе 5 сформированы требования к математической модели компьютерного вируса. Далее на этапе 6 проведен анализ существующих моделей вируса и возможного их развития на соответствие данным требованиям, в результате которого выявлено, что ни одна из моделей не удовлетворяет им полностью. На этапе 7 на основе проведенного анализа существующих математических моделей и требований к ним разработана собственная модель системы «компьютерный вирус». В рамках разработанного формализма и моделей на этапе 8 сформировано решение задачи распознавания компьютерных вирусов, которое реализовано в виде программной системы распознавания вирусов на этапе 9. На этапе 10 проведена экспериментальная проверка решения, то есть тестирование способности системы к распознаванию вирусов. Оценка эффективности по сравнению с существующими

антивирусными средствами проведена на этапе 11. В результате выявлено, что решение эффективно и цель исследования достигнута. В случае, если бы этого не произошло, выполнялся бы этап 12, который заключается в доработке модели решения и последующем переходе к этапу 8.

Проведенный системный анализ компьютерных вирусов и полученные результаты свидетельствуют о работоспособности предложенной методики системного анализа дестабилизирующих программных воздействий. Необходимо отметить, что с помощью данной методики возможен системный анализ других классов дестабилизирующих программных воздействий, например троянских программ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Теоретические основы системного анализа / В.И. Новосельцев и др.; Под ред. В.И. Новосельцева. – М.: Майор, 2006. – 592 с.
2. Теория систем и системный анализ в управлении организациями: Справочник: Учеб. пособие / Под ред. В.Н. Волковой и А.А. Емельянова. – М.: Финансы и статистика, 2006. – 848 с.
3. Квейд Э. Анализ сложных систем. Пер. с англ. под ред. И.И. Ануреева, И.М. Верещагина. – М.: Сов. радио, 1969. – 520 с.
4. Оптнер С. Системный анализ для решения деловых и промышленных проблем. – М.: Сов. радио, 1969. – 216 с.
5. Янг С. Системное управление организацией. – М.: Сов. радио, 1972. – 455 с.
6. Федоренко Н.П. О методах социально-экономического прогнозирования // Методология прогнозирования экономического развития СССР. – М.: Экономика, 1971.
7. Голубков Е.П. Использование системного анализа в отраслевом планировании. – М.: Экономика, 1977. – 136 с.
8. Черняк Ю.И. Системный анализ в управлении экономикой. – М.: Экономика, 1975. – 191 с.

Статья поступила в редакцию 14 июня 2012 г.

A SYSTEMS ANALYSIS METHOD FOR DESTABILIZING PROGRAMMATIC INFLUENCES

V.I. Batishchev, A.V. Dorfman

Samara State Technical University
244, Molodogvardeyskaya st., Samara, 443100

Some basic methods of systems analysis are analyzed. A new systems analysis method for destabilizing programmatic influences is developed on their basis, the stages of problem formulating and problem solving being given with iterations, which makes possible finding the best solution of the problem.

Keywords: *computer viruses, destabilizing programmatic influences, method of analysis of the systems, mathematical and system design.*

*Vitaly I. Batishchev (Dr. Sci. (Techn.)), Professor.
Anton V. Dorfman (Ph.D. (Techn.)), Associate Professor.*