Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»

Ю. М. МОНАХОВ Л. М. ГРУЗДЕВА

ТЕОРЕТИЧЕСКОЕ И ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ РАСПРЕДЕЛЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ ВРЕДОНОСНЫХ ПРОГРАММ

Монография

Владимир 2013

УДК 930.1
ББК 32.81
М77

Рецензенты:
Заслуженный деятель науки России
доктор технических наук, профессор
зав. кафедрой радиотехники и радиосистем
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых
О. Р. Никитин

Доктор физико-математических наук, профессор
зав. кафедрой алгебры и геометрии
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых
Н. И. Дубровин

Доктор технических наук, профессор
кафедры инновационного предпринимательства Московского
государственного технического университета им. Н. Э. Баумана
Д. В. Александров

Доктор технических наук, профессор
зав. кафедрой информационного обеспечения в правовой сфере
Юридического института Московского
государственного университета путей сообщения
С. Л. Лобачев

Печатается по решению редакционно-издательского совета ВлГУ

Монахов, Ю. М.

М77 Теоретическое и экспериментальное исследование распределенных телекоммуникационных систем в условиях воздействия вредоносных программ : монография / Ю. М. Монахов, Л. М. Груздева ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2013. – 132 с.
ISBN 978-5-9984-0293-7

Приведены результаты теоретического и экспериментального исследований распределенных телекоммуникационных систем, находящихся под воздействием вредоносных программ.

Предназначена для научных и инженерных работников, занимающихся проблемой обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах.

Ил. 71. Табл. 19. Библиогр.: 117 назв.

УДК 930.1
ББК 32.81

ISBN 978-5-9984-0293-7

Предисловие

Основная проблема, которой посвящена данная работа, – существенное снижение производительности и качества функционирования современных распределенных телекоммуникационных систем (РТКС) из-за воздействия вредоносного программного обеспечения. Вредоносные программы – это, прежде всего, компьютерные вирусы, ,,сетевые черви'' и ,,троянские кони''. Компьютерные вирусы и ,,сетевые черви'' характеризуются в первую очередь способностью к саморазмножению (саморепродукции). Распространением на другие компьютеры вирус сам не занимается, предоставляя делать это человеку, копирующему программы с одной машины на другую. Для сетевого червя саморазмножение – это именно процесс распространения с одного компьютера на другой по сети, а на одной машине иметь более одной копии ему не только не нужно, но и вредно, так как каждая копия отнимает дополнительные ресурсы.

,,Троянские кони'' характеризуются, прежде всего, функцией нанесения ущерба.

В данной работе мы будем рассматривать компьютерные вирусы, ,,черви'', и ,,трояны'', называя их обобщенно вредоносными программами (ВП).

Эпидемии выделенных ВП в настоящее время наносят существенный ущерб различным организациям. За последние 10 – 15 лет распространение вредоносного кода, носившее локальный характер, превратилось в глобальные эпидемии вредоносных программ. Работа и функционирование многих структур и организаций тесно связаны с глобальными сетями или полностью зависят от них. Сетевые ВП, размножающиеся в неограниченном количестве, забивают каналы передачи информации, тем самым нанося огромные убытки, не говоря уже о том, что код вредоносной программы может содержать деструктивные функции, что может привести к потере или утечке конфиденциальной информации.

Современная ВП может инфицировать большую часть вычислительных машин всего за несколько часов ввиду масштабов Интернета и огромных пропускных способностей каналов передачи данных. Многие исследователи вирусных компьютерных эпидемий отмечают, что со-

временные ВП используют далеко не самые оптимальные стратегии поиска новых компьютеров для заражения. В будущем возможно появление вредоносного кода, способного распространяться за считанные секунды, благодаря использованию усовершенствованных стратегий распространения. Моделирование эпидемий ВП показывает, что большую часть времени, за которое доля инфицированных компьютеров достигает своего максимального значения, вредоносная программа тратит на заражение небольшого в масштабах эпидемии числа компьютеров. Таким образом, в будущем возможно ускоренное развитие эпидемий ВП в результате внедрения механизма предварительного анализа состояния сети передачи данных, т.е. составления списка уязвимых компьютеров, который будет использоваться для того, чтобы захватить некоторое «критическое» число уязвимых компьютеров. Если это «критическое» число компьютеров будет захвачено, дальнейшее распространение будет происходить лавинообразно.

Современное программное обеспечение также не способствует снижению числа новых эпидемий ВП. Новые уязвимости в различных программах находят практически каждый день, производители программного обеспечения не всегда оперативно их устраняют, а готовые „заплатки" устанавливаются очень медленно.

Таким образом, в настоящее время существует множество факторов, способствующих появлению массовых эпидемий ВП.

Задача противодействия распространению ВП крайне актуальна. Все организации, работа которых так или иначе связана с использованием сетей передачи данных, терпят убытки от постоянных вспышек эпидемий сетевых червей, новые модификации которых появляются каждый день.

Противодействие распространению и созданию вредоносных программ – очень сложная задача, которая имеет множество аспектов, в том числе моделирование и методы предсказания распространения вредоносных программ. С помощью математических моделей можно оценить масштабы возможной эпидемии, изучить динамику изменения числа зараженных компьютеров и т. д. Моделирование также может быть использовано для того, чтобы оценить эффективность тех или иных мер противодействия распространению.

Анализ производительности распределенной телекоммуникационной системы в условиях вредоносного информационного воздействия, приводящего, возможно, к ее непредсказуемому функционированию, является задачей весьма непростой. Причина тому – усложнение структуры и режимов функционирования распределенных систем, что за-

трудняет применение классических методов теории систем массового обслуживания ввиду возрастающей размерности решаемых задач.

Монография отражает результаты теоретической и экспериментальной работы авторов по данной проблеме. В многочисленных экспериментах по моделированию атак вредоносных программ, методов противодействия и структурных решениях РТКС принимали участие аспиранты и студенты кафедры «Информатика и защита информации» Владимирского государственного университета.

В первой главе на основе нелинейной модели трофического взаимодействия популяций Лотки – Вольтерра предложена модель захвата ресурса распределенной телекоммуникационной системы. Формализация модели позволила систематизировать подход к определению необходимости и достаточности мер защиты распределенной системы от внешних угроз. Приводятся результаты экспериментального исследования, показавшие возможность предсказания с определенной степенью точности конечного состояния РТКС при известных начальных параметрах системы и атаки.

Во второй главе рассмотрены модели построения решающих правил обнаружения вредоносных программ в РТКС. Предложен алгоритм обнаружения вредоносных программ, основанный на понятии критической области угроз, реализация которого позволяет улучшить временные и вероятностные характеристики колец защиты. Приводятся результаты экспериментального исследования вероятностных характеристик антивирусных программ, по результатам которого построена критическая область угроз.

В третьей главе рассмотрены модели противодействия атакам вредоносных программ в распределенной телекоммуникационной системе, основанные на результатах теории нелинейных динамических систем. Модели учитывают системные параметры, характеристики вредоносных программ и программ информационной защиты. Приводятся результаты теоретического исследования разработанных моделей. Анализируются возможности прогнозирования всплесков деструктивной активности в распределенной системе.

В четвертой главе предложены аналитические и имитационные модели оценки производительности РТКС в условиях воздействия вредоносных и антивирусных программ. Приведены методики и алгоритмы расчета локальных временных и безразмерных характеристик производительности. Приводятся результаты экспериментального и модельного исследования влияния вредоносных программ на характеристики распределенной системы.

Глава 1

Модель атаки захвата ресурса распределенной телекоммуникационной системы

√ Классическая модель трофического взаимодействия биологических популяций – прообраз модели захвата ресурсов РТКС

√ Модель атаки и противодействия в распределенной телекоммуникационной системе

√ Исследование модели

√ Модель с многоуровневой системой информационной защиты

На основе нелинейной модели трофического взаимодействия популяций Лотки – Вольтерра предложена модель захвата ресурса распределенной телекоммуникационной системы. Формализация модели позволяет систематизировать подход к определению необходимости и достаточности мер защиты распределенной системы от внешних угроз. Экспериментальное исследование показало возможность предсказания с определенной степенью точности конечного состояния РТКС при известных начальных параметрах системы и атаки

Введение

Возросшая сложность архитектуры распределенных телекоммуникационных систем (РТКС) и, как следствие, увеличение количества уязвимостей и потенциальных ошибок в их функционировании, а также возросшие возможности по реализации атак обусловливают необходимость разработки мощных автоматизированных интеллектуальных систем противодействия информационным угрозам.

Обеспечение работоспособности РТКС и функционирующих в ней прикладных информационных систем, гарантированно устойчивых к вредоносным воздействиям и компьютерным атакам, сопряжено с существенными затратами как времени, так и материальных ресурсов. Кроме того, существует известная обратная зависимость между удобством пользования системой и её защищённостью: чем совершеннее системы защиты, тем сложнее пользоваться основным функционалом информационной системы.

К настоящему времени опубликован ряд работ, раскрывающих различные подходы к моделированию информационных атак и анализу защищенности, из них выделим метод анализа изменения состояний [91], причинно-следственную модель атак [92], описательные модели сети и злоумышленников [117], структурированное описание на базе деревьев [94], использование и создание графов атак для анализа уязвимостей [102], объектно-ориентированное дискретное событийное моделирование [90] и др. Тем не менее методы обнаружения атак и защиты от них в современных РТКС недостаточно проработаны в части формальной модели атаки, для которой достаточно сложно строго оценить такие параметры, как вычислительная сложность, корректность, завершимость и т.д.

Поэтому возрастает необходимость разработки адекватных моделей информационных атак, исследования их влияния на РТКС с целью совершенствования системы обеспечения информационной безопасности.

Целью настоящей работы является разработка и исследование модели информационной атаки захвата ресурса распределенной телекоммуникационной системы, модели функционирования (поведения) РТКС, находящейся под воздействием информационной атаки.

Функционирование механизма, положенного в основу разработанных моделей, происходит исходя из следующих предположений [34 – 36, 53, 58 – 61]:

а) рассматривается атака на РТКС, заключающаяся в «захвате» вычислительных ресурсов (памяти, процессорного времени) компьютеров распределенной телекоммуникационной системы. Захват вычислительных ресурсов пораженного компьютера преследует цель инициирования еще одной (аналогичной) информационной атаки на другие компьютеры РТКС;

б) компьютеры распределенной телекоммуникационной системы пытаются отражать вышеназванную угрозу. Успешность отражения зависит как от параметров атакующего процесса, так и от системных характеристик РТКС, включая среду передачи данных, компьютеры, систему информационной защиты;

в) характер противоборства атакующих и защищающихся компьютеров описывается по аналогии с известными динамическими моделями размножения – гибели биологических существ (трофическое взаимодействие популяций).

1.1. Классическая модель трофического взаимодействия биологических популяций – прообраз модели захвата ресурсов РТКС

Нелинейные динамические системы даже небольшой размерности могут демонстрировать весьма сложное поведение [43]. В частности, в них возможны хаотические режимы различных типов. Динамика процесса в одной области фазового пространства может существенно отличаться от динамики в другой области этого пространства. Рассмотрим пример такой системы малой размерности, имея в виду, что методы её анализа могут быть применены и к более сложным задачам.

В частности, ряд методов решения задач большой размерности основан на том, что фазовое пространство динамических систем зачастую неоднородно: состояние системы в определённых его областях может быть с приемлемой точностью охарактеризовано небольшим количеством переменных, составляющих проекцию малой размерности. Прочие переменные могут быть подчинены переменным проекции (называемым параметрами порядка) и/или несущественны с точ-

ки зрения описания системы в рамках решаемой задачи. Типичность этой ситуации показывает теория самоорганизации, или синергетика, где такое поведение часто связывают с принципом подчинения короткоживущих мод долгоживущим [30, 40, 83, 103].

Проекция малой размерности может иметь смысл на всём фазовом пространстве и в широком классе задач, как это имеет место, например, во многих физических системах. Также возможны более сложные случаи, когда проекции малой размерности могут использоваться в ограниченных областях фазового пространства, причём в разных областях проекции необязательно одинаковы. Примером последнего являются автономные системы с чередующейся медленно-быстрой динамикой: лазеры, сложные пищевые цепи в биологии, колебательные химические реакции, и др. Фазовые переменные таких систем могут делиться на медленно меняющиеся и быстро меняющиеся. Тогда в фазовом пространстве выделяются зоны медленного движения, где медленно меняющиеся переменные являются параметрами порядка, и зоны быстрого движения, где медленно меняющиеся переменные играют роль параметров.

К системам, демонстрирующим медленно-быструю динамику, относятся многие сингулярно возмущённые системы обыкновенных дифференциальных уравнений, иерархизированные по характерным временам изменения переменных в силу наличия малых параметров при производных. Как известно, решение такой системы в соответствии с теоремой Тихонова [10, 75, 76] стремится к решению вырожденной системы, в которой соответствующие параметры взяты равными нулю.

Модели пищевых цепей в биологии – класс систем, весьма любопытный с точки зрения изучения сложной динамики. Будучи сравнительно просто устроенными, они в то же время могут демонстрировать довольно разнообразное, сложное и интересное поведение [98].

В качестве элементарного объекта рассматривается популяция (сообщество) – совокупность особей одного вида. Главной характеристикой популяции будем считать её численность x, а основной функцией – размножение (ауторепродукцию). Свойства популяций:

– непрерывность. Предполагается, что численность популяций можно считать величиной непрерывной, что позволяет использовать дифференциальные уравнения для моделирования ее поведения (в

случае моделирования с помощью отображений (модели с дискретным временем), это свойство не является необходимым);

– однородность – абсолютная идентичность особей;

– локальность (сосредоточенность, полное перемешивание). Предполагается отсутствие каких-либо пространственных эффектов, т.е. исследуется зависимость численности популяции исключительно от времени: $x = x(t)$. Пространственные переменные в модель не входят;

– автономность. Данный термин употребляется в том же смысле, что и в теории дифференциальных уравнений. Будем считать, что условия обитания, а также характер взаимодействия сообщества с другими сообществами и со средой обитания не зависят от времени. В частности, имеется в виду отсутствие зависимости от времени способности особей к размножению. Также сделаем предположение об отсутствии внешних воздействий на популяцию, таких как изменения климата, мутагенные воздействия, сезонный промысел и т.п. Будем учитывать только воздействия других сообществ, а также изменения среды обитания в результате жизнедеятельности самой популяции [3, 98, 110].

Представления о ряде свойств сообщества и среды обитания можно получить, рассматривая простейший случай – изолированную популяцию, то есть популяцию, не взаимодействующую ни с какими другими. В данном случае для описания динамики численности популяции (в условиях сделанных предположений) достаточно единственного уравнения вида

$$\frac{dx}{dt} = F(x) \equiv xf(x), \qquad (1.1)$$

называемого *моделью роста популяции,* или *уравнением популяционного баланса.* Функция $F(x)$ называется абсолютной скоростью размножения особей, а будучи отнесённой к численности популяции, – удельной скоростью размножения $f\{x)$ [7, 85, 86, 104].

Усложняя модель, предполагают, что процессы рождения и гибели особей описываются разными функциями:

$$\frac{dx}{dt} = x[b(x) - d(x)]. \qquad (1.2)$$

Здесь, помимо функции скорости размножения $b(x)$, в модель вводится функция скорости смертности $d(x)$.

Вид функций размножения и смертности определяется исходя из учитываемых элементарных факторов. В простейшем случае считается, что скорости размножения и смертности постоянны: $f(x) = const$. Отсюда следует классическое уравнение размножения, или удельная скорость роста (per-capita growth rate), – уравнение Мальтуса [7, 71, 77, 95]

$$\frac{dx}{dt} = x[b(x) - d(x)] = ax\,. \qquad (1.3)$$

При положительных значениях a имеет место неограниченный экспоненциальный рост популяции, а при отрицательных – экспоненциальное вымирание.

В рассмотренных выше простейших моделях, если популяция растёт, а не вымирает, то она растёт неограниченно. На практике, как известно, подобного не наблюдается в силу наличия ряда факторов, ограничивающих рост изолированной популяции. Самым простым распространённым и важным из таких ограничивающих факторов является ограничение на ресурсы – пищу, воду, энергию, жизненное пространство, удаление отходов. Данное ограничение приводит к внутривидовой конкуренции за ресурсы, результатом является уменьшение скорости размножения и/или увеличение скорости смертности с ростом популяции. Проще всего было бы предположить, что ограничивающее влияние численности популяции на размножение и смертность линейно:

$$\begin{cases} b(x) = b_0(x) - e_b x, \\ d(x) = d_0(x) + e_d x. \end{cases} \qquad (1.4)$$

Подстановка в (1.2) с учётом (1.3) даёт уравнение Ферхюльста – Пирла, или логистическое уравнение [77, 95]

$$\frac{dx}{dt} = ax - ex^2 = ax\left(1 - \frac{x}{K}\right), \qquad (1.5)$$

где e называется коэффициентом внутривидовой конкуренции.

Параметр $K = \frac{a}{e}$ именуется ёмкостью экологической ниши популяции, так как в пределе при $t \to 0$ численность сообщества стабилизируется на уровне $K = x$.

Усложняем модель путем учета нескольких взаимодействующих популяций. Из всех типов межвидовых отношений [69] нас прежде всего интересуют трофические отношения – паразитизм, хищниче-

ство, поедание растений: увеличение биомассы популяции 2 за счёт уменьшения биомассы популяции 1 (различные термины используются в зависимости от деталей процесса перераспределения биомассы). Вид, увеличивающий биомассу в результате взаимодействия, будем называть хищником, а вид, уменьшающий биомассу, – жертвой. В отличие от случая изолированной популяции для описания совокупности взаимодействующих популяций требуется система дифференциальных уравнений вида

$$\begin{cases} \dfrac{dx_1}{dt} = F_1(x_1,\ldots,x_N) \equiv x_1 f_1(x_1,\ldots,x_N), \\ \ldots \\ \dfrac{dx_N}{dt} = F_N(x_1,\ldots,x_N) \equiv x_N f_N(x_1,\ldots,x_N), \end{cases} \tag{1.6}$$

где N – количество взаимодействующих популяций; x_i – их численности; F_i – абсолютные скорости размножения особей вида i ; f_i – удельные скорости размножения.

Уравнения системы должны включать члены, отвечающие за межпопуляционное взаимодействие; их вид определяется на основе перечня учитываемых элементарных факторов.

Пусть дана простейшая экосистема, состоящая из двух взаимодействующих видов, один из которых играет роль хищника, а другой – жертвы. Для построения её математической модели необходим учёт, как минимум, следующих элементарных факторов:

а) размножение жертв. Как и в случае изолированной системы, уравнение для жертвы должно включать член, отвечающий за размножение (жертва является источником биомассы). Также говорят, что популяция жертв обладает свойством автотрофности, т.е., будучи изолированной, способна размножаться;

б) вымирание хищников. В отсутствие пищи (жертв) уравнение для хищника выглядит как $\dfrac{dx}{dt} = -d(x)$, где $d(x)$ – функция смертности. Также говорят, что популяция хищников обладает свойством гетеротрофности, т.е., будучи изолированной, вымирает. Для простоты будем считать, что у хищника нет альтернативных источников питания;

в) переработка биомассы. Как было отмечено выше, в результате взаимодействия биомасса жертв уменьшается, а биомасса хищников увеличивается. Данный фактор, таким образом, играет двоякую роль: с одной стороны, он отвечает за ограничение размножения

жертв, а с другой стороны, – за поддержание численности популяции хищников (предотвращение вымирания). В условиях сделанных предположений члены, отвечающие за переработку биомассы, должны зависеть от численности обеих популяций и входить в уравнения системы с разным знаком.

Таким образом, уравнения популяционного баланса (1.6) примут вид

$$\begin{cases} \dfrac{dy_1(t)}{dt} = (a - by_2(t))y_1(t), \\ \dfrac{dy_2(t)}{dt} = (-c + dy_1(t))y_2(t), \end{cases} \tag{1.7}$$

где $t \in [t_0, t_1]$ – текущее время, изменяющееся на указанном интервале решения задачи; $y_1(t)$, $y_2(t)$ – текущие численности популяций жертв и хищников соответственно.

Параметры a, b, c, d предполагаются известными постоянными. Смысл их следующий. Параметр a выражает скорость естественного прироста популяции жертв в единицу времени в расчете на одну жертву в отсутствие хищников. Параметр c – скорость естественной гибели (от голода) популяции хищников в единицу времени в расчете на одного хищника в отсутствие жертв. Коэффициенты b – относительная скорость гибели популяции жертв хищников, d – относительная скорость прироста популяции.

Простейшая математическая модель трофического взаимодействия двух популяций известна под названием модели Лотки – Вольтерра [13, 107].

1.2. Модель атаки и противодействия в распределенной телекоммуникационной системе

Модифицируем вышеприведенную модель применительно к РТКС. Пусть жертвы – уязвимые компьютеры – узлы РТКС, их количество $y_1(t)$, хищники – пораженные компьютеры (узлы), они осуществляют информационные преднамеренные воздействия – атаки, количество таких компьютеров $y_2(t)$. С течением времени в отсутствии атак поврежденная система восстанавливается, следовательно, коэффициент a (1.7) будет выражать скорость прироста уязвимых компьютеров. В дальнейшем эту скорость будем обозначать f. В случае отсутствия уязвимых компьютеров (т.е. РТКС неуязвима для ата-

ки) число атакующих компьютеров уменьшается, параметр c выражает скорость такого уменьшения. Параметр d будет отражать влияние на скорость прироста атакующих компьютеров числа уязвимых компьютеров (назовем данный параметр «коэффициентом уязвимости»). Выражение $(-by_2(t))$ количественно отражает текущие потери от атак, т.е. количество захваченных компьютеров.

Пусть РТКС содержит N (потенциально уязвимых к атакам) компьютеров (узлов). Параметр K содержит начальное значение среднего количества атакуемых компьютеров за выбранную единицу времени. В дальнейших рассуждениях будем считать, что K является константой на протяжении всего противостояния, несмотря на различия в мощностях и типах атакуемых компьютеров и пропускной способности каналов связи. Кроме того, модель упрощается за счет того, что один и тот же компьютер не может быть атакован дважды.

Пусть $\mu(t)$ – доля уязвимых компьютеров, которые были успешно атакованы за время t, тогда $(N \cdot \mu(t))$ представляет собой общее количество успешно атакованных компьютеров, каждый из которых будет использован для проведения последующих атак со средним их количеством K. Поскольку часть компьютеров уже была успешно атакована, каждым новым захваченным компьютером будет произведено $(K(1-\mu(t))$ новых успешных атак. Таким образом, прирост количества успешно атакованных компьютеров за период времени dt будет определяться из уравнения

$$\frac{dN_{усп}}{dt} = \mu(t)K(1-\mu(t)). \qquad (1.8)$$

С другой стороны, $N_{усп} = N \cdot \mu(t)$, что ведет к дифференциальному уравнению вида

$$\frac{d\mu(t)}{dt} = K\mu(t)(1-\mu(t)). \qquad (1.9)$$

Еще усложним модель. Учтем тот факт, что РТКС состоит из нескольких автономных подсетей. Каждый компьютер РИВС может взаимодействовать в любой момент времени с любым другим (и произвольным количеством компьютеров вне РТКС, например в Интернете).

Введем параметр p_j – вероятность того, что захваченный компьютер в подсети, состоящей из N_j компьютеров, будет атаковать компьютеры в этой же подсети, тогда $(1-p_j)$ – вероятность того, что

атакуемый компьютер будет находиться вне этой подсети. Тогда для автономной системы – подсети j – будет верно

$$\frac{d\mu_j(t)}{dt} = \frac{1-\mu_j(t)}{N}\left\{N_j\mu_j(t)p_jK + (1-p_j)\sum_{i\neq j}N_i\mu_i(t)K\right\} \qquad (1.10)$$

Будем считать постоянной долю уязвимых компьютеров, которые были успешно атакованы за время t в любой подсети РТКС:

$$\mu_j(t) = \mu_w(t) = \mu$$

Подставим уравнение (10) в исходную систему (7). Получим

$$\begin{cases} \dfrac{dy_1(t)}{dt} = \dfrac{1-\mu(t)}{N}(a - (N_j\mu\, p_j + (1-p_j)(N-N_j)\mu\, y_2(t))y_1(t), \\ \dfrac{dy_2(t)}{dt} = (-c + dy_1(t))y_2(t), \end{cases} \qquad (1.11)$$

Поскольку система информационной защиты «срабатывает» не сразу, т.е. с момента начала атаки проходит некоторое время, введем дополнительный параметр λ (коэффициент осцилляции), который будет выражать задержку в срабатывании системы безопасности.

Тогда конечная система уравнений будет иметь вид

$$\begin{cases} \dfrac{dy_1(t)}{dt} = (a - (s_j\mu\, p_j + (1-p_j)(1-s_j)\mu(1-\mu)\, y_2(t))\; y_1(t) - \lambda\, y_1^2(t), \\ \dfrac{dy_2(t)}{dt} = (d\; y_1(t) - c)\, y_2(t) - \lambda\, y_1^2(t). \end{cases} \qquad (1.12)$$

Здесь $s_j = \dfrac{N_j}{N}$.

1.3. Исследование модели

Будем анализировать динамику атак в РТКС и зависимость интенсивности атак от различных параметров. Для построения графиков функций необходимо решить систему дифференциальных уравнений (1.12). Используем классический метод Рунге – Кутта 4-го порядка,

который описывается системой следующих пяти соотношений:

$$\begin{cases} y_{m+1} = y_m + \dfrac{h}{6}(R_1 + 2R_2 + 2R_3 + R_4), \\ R_1 = f(x_m, y_m), \\ R_2 = f(x_m + \dfrac{h}{2}, y_m + \dfrac{hR_1}{2}), \\ R_3 = f(x_m + \dfrac{h}{2}, y_m + \dfrac{hR_2}{2}), \\ R_4 = f(x_m + \dfrac{h}{2}, y_m + \dfrac{hR_3}{2}). \end{cases} \qquad (1.13)$$

Пример 1. Начальные значения параметров: $Y_1 = 3$; $Y_2 = 1$; $a = 3$, $c = 1{,}8$, $d = 0{,}8$; $\mu = 0{,}095$, $s = 0{,}6$, $p_j = 0{,}1$.

На рис. 1.1 и 1.2 приведены результаты решения системы дифференциальных уравнений. Данная система находится в состоянии равновесия и образует на фазовом пространстве асимптотически устойчивый аттрактор.

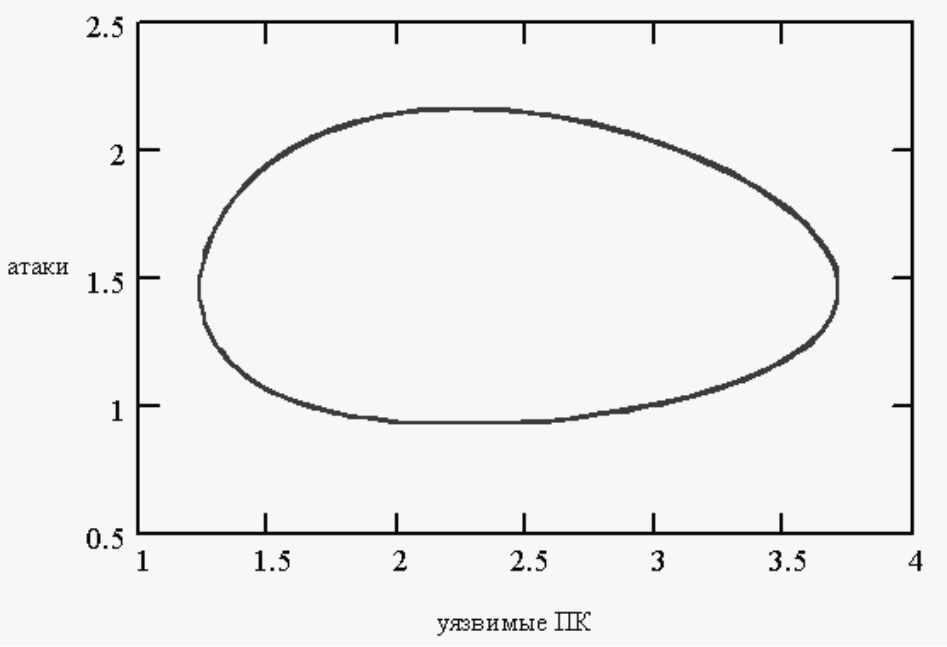


Рис. 1.1. Фазовая траектория (начальное состояние РИВС: $Y_1 = 3$; $Y_2 = 1$; $a = 3$; $c = 1{,}8$; $d = 0{,}8$; $\mu = 0{,}095$; $s = 0{,}6$; $p_j = 0{,}1$)

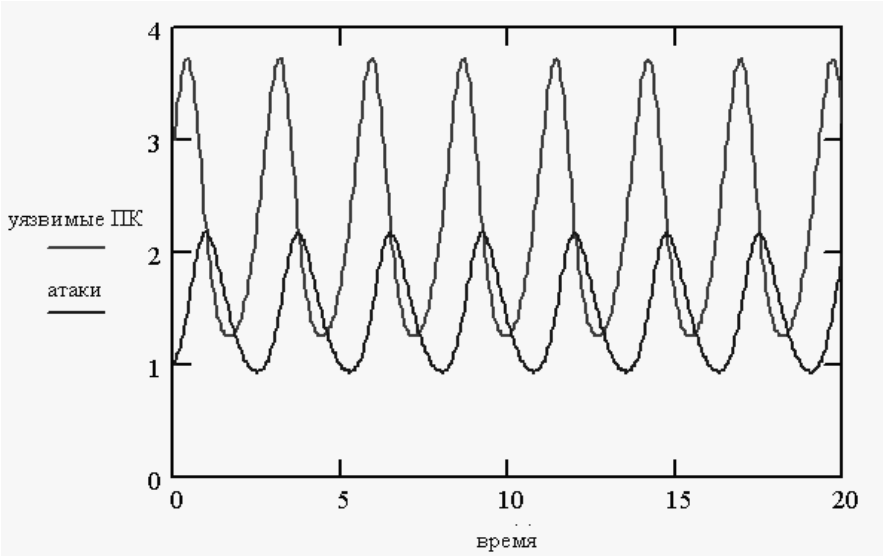


Рис. 1.2. Интегральные кривые решения (начальное состояние РИВС: a = 3; c = 1,8; d = 0,8; μ = 0,095; s = 0,6; p_j = 0,1)

Пример 2. Начальные значения параметров: Y_1 = 3; Y_2 =1; a = 0,03, c = 1,8, d = 0,8; μ = 0,095, s = 0,6, p_j = 0,1.

На рис. 1.3 и 1.4 приведены графические результаты решения системы дифференциальных уравнений. В случае когда скорость восстановления системы после атаки невысока (a < 0), число уязвимых компьютеров начинает уменьшаться вследствие успешных атак. Соответственно начинает снижаться и число атак, но поскольку коэффициент уязвимости мал (d<0), т.е. система имеет защиту перед атаками, то количество атак уменьшается до нуля, и быстрее, чем будут поражены все компьютеры РТКС.

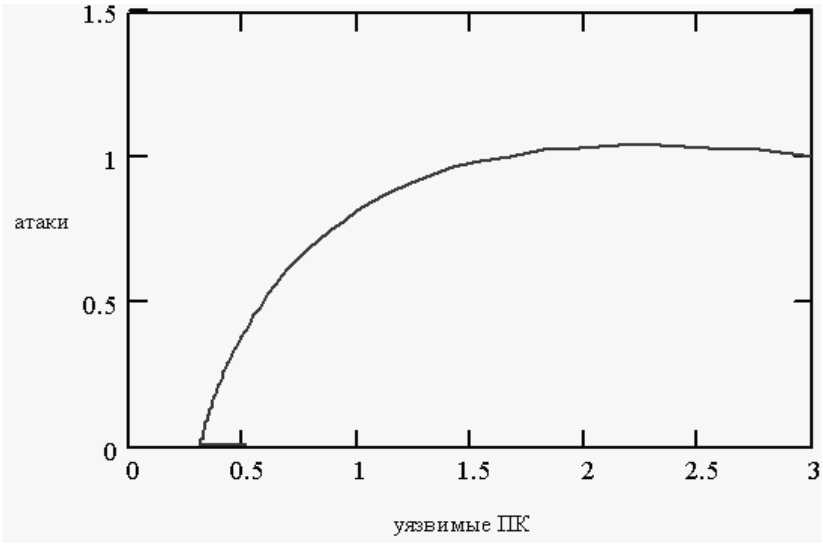


Рис. 1.3. Фазовая траектория (начальное состояние РТКС: a = 0,03; c = 1,8; d = 0,8; μ = 0,095; s = 0,6; p_j = 0,1)

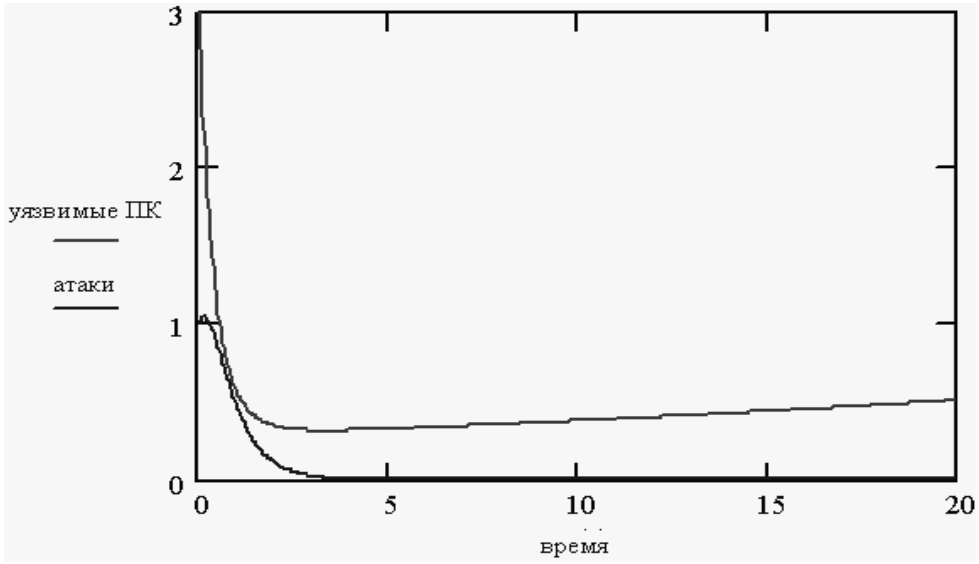


Рис. 1.4. Интегральные кривые решения (начальное состояние РТКС: a = 0,03; c = 1,8; d = 0,8; μ = 0,095; s = 0,6; p_j = 0,1)

Пример 3. Начальные значения параметров: Y_1 = 3; Y_2 = 1; a = 0,03, c = 1,8, d = 5; μ = 0,095, s = 0,6, p_j = 0,1. На рис. 1.5 и 1.6 приведены графические результаты. В случае когда коэффициент уязвимости высок (d>0), т.е. система фактически не имеет никакой защиты перед атаками, число уязвимых компьютеров в сети уменьшается гораздо быстрее числа атак (очень быстро наступает полный захват системы).

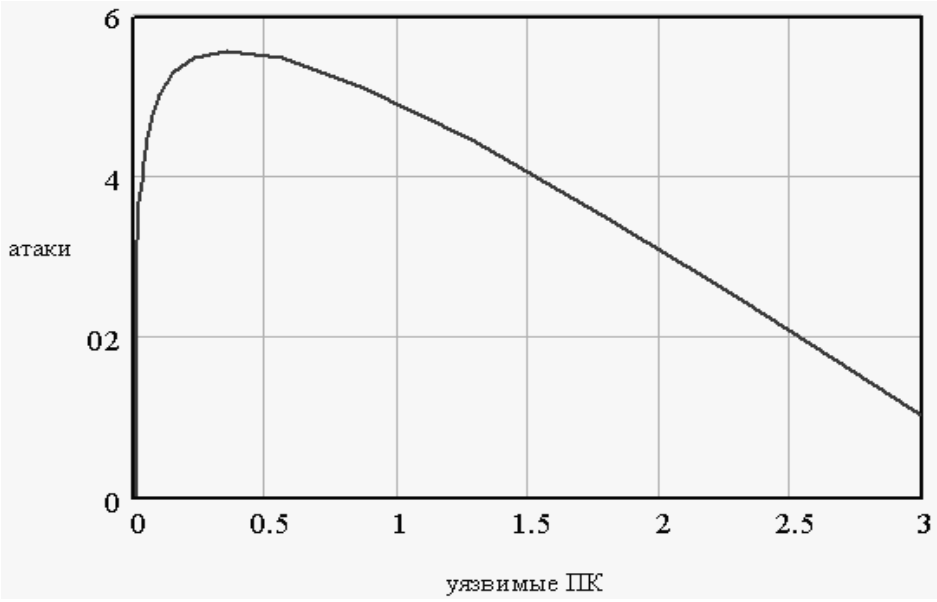


Рис. 1.5. Фазовая траектория (начальное состояние РТКС: a = 0,03; c = 1,8; d = 5; μ = 0,095; s = 0,6; p_j = 0,1)

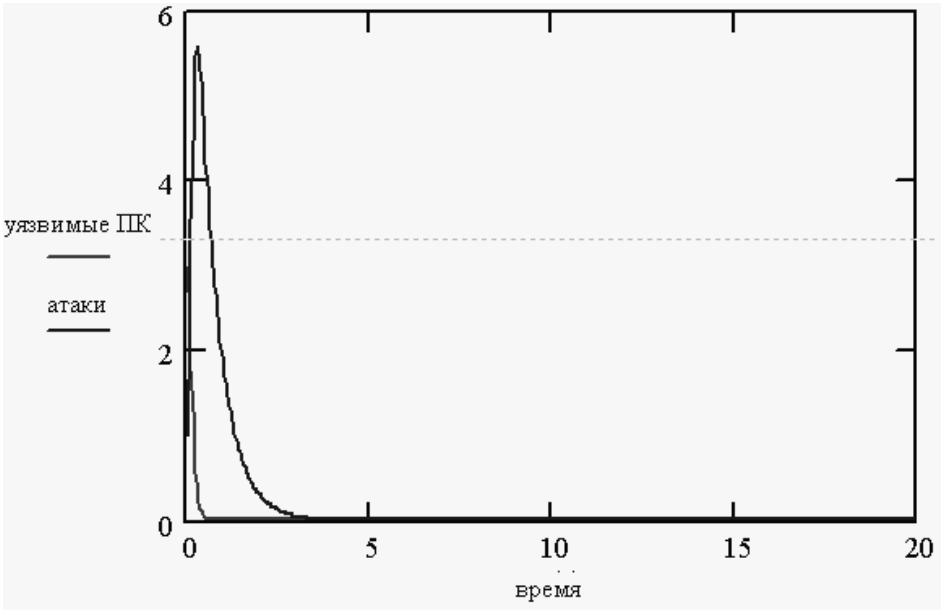


Рис. 1.6. Интегральные кривые решения (состояние РТКС: a = 0,03; c = 1,8; d = 5; μ = 0,095; s = 0,6; p_j = 0,1)

Пример 4. Начальные значения параметров: Y_1 = 3; Y_2 =1; a = 3, c = 1,8, d = 0,8; μ = 0,095, s = 0,6, p_j = 0,1. На рис. 1.7 и 1.8 приведены графические результаты решения системы дифференциальных уравнений. В случае когда вероятность успешной атаки высока ($a \rightarrow 1$), т.е. скорость захвата компьютеров будет достаточно высокой, ситуация будет аналогичной случаю с высоким коэффициентом уязвимости.

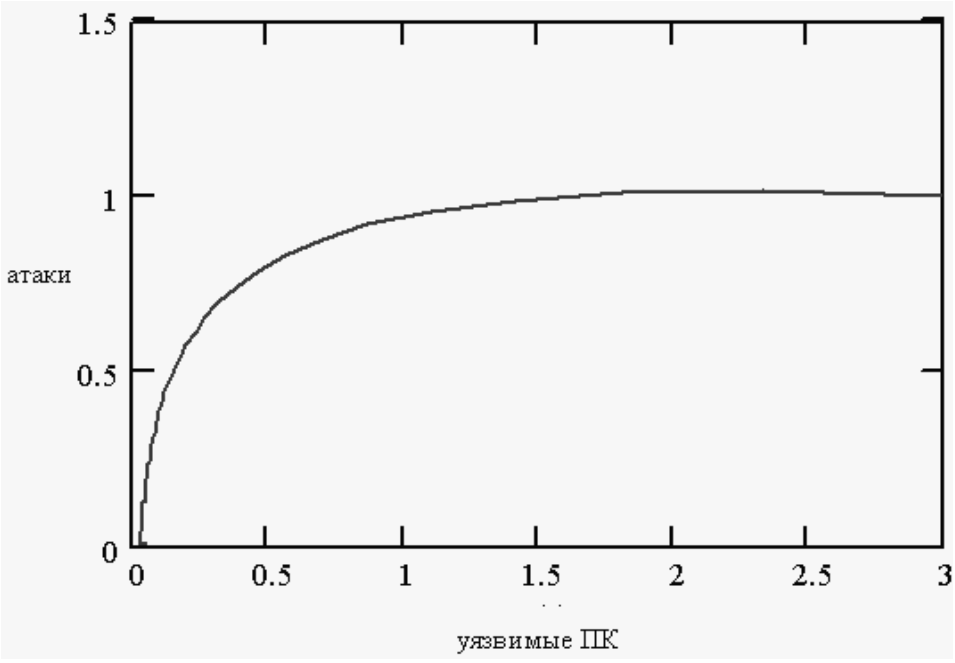


Рис. 1.7. Фазовая траектория (начальное состояние РТКС: a = 3, c = 1,8; d = 0,8; μ = 0,095; s = 0,6; p_j = 0,1)

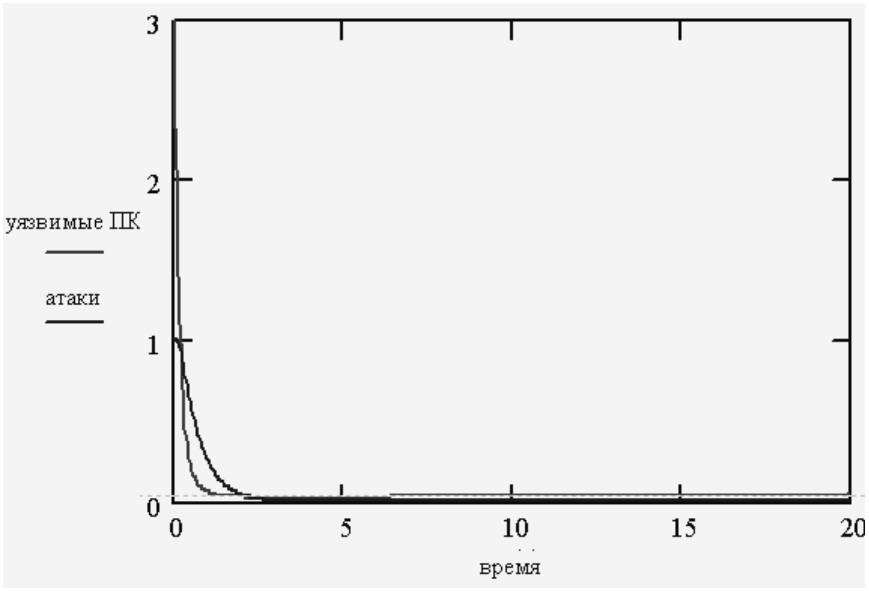


Рис. 1.8. Интегральные кривые решения (состояние РТКС:
$a = 3$; $c = 1{,}8$; $d = 0{,}8$; $\mu = 0{,}095$; $s = 0{,}6$; $p_j = 0{,}1$)

Пример 5. Начальные значения параметров: $Y_1 = 3$; $Y_2 = 1$; $a = 3$, $c = 0{,}018$, $d = 0{,}8$; $\mu = 0{,}095$, $s = 0{,}6$, $p_j = 0{,}1$. На рис. 1.9 и 1.10 приведены графические результаты. В случае когда коэффициент, выражающий скорость уменьшения числа атак, слишком мал ($c < 0$), т.е. система информационной защиты никак не может воспрепятствовать атакам и замедлить их рост, с течением времени все компьютеры в системе будут захвачены.

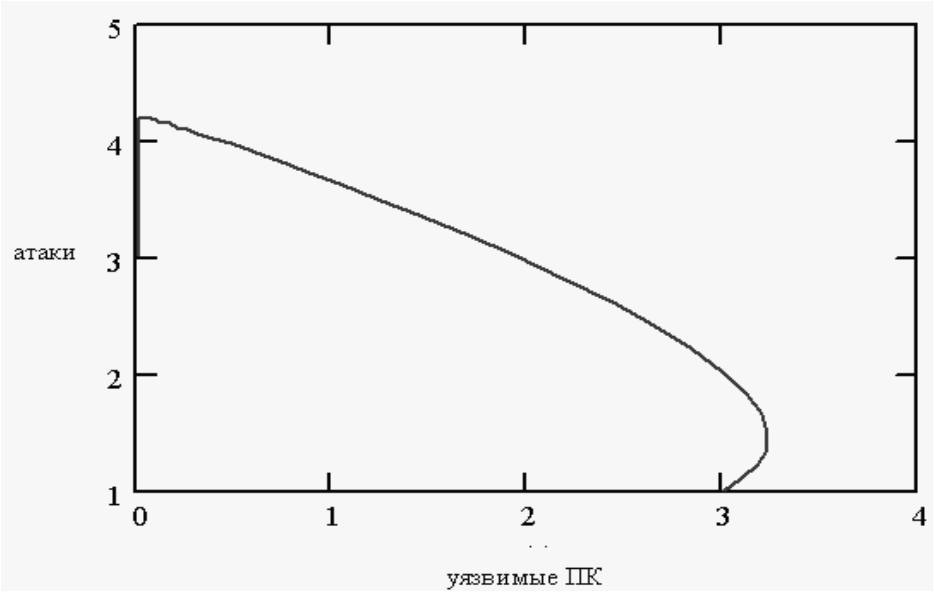


Рис. 1.9. Фазовая траектория (начальное состояние РТКС:
$a = 3$; $c = 0{,}018$; $d = 0{,}8$; $\mu = 0{,}095$; $s = 0{,}6$; $p_j = 0{,}1$)

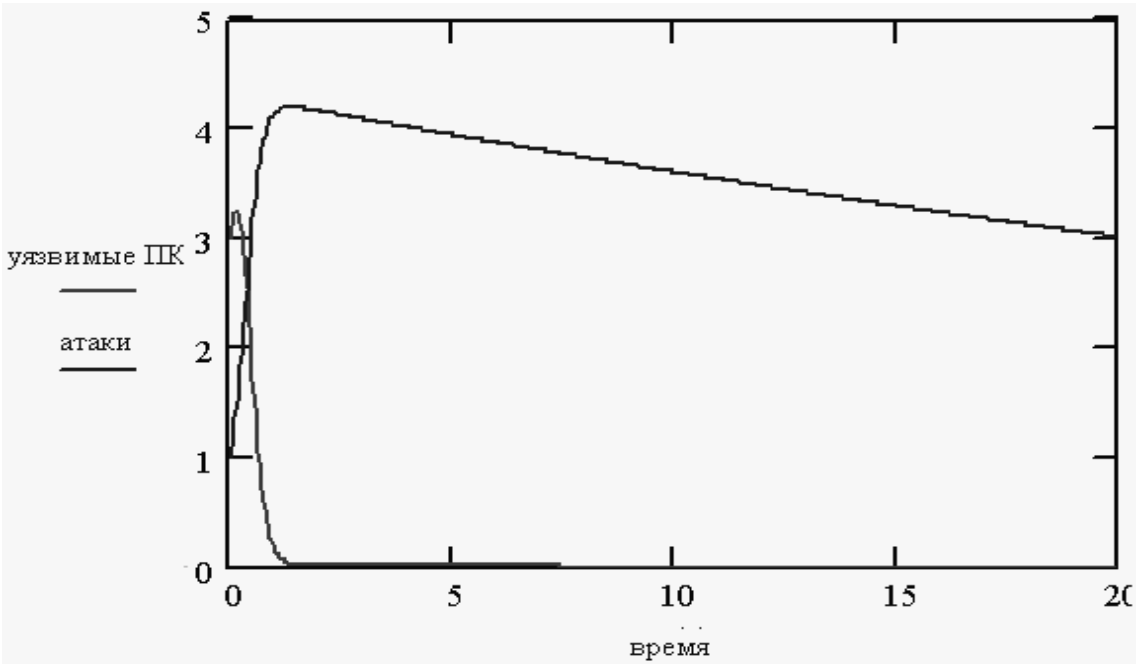


Рис. 1.10. Интегральные кривые решения (начальное состояние РТКС: a = 3, c = 0,018; d = 0,8; μ = 0,095; s = 0,6; p_j = 0,1)

Пример 6. Начальные значения параметров: Y_1 = 3; Y_2 =1; a = 3, c = 0,018, d = 0,008; μ = 0,095, s = 0,6, p_j = 0,1. На рис. 1.11 и 1.12 приведены графические результаты.

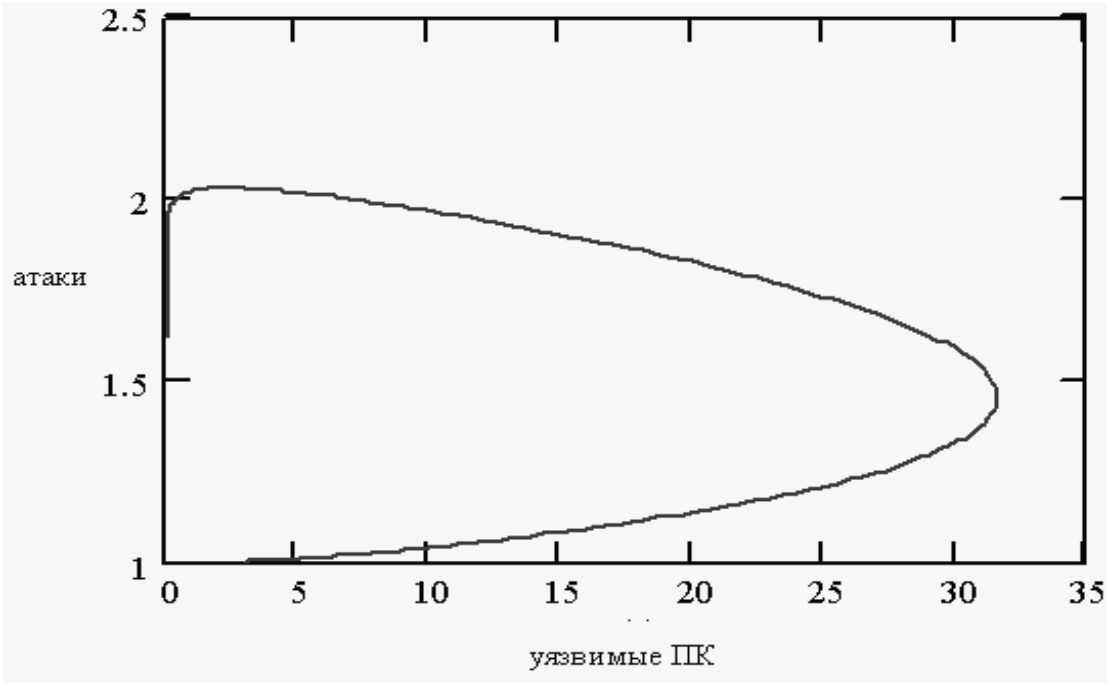


Рис. 1.11. Фазовая траектория (начальное состояние РТКС: a = 3; c = 0,018; d = 0,008; μ = 0,095; s = 0,6; p_j = 0,1)

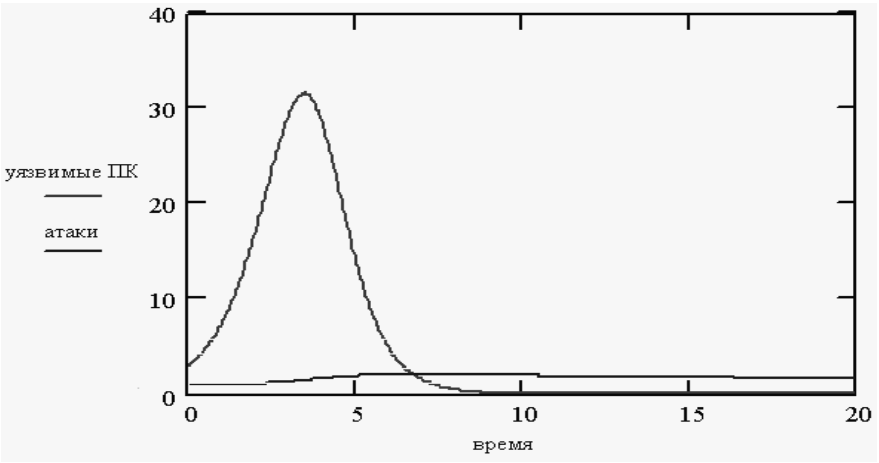


Рис. 1.12. Интегральные кривые решения (начальное состояние РТКС: a = 3; c = 0,018; d = 0,008; μ = 0,095; s = 0,6; p_j = 0,1)

В аналогичном случае с очень низким коэффициентом уязвимости перед атаками ($d \to 0$) система сначала развивается стабильно, но постепенно, со временем атаки адаптируясь к системе, вредоносные программы быстро поражают все компьютеры РТКС. Колебания числа зараженных компьютеров и числа атак на самом деле наблюдаются не всегда. Нередко наблюдается стабильное количество и тех и других, хотя процесс захвата компьютеров идет постоянно. Такой случай требует введения некоторой поправки – коэффициента осцилляции λ.

Пример 7. Начальные значения параметров: Y_1 = 3; Y_2 =1; a = 3, c = 1,8, d = 0,8; μ = 0,095, s = 0,6, p_j = 0,1; λ = 0,08.

На рис. 1.13 и 1.14 приведены графические результаты.

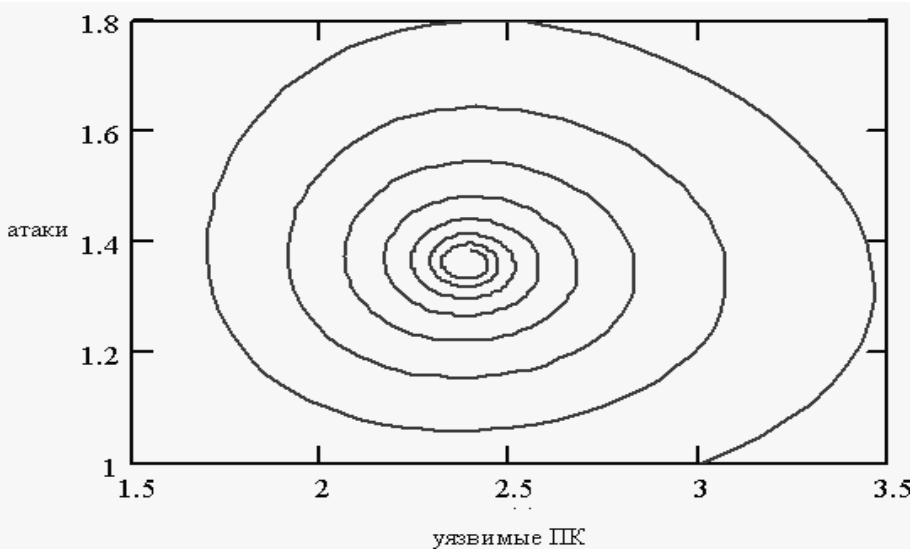


Рис. 1.13. Фазовая траектория (начальное состояние РИВС: Y_1 = 3; Y_2 =1; a = 3; c = 1,8; d = 0,8; μ = 0,095; s = 0,6; p_j = 0,1; λ = 0,08)

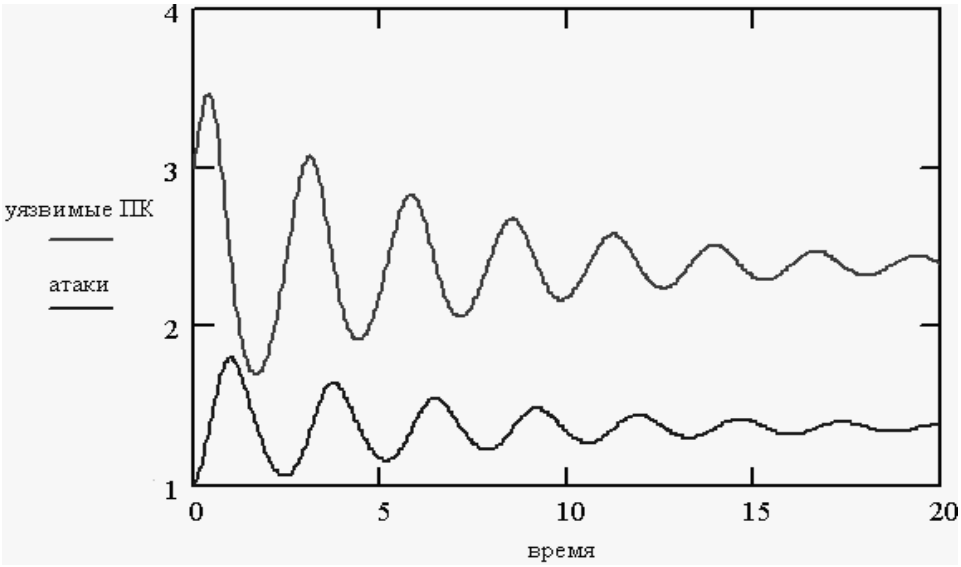


Рис. 1.14. Интегральные кривые решения (начальное состояние РТКС: $Y_1 = 3$; $Y_2 = 1$; $a = 3$; $c = 1{,}8$; $d = 0{,}8$; $\mu = 0{,}095$; $s = 0{,}6$; $p_j = 0{,}1$; $\lambda = 0{,}08$)

На графиках видно, как численности уязвимых компьютеров и атак приближаются со временем к равновесным значениям. Фазовый портрет системы имеет аттрактор, являющийся точкой (так называемый фазовый фокус). В то же время интегральные кривые числа атак и уязвимых компьютеров принимают форму затухающих колебаний.

Пример 8. Начальные значения параметров: $Y_1 = 3$; $Y_2 = 1$; $a = 3$, $c = 1{,}8$, $d = 0{,}8$; $\mu = 0{,}095$, $s = 0{,}6$, $p_j = 0{,}1$; $\lambda = 0{,}08$.

На рис. 1.15 и 1.16 приведены графические результаты.

В случае когда коэффициент уязвимости слишком низок ($d \to 0$), т.е. система невосприимчива к атакам, равновесное состояние в системе наступает очень быстро.

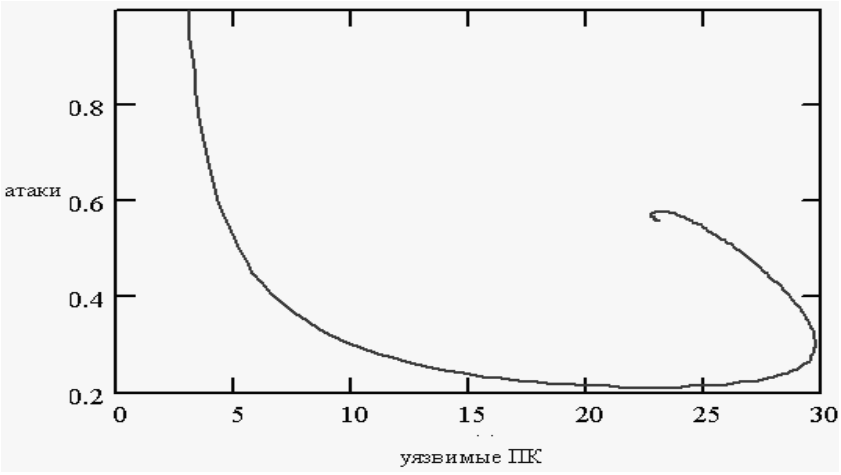


Рис. 1.15. Фазовая траектория (начальное состояние РТКС: $a = 3$; $c = 1{,}8$; $d = 0{,}8$; $\mu = 0{,}095$; $s = 0{,}6$; $p_j = 0{,}1$; $\lambda = 0{,}08$)

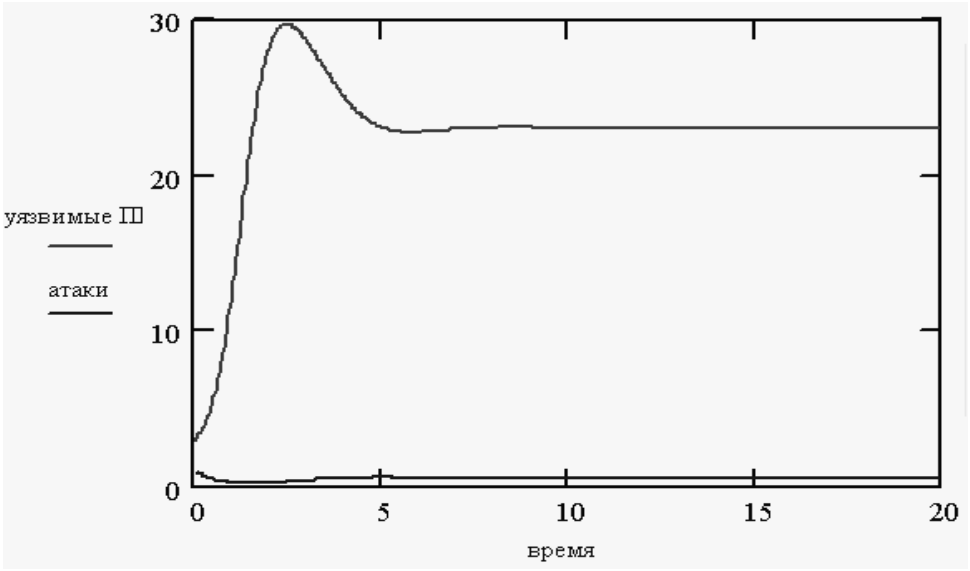


Рис.1.16. Интегральные кривые решения (начальное состояние РТКС: $Y_1 = 3$; $Y_2 = 1$; $a = 3$; $c = 1{,}8$; $d = 0{,}8$; $\mu = 0{,}095$; $s = 0{,}6$; $p_j = 0{,}1$; $\lambda = 0{,}08$)

Пример 9. Начальные значения параметров: $Y_1 = 3$; $Y_2 = 1$; $a = 3$, $c = 1{,}8$, $d = 0{,}8$; $\mu = 0{,}095$, $s = 0{,}6$, $p_j = 0{,}1$; $\lambda = 0{,}08$. На рис. 1.17 и 1.18 приведены графические результаты решения системы дифференциальных уравнений. Аналогичная ситуация наблюдается в случае с низкой вероятностью успеха атаки. Поскольку скорость захвата компьютеров так же низка, равновесное состояние наступает быстро.

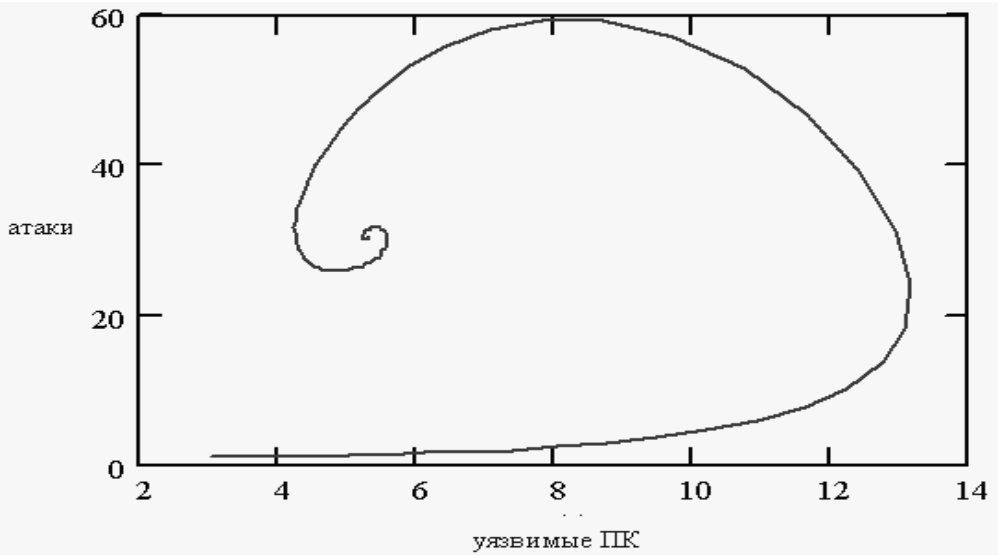


Рис. 1.17. Фазовая траектория (начальное состояние РТКС: $Y_1 = 3$; $Y_2 = 1$; $a = 3$; $c = 1{,}8$; $d = 0{,}8$; $\mu = 0{,}095$; $s = 0{,}6$; $p_j = 0{,}1$; $\lambda = 0{,}08$)

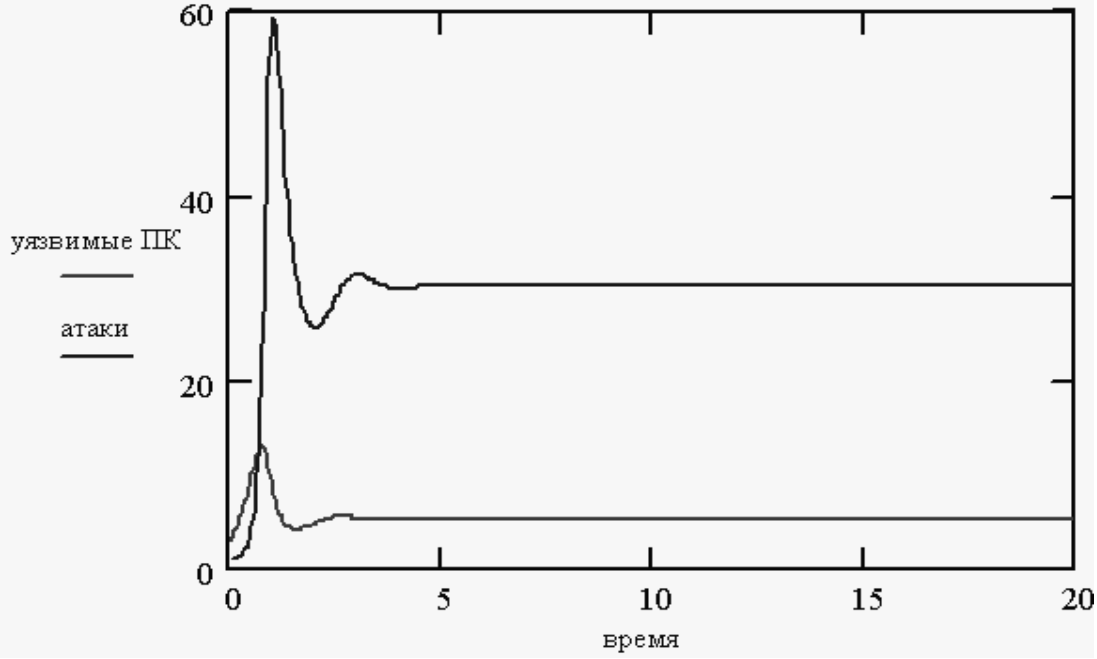


Рис. 1.18. Интегральные кривые решения (начальное состояние РТКС: $Y_1 = 3$; $Y_2 = 1$; $a = 3$; $c = 1{,}8$; $d = 0{,}8$; $\mu = 0{,}095$; $s = 0{,}6$; $p_j = 0{,}1$; $\lambda = 0{,}08$)

1.4. Модель с многоуровневой системой информационной защиты

Доработаем созданную модель. Для этого будем считать, что система информационной защиты РТКС имеет несколько уровней защиты, каждый из которых срабатывает в случае, если число атак (пораженных компьютеров) достигает критического уровня. При переходе на новый уровень система информационной защиты повышает свои характеристики, т.е. осуществляется прирост коэффициентов *a, c* и *d* на некоторую величину. Данный прирост обозначим как Δa, Δc и Δd соответственно.

Пример 10. Начальные значения параметров: $Y_1 = 3$; $Y_2 = 1$; $a = 3$, $c = 1{,}8$, $d = 0{,}8$; $\mu = 0{,}095$, $s = 0{,}6$, $p_j = 0{,}1$; $\lambda = 0{,}08$. На рис. 1.19 показан фазовый портрет системы без учета многоуровневой системы информационной защиты. Введем новые параметры: $\Delta c = 1$, $\Delta a = 0{,}5$, $\Delta d = 0$; количество уровней безопасности 4; интервал между ними 1; начало первого уровня 2.

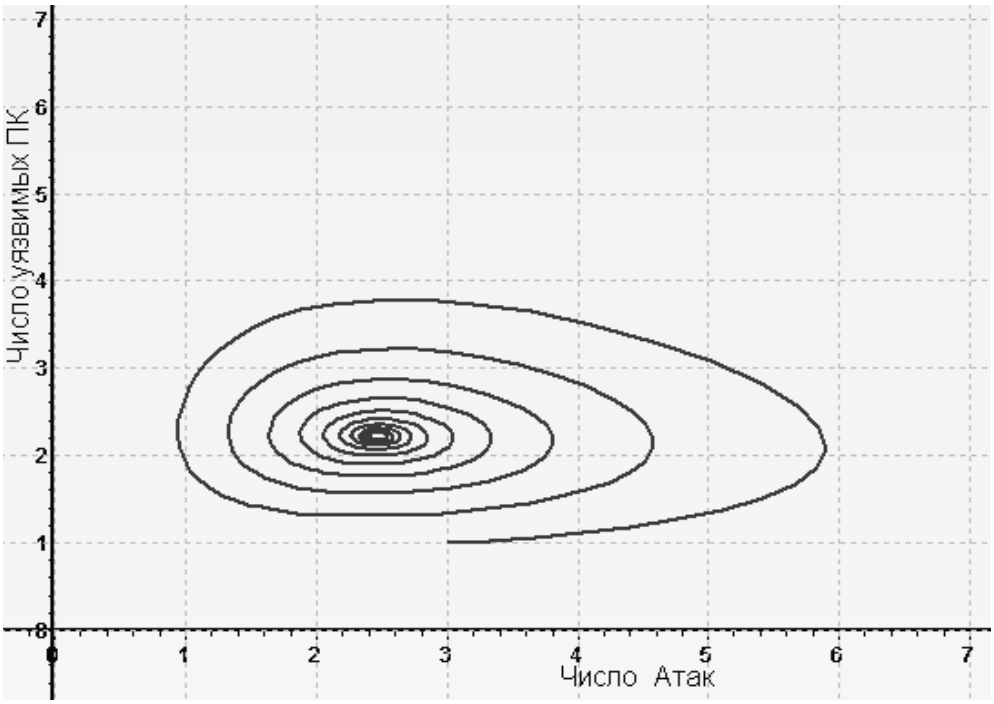


Рис. 1.19. Фазовая траектория (РТКС без учета многоуровневой системы информационной защиты $Y_1 = 3$; $Y_2 = 1$; $a = 3$; $c = 1{,}8$; $d = 0{,}8$; $\mu = 0{,}095$; $s = 0{,}6$; $p_j = 0{,}1$; $\lambda = 0{,}08$)

В результате серии тестов была выявлена закономерность: независимо от поведения фазовой траектории, график системы с некоторой вероятностью (вероятность тем выше, чем меньше скорость срабатывания системы информационной защиты) стремится к единственному аттрактору, находящемуся в одной и той же точке. Следовательно, можно предсказать конечный результат поведения системы, зная лишь начальные данные.

Пример 11. Начальные значения параметров: $Y_1 = 3$; $Y_2 = 1$; $a = 5$; $c = 1{,}8$; $d = 0{,}8$; $\mu = 0{,}9$; $s = 0{,}6$; $p_j = 0{,}1$; $\lambda = 0{,}08$; $\Delta c = 10$; $\Delta a = 0{,}5$; $\Delta d = 0$; количество уровней безопасности 4, интервал между уровнями 1, начало первого уровня 2.

Если же прирост скорости уменьшения числа атак при переходе на новый уровень безопасности выше в несколько раз, то происходит резкая редукция фазовой траектории и число атак постепенно стремится к нулю (рис. 1.20).

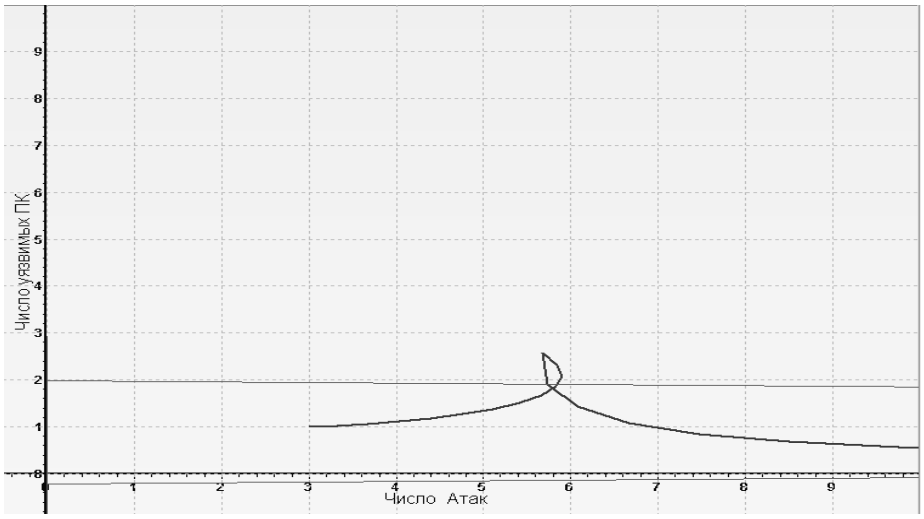


Рис. 1.20. Фазовая траектория (состояние РТКС: a = 5; c = 1,8; d = 0,8; μ = 0,9; s = 0,6; p_j = 0,1; λ = 0,08; Δc = 10; Δa = 0,5; Δd = 0; уровней безопасности 4; интервал 1; начало первого уровня 2)

Пример 12. Начальные значения параметров: Y_1 = 3; Y_2 =1; a = 5; c = 1,8; d = 0,8; μ = 0,9; s = 0,6; p_j = 0,1; λ = 0,08; Δc = 0; Δa = 0; Δd = 0,5; количество уровней безопасности 4, интервал между уровнями 1, начало первого уровня 2.

В случае перехода на новый уровень безопасности, понижения коэффициента уязвимости (вследствие ужесточения политики безопасности) на графике фазовой траектории происходит резкий обрыв и постепенное уменьшение числа атак (рис. 1.21). Причем чем больше снижение коэффициента уязвимости, тем более крутым становится график (иными словами, снижение уровня атак происходит гораздо быстрее).

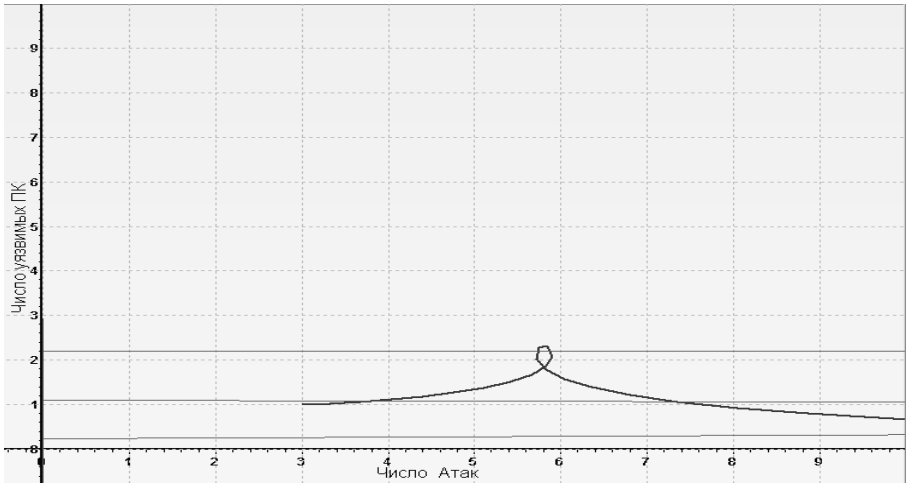


Рис. 1.21. Фазовая траектория (Y_1 = 3; Y_2 =1; a = 5; c = 1,8; d = 0,8; μ = 0,9; s = 0,6; p_j = 0,1; λ = 0,08; Δc = 0; Δa = 0; Δd = 0,5; количество уровней безопасности 4; интервал между уровнями 1; начало первого уровня 2)

Однако если коэффициент слишком мал ($\Delta d \to 0$), то редукция может не произойти, и система устремится к равновесному состоянию, т.е. на фазовом пространстве появится аттрактор в одной точке (рис. 1.22).

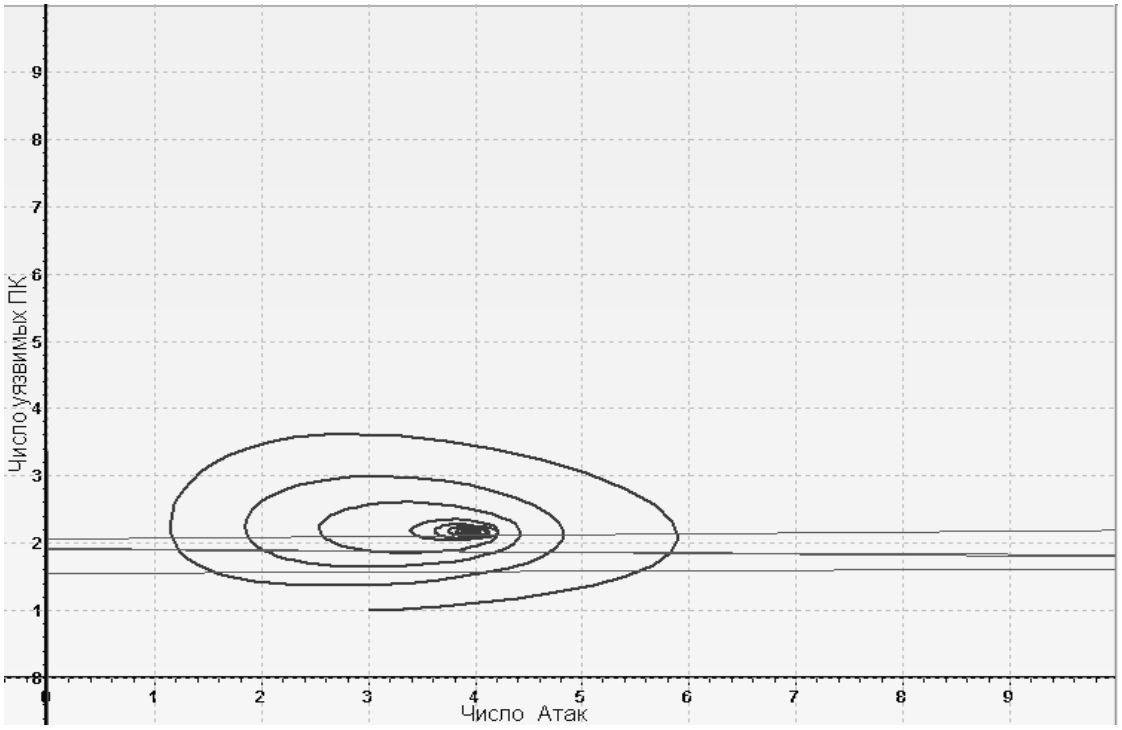


Рис. 1.22. Фазовая траектория ($Y_1 = 3$; $Y_2 = 1$; $a = 5$; $c = 1{,}8$; $d = 0{,}8$; $\mu = 0{,}9$; $s = 0{,}6$; $p_j = 0{,}1$; $\lambda = 0{,}08$; $\Delta c = 0$; $\Delta a = 0$; $\Delta d \to 0$; количество уровней безопасности 4; интервал 1; начало первого уровня 2)

Выводы

На основе биологических моделей, идеально подходящих для моделирования поведения динамических систем, разработаны модели атаки захвата ресурса распределенной информационно-вычислительной системы и ее функционирования под действием атаки.

Формализация предложенных моделей позволяет систематизировать подход к определению необходимости и достаточности мер защиты РТКС от внешних угроз.

Экспериментальное исследование показало возможность предсказания с определенной степенью точности конечного состояния РТКС при известных начальных параметрах системы и атаки.

Глава 2

Модели и алгоритмы достоверного обнаружения вредоносных программ в распределенной телекоммуникационной системе

√ Постановка задачи обнаружения вредоносной программы в РТКС

√ Модели построения решающих правил обнаружения вредоносной программы

√ Алгоритмы обнаружения ВП

Рассмотрены модели построения решающих правил обнаружения вредоносных программ в распределенной телекоммуникационной системе. Предложен алгоритм обнаружения вредоносных программ, основанный на понятии критической области угроз, реализация которого позволяет улучшить временные и вероятностные характеристики колец защиты. Приводятся результаты экспериментального исследования вероятностных характеристик антивирусных программ, по результатам которого построена критическая область угроз

Введение

Противодействие атакам вредоносных программ предполагает комплекс разнообразных мер и использование разнообразных средств защиты. Цели принимаемых мер – это снижение вероятности тотального инфицирования распределенной телекоммуникационной системы, уменьшение последствий таких воздействий [25, 27, 31].

Под оптимальной защитой в данной связи будем понимать такую совокупность методов и средств защиты для заданного числа объектов, которая обеспечивает минимальное время обнаружения атакующей программы при одновременно максимальном уменьшении последствий от ее действия.

При разработке системы защиты обычно необходимо выбрать такую совокупность методов и средств, которая обеспечивает:

– или минимальную вероятность вредоносного воздействия при ограничении на стоимостные, временные и другие показатели;

– или минимальные суммарные потери от взлома защиты и затрат на разработку и эксплуатацию системы защиты;

– или минимальные затраты на разработку и эксплуатацию системы защиты при ограничениях на вероятность взлома защиты.

Цель данной работы – проанализировать возможности оперативного построения адекватных защитных механизмов, разработать комплекс моделей и алгоритмов достоверного обнаружения вредоносных программ (ВП) в РТКС за ограниченное время.

2.1. Постановка задачи обнаружения вредоносной программы в РТКС

Рассмотрим формальную постановку задачи построения системы защиты РТКС, обеспечивающей максимальную вероятность обнаружения вредоносных программ [45] за ограниченное время. Введем необходимые обозначения.

Пусть система имеет множество объектов информационной защиты $O = \{o_1, o_2, ..., o_S\}$ и N множество модулей защиты (МЗ). Модуль защиты включает в состав средство обнаружения (СрО) и средство противодействия (СП) ВП.

Пусть $p_j(o)$ – вероятность обнаружения ВП для j-го СрО, за-

крепленного за объектом РИВС; $T^{\text{ОБ}}$ – время обнаружения ВП системой защиты; $c_j^{П}(o)$, $c_j^{Э}(o)$ – затраты на разработку и эксплуатацию j-го МЗ для объекта РТКС; $\tau_j^{П}(o)$, $\tau_j^{Э}(o)$ – временные затраты на разработку и эксплуатацию соответствующего МЗ; $d_j(o)$ – потери в системе, вызванные неадекватной работой рассматриваемого МЗ. Тогда задача имеет вид

$$\begin{cases} \prod\limits_{o\in O}\sum\limits_{j=1}^{N} p_j(o)x_j(o) \to \max;\ T^{\text{ОБ}} \le T^{Д} \\ \sum\limits_{o\in O}\sum\limits_{j=1}^{N} c_j^{П}(o)x_j(o) \le C^{П}; \quad \sum\limits_{o\in O}\sum\limits_{j=1}^{N} c_j^{Э}(o)x_j(o) \le C^{Э} \\ \sum\limits_{o\in O}\sum\limits_{j=1}^{N} \tau_j^{П}(o)x_j(o) \le T^{П}; \quad \sum\limits_{o\in O}\sum\limits_{j=1}^{N} \tau_j^{Э}(o)x_j(o) \le T^{Э} \\ \sum\limits_{o\in O}\sum\limits_{j=1}^{N} d_j(o)x_j(o) \le D; \quad \sum\limits_{j=1}^{N} x_j(o) = 1,\ o \in O, \end{cases} \tag{2.1}$$

где $T^{Д}$ – допустимые временные затраты на обнаружения ВП системой защиты; $C^{П}$ – выделяемые ресурсы на разработку системы защиты; $C^{Э}$ – выделяемые ресурсы на эксплуатацию системы защиты; $T^{П}$ – допустимые временные затраты на разработку системы защиты; $T^{Э}$ – допустимые временные затраты на эксплуатацию системы защиты; D – допустимые суммарные потери от взлома системы защиты;

$$x_j(o) = \begin{cases} 1, \text{ если } \text{j–й МЗ закреплен за объектом Р РИ}, \\ 0 \text{ в противном случае.} \end{cases}$$

Аналогичные задачи решались в работах [37, 41, 44, 57, 79]. Рассмотренная задача сводится к задаче линейного программирования, но данная формальная постановка не учитывает тот факт, что на каждом объекте системы o_i $\left(i = \overline{1, S}\right)$ может функционировать несколько МЗ, и то, что каждое СрО, входящее в состав МЗ, характеризуется не только вероятностью обнаружения ВП p_j $\left(j = \overline{1, N}\right)$, но и вероятностью возникновения «ложной тревоги» $\overline{p_j}$ $\left(j = \overline{1, N}\right)$.

Наиболее существенным условием в задаче (2.1) является ограничение на время обнаружения ВП, так как только раннее обнаружение ВП позволит минимизировать ущерб РТКС.

Учитывая данные обстоятельства, получим новую формулировку задачи (2.1):

$$\begin{cases} \prod_{o\in O}\prod_{j=1}^{N} p_j^{z}(o) \to \max, \quad \prod_{o\in O}\prod_{j=1}^{N} \overline{p_j}^{z}(o) \to \min; \\ T^{\text{ОБ}} \le T^{Д}. \end{cases} \tag{2.2}$$

где степень

$$z = \begin{cases} 1, \text{ если j}-\text{й МЗ закреплен за объектом РИВС}, \\ 0 \text{ в противном случае}. \end{cases}$$

В дальнейшем будем рассматривать задачу (2.2) в качестве концептуальной в данной работе.

2.2. Модели построения решающих правил обнаружения вредоносных программ

Модель I. Один модуль защиты

Рассмотрим простейшую модель организации защитных механизмов от ВП одного объекта РТКС (рис. 2.1). Модель включает два основных элемента – объект защиты (ОЗ) и модуль защиты. Объектом защиты может быть любой информационный ресурс или какой-либо информационный процесс РТКС. Модуль защиты включает в состав средство обнаружения (СрО) и средство противодействия (СП) ВП. Решающий модуль (РМ) по сигналам от СрО вырабатывает управляющее воздействие для СП модуля защиты.

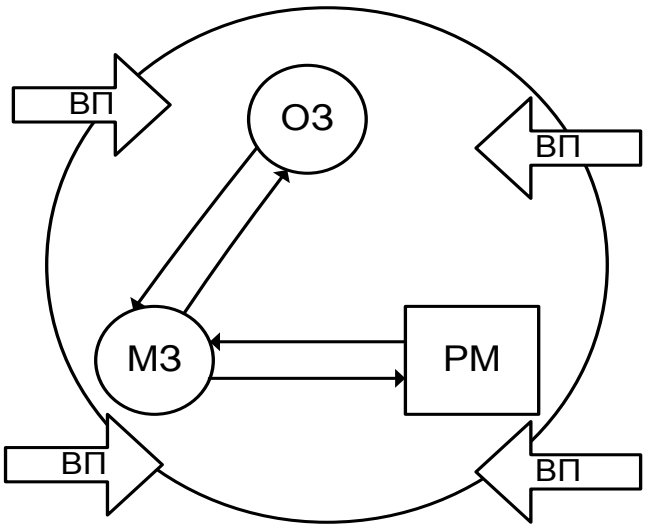


Рис. 2.1. Модель организации защитных механизмов в РТКС с одним модулем защиты

В модуле каждое СрО предназначено для обнаружения конкретных видов ВП, характеризуется вероятностью выработки сигнала о наличии вредоносной программы p, вероятностью «ложной тревоги» $\bar{p}$ и временем генерации сигнала тревоги $T^{ОБ}$. Целью модели является выработка решающего правила формирования сигнала о наличии и отсутствии ВП в системе.

Будем полагать, что на выходе МЗ формируется бинарный сигнал u, принимающий либо 1 (ВП обнаружена на ОЗ), либо 0 (ВП не обнаружена). Сигнал u характеризуется плотностями распределения вероятностей его появления – $f_y(u)$ (ВП есть) и $f_n(u)$ (ВП нет).

$$f_y(u) = \begin{cases} p & при \ \ u = 1, \\ 1 - p & при \ \ u = 0, \end{cases} \tag{2.3}$$

где p – вероятность обнаружения ВП.

$$f_n(u) = \begin{cases} \bar{p} & при \ \ u = 1, \\ 1 - \bar{p} & при \ \ u = 0, \end{cases} \tag{2.4}$$

где $\bar{p}$ – вероятность возникновения «ложной тревоги».

По критерию Неймана – Пирсона [93] решающее привило может быть записано в виде

$$lg \frac{f_y(u)}{f_n(u)} > c, \tag{2. 5}$$

где c – постоянная, определяемая необходимой (минимально достаточной) вероятностью защиты (пороговое значение).

При выполнении (2.5) принимается решение о наличии ВП в системе и, если возможно, проводятся меры по ее уничтожению. Время $T^{ОБ}$ в общем плане зависит от характеристик СрО, условий его эксплуатации и внешних факторов.

Достоинство данной модели – простота алгоритма работы РМ. Недостатком является то, что один МЗ не может обеспечить надежную (эффективную) защиту от многих вредоносных программ. Это связано с тем, что, как правило, МЗ предназначен для решения задачи противодействия только определенному множеству вредоносных программ.

Для ликвидации указанного недостатка модели можно произвести:

1. Дублирование МЗ.

2. Добавление МЗ с разными принципами действия и областями контроля.

Модель II. Кольцо защиты

Пусть «вокруг» объекта защиты расположены N модулей защиты. По их бинарным сигналам принимается общее решение о наличии или отсутствии ВП (рис. 2.2).

Кольцом защиты (КЗ) будем называть совокупность модулей защиты $(m_1, m_2, ..., m_N)$, количество и состав которых зависят от характеристик объекта защиты. Для эффективной работы системы кольцо защиты с течением времени должно претерпевать модернизацию в связи с изменением характеристик самих объектов РТКС.

В процессе формирования колец защиты должны выполняться следующие условия:

1. Возможность совместной работы объединяемых средств обнаружения.

2. Время работы кольца защиты по обнаружению и противодействию ВП не выше требуемого.

3. Обеспечение заданной вероятности обнаружения вредоносных программ за счет использования нескольких СрО, построенных на различных принципах, имеющих общую зону обнаружения и совпадающие характеристики объекта обнаружения.

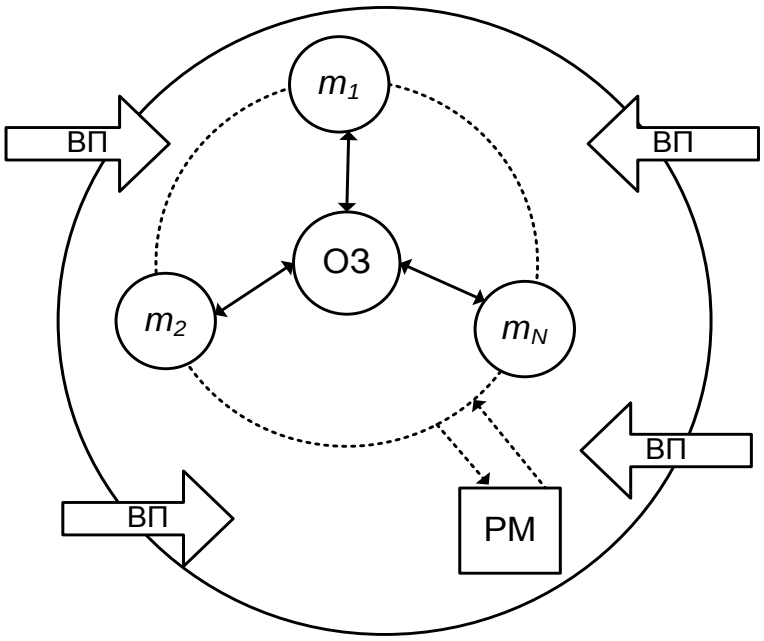


Рис. 2.2. Модель организации защитных механизмов в РТКС с кольцом защиты

4. Снижение средней частоты «ложных тревог», вызываемых различными помехами.

Кроме этого необходима выработка метода объединения сигналов от нескольких средств обнаружения, образующих кольцо защиты, для принятия решения о наличии вредоносной программы в системе.

Пусть на выходе каждого МЗ формируется бинарный сигнал u_j $(j = 1, 2, ..., N)$, принимающий с определенной вероятностью либо 1 (ВП обнаружена), либо 0 (ВП не обнаружена).

Введем обозначения для характеристик j-го МЗ $(j = \overline{1, N})$: p_j – вероятность обнаружения ВП; $\overline{p_j}$ – вероятность возникновения «ложной тревоги», $T_j^{об}$ – время, необходимое механизмам обнаружения МЗ для генерации сигнала тревоги.

Алгоритм обнаружения вредоносной программы по схеме «И»

Шаг 1. Запуск средств обнаружения кольца защиты.

Шаг 2. Снятие показаний, генерируемых МЗ $u_1, u_2, ..., u_N$.

Шаг 3. Если каждый из МЗ сгенерировал бинарный сигнал 1 ($u_1 = u_2 = ... = u_N = 1$), то принимается решение о наличии ВП в системе и производится инициирование СП. В противном случае – переход на шаг 2. Конец алгоритма.

Вероятность обнаружения ВП кольцом защиты

$$p_И = \prod_{j=1}^{N} p_j .$$

Вероятность «ложной тревоги» кольца защиты

$$\overline{p_И} = \prod_{j=1}^{N} \overline{p_j} .$$

Время обнаружения ВП кольцом защиты

$$T_И^{об} = \max_{j \in \overline{1, N}} T_j .$$

Достоинством алгоритма является оптимизация целевой функции задачи обнаружения вредоносных программ в постановке (2.2), т.е. достигнута минимальная вероятность возникновения «ложной тревоги»: $\overline{p_И} \to \min$ (ВП обнаружена каждым МЗ).

Недостатки схемы «И»:

1. Алгоритм обнаружения ВП обеспечивает предельно низкую вероятность «ложной тревоги», но и невысокую вероятность обнаружения.

2. Решение задачи (2.2) возможно только в том случае, если все модули защиты обеспечивают одинаковые вероятности обнаружения, а вероятности «ложных тревог» не хуже заданных.

3. Для выполнения условия $T^{ОБ} \le T^{Д}$ необходимо, чтобы время обнаружения ВП каждого модуля защиты было меньше допустимого времени, так как $T_{И}^{ОБ} = \max\limits_{j \in \overline{1,N}} T_j$.

Рассмотренный алгоритм предъявляет высокие требования к модулям защиты.

Алгоритм обнаружения вредоносной программы по схеме «ИЛИ»

Шаг 1. Запуск средств обнаружения кольца защиты.

Шаг 2. Снятие показаний, генерируемых МЗ $u_1, u_2, ..., u_N$.

Шаг 3. Если хотя бы один из МЗ сгенерировал бинарный сигнал 1 ($u_1 = 1$ или $u_2 = 1$ ... или $u_N = 1$), то принимается решение о наличии ВП в системе и производится инициирование СП. В противном случае – переход на шаг 2. Конец алгоритма.

Найдем аналитические зависимости вероятностных характеристик кольца защиты, содержащего несколько МЗ. Рассматривается кольцо защиты из трех МЗ. Для каждого МЗ известны вероятности обнаружения p_1, p_2, p_3 и вероятности «ложной тревоги» $\overline{p_1}$, $\overline{p_2}$, $\overline{p_3}$.

На выходе каждого МЗ формируется бинарный сигнал u_j $(j = 1, 2, 3)$, принимающий значение 1 с вероятностью p_j и 0 с вероятностью $(1 - p_j)$, так как два данных события противоположны (т.е. несовместны и образуют полную группу). Например, ситуацию (0, 0, 1) следует трактовать следующим образом: ВП обнаружена только третьим модулем защиты. Поскольку МЗ формируют независимые бинарные сигналы с заданными вероятностями обнаружения ВП, то вероятность появления набора (0, 0, 1) равна $(1 - p_1)(1 - p_2)p_3$.

Аналогично вероятность возникновения «ложной тревоги» для набора бинарных сигналов (0, 0, 1) равна $(1 - \overline{p_1})(1 - \overline{p_2})\overline{p_3}$. В табл. 2.1 представлены вероятностные характеристики кольца защиты для всех возможных комбинаций сработавших МЗ.

Табл. 2.1. *Вероятностные характеристики кольца защиты*

i	Комбинация сработавших МЗ	Вероятность обнаружения ВП, Δp_i	Вероятность «ложной тревоги», $\overline{\Delta p_i}$
0	0 0 0	$(1-p_1)(1-p_2)(1-p_3)$	$(1-\overline{p_1})(1-\overline{p_2})(1-\overline{p_3})$
1	0 0 1	$(1-p_1)(1-p_2)p_3$	$(1-\overline{p_1})(1-\overline{p_2})\overline{p_3}$
2	0 1 0	$(1-p_1)p_2(1-p_3)$	$(1-\overline{p_1})\overline{p_2}(1-\overline{p_3})$
3	0 1 1	$(1-p_1)p_2 p_3$	$(1-\overline{p_1})\overline{p_2}\,\overline{p_3}$
4	1 0 0	$p_1(1-p_2)(1-p_3)$	$\overline{p_1}(1-\overline{p_2})(1-\overline{p_3})$
5	1 0 1	$p_1(1-p_2)p_3$	$\overline{p_1}(1-\overline{p_2})\overline{p_3}$
6	1 1 0	$p_1 p_2(1-p_3)$	$\overline{p_1}\,\overline{p_2}(1-\overline{p_3})$
7	1 1 1	$p_1 p_2 p_3$	$\overline{p_1}\,\overline{p_2}\,\overline{p_3}$

Множество комбинаций вероятностей в таблице должно быть полным:

$$\sum_{i=0}^{7}\Delta p_i = 1;\ \sum_{i=0}^{7}\overline{\Delta p_i} = 1.$$

Вероятность обнаружения ВП для схемы логической обработки «ИЛИ», когда общий сигнал тревоги кольца защиты вызывает любая комбинация с единицей (кроме 0):

$$p_{ИЛИ} = p_1 p_2 p_3 + p_1 p_2(1-p_3) + p_1(1-p_2)p_3 +$$
$$+ p_1(1-p_2)(1-p_3) + (1-p_1)p_2 p_3 + (1-p_1)p_2(1-p_3) +$$
$$+ (1-p_1)(1-p_2)p_3.$$

Вероятность «ложной тревоги» кольца защиты для схемы «ИЛИ» составит:

$$\overline{p_{ИЛИ}} = \sum_{i=0}^{7}\overline{\Delta p_i} \ \text{ без } \overline{\Delta p_0}.$$

Алгоритм определения времени обнаружения ВП кольцом защиты $\overline{T_{ИЛИ}^{ОБ}}$

Шаг 1. Определить номера сработавших средств обнаружения.

Шаг 2. Найти минимальное значение из времен обнаружения ВП сработавших СрО. Конец алгоритма.

Достоинства алгоритма:

1. Оптимизация целевой функции задачи обнаружения вредоносных программ в постановке (2.2), т.е. достигнута максимальная вероятность обнаружения ВП: $p_{ИЛИ} \to \max$.

2. Существенное уменьшение времени обнаружения вредоносной программы $T^{ОБ}$ по сравнению со схемой «И».

Недостатки схемы «ИЛИ»:

1. Алгоритм обнаружения ВП обеспечивает предельно высокую вероятность обнаружения, но и высокую вероятность «ложной тревоги».

2. Решение задачи (2.2) возможно только в том случае, если все модули защиты обеспечивают одинаковые вероятности «ложных тревог», а вероятности обнаружения ВП были бы не ниже заданных.

Алгоритм обнаружения вредоносной программы по схеме «K из N»

Шаг 1. Запуск средств обнаружения кольца защиты.

Шаг 2. Снятие показаний, генерируемых МЗ $u_1, u_2, ..., u_N$.

Шаг 3. Если число сработавших МЗ достигло и/или превысило заданную величину K, то принимается решение о наличии ВП в системе и производится инициирование СП. В противном случае – переход на шаг 2. Конец алгоритма.

Для конкретности воспользуемся данными табл. 2.1. В соответствии с исходными данными вероятность обнаружения ВП для схемы логической обработки «2 из 3»:

$$p_{2/3} = (1-p_1)p_2\,p_3 + p_1(1-p_2)p_3 + p_1\,p_2\,(1-p_3) + p_1\,p_2\,p_3\,.$$

Вероятность «ложной тревоги» кольца защиты для схемы «2 из 3»:

$$\overline{p_{2/3}} = \left(1-\overline{p_1}\right)\overline{p_2}\;\overline{p_3} + \overline{p_1}\left(1-\overline{p_2}\right)\overline{p_3} + \overline{p_1}\;\overline{p_2}\left(1-\overline{p_3}\right) + \overline{p_1}\;\overline{p_2}\;\overline{p_3}.$$

Алгоритм определения времени обнаружения ВП кольца защиты $T^{ОБ}_{2\,из\,3}$

Шаг 1. Определить номера двух сработавших средств обнаружения.

Шаг 2. Найти максимальное значение из времен обнаружения ВП сработавших МЗ. Конец алгоритма.

Достоинство алгоритма: алгоритм является наиболее гибким из традиционных логических алгоритмов обработки бинарных сигналов различных МЗ, так как может обеспечить N различных правил ($K = 1, 2, ..., N$). Кроме этого он позволяет добиться лучшего соотношения вероятностных характеристик работы кольца защиты по сравнению со схемами «И» и «ИЛИ».

Недостаток алгоритма: обработка бинарных сигналов по схеме «K из N» проста, однако отсутствие учета индивидуальных особенно-

стей и характеристик каждого отдельно взятого МЗ не позволяет добиться наилучшего соотношения между вероятностью обнаружения и частотой генерации «ложной тревоги» кольца защиты в целом.

Для устранения недостатков традиционных алгоритмов необходимо учитывать при формировании общего сигнала кольца защиты тот факт, что независимые модули защиты обладают разными значениями вероятности и времени обнаружения ВП, вероятности «ложной тревоги».

Таким образом, возникает необходимость применять алгоритмы логической обработки для колец защиты, позволяющие за счет учета индивидуальных особенностей МЗ добиваться снижения вероятности «ложной тревоги» при сохранении заданной вероятности обнаружения за ограниченное время [23, 25]. Сигналы тревоги от отдельных МЗ в этом случае будут обрабатываться не как одинаково достоверные, а алгоритм обработки будет меняться в зависимости от применяемых МЗ.

Алгоритм обнаружения вредоносной программы «Комбинация сигналов»

Алгоритм основан на переборе всех возможных комбинаций сигналов от кольца защиты. Из них формируется множество таких наборов, при получении которых кольцо защиты генерирует сообщение об обнаружении ВП. Множество отобранных в результате комбинаций определяет решающее правило кольца защиты.

Для реализации поставленной задачи необходимо знать:

1. Вероятности обнаружения ВП p_j $(j=\overline{1,N})$ и вероятности возникновения «ложной тревоги» $\overline{p_j}$ $(j=\overline{1,N})$ каждого из N МЗ, образующих кольцо защиты.

2. Вероятности появления сигнала о ВП кольца защиты Δp_i и вероятности возникновения «ложной тревоги» $\overline{\Delta p_i}$, i – номер комбинации сработавших МЗ (см. табл. 2.1).

Будем рассматривать отношение величин Δp_i и $\overline{\Delta p_i}$ как качественную характеристику логической схемы обработки сигналов кольца защиты, так как наилучшей схемой следует признать ту, которая при обеспечении заданной вероятности обнаружения обладает наименьшей вероятностью «ложной тревоги» (задача в постановке (2.2)).

Для синтеза данной схемы предлагается следующий алгоритм:

Шаг 1. Расставить в таблице комбинации в порядке убывания отношений $\frac{\Delta p_i}{\overline{\Delta p_i}}$.

Шаг 2. Выбрать из полученной таблицы те комбинации, которые в совокупности обеспечивают заданную вероятность обнаружения. Конец алгоритма.

При попытке использования алгоритма, основанного на другом наборе комбинаций, заведомо не будет обеспечиваться заданная точность работы кольца защиты, так как этот набор может быть получен из исходного множества только путем добавления комбинаций, не соответствующих по отношению вероятностей обнаружения и «ложной тревоги» заданному пороговому значению.

Поясним предложенный алгоритм на конкретных данных. Пусть известны вероятности обнаружения $p_1 = 0{,}70$; $p_2 = 0{,}70$; $p_3 = 0{,}99$ и вероятности «ложной тревоги» $\overline{p_1} = 0{,}10$; $\overline{p_2} = 0{,}20$; $\overline{p_3} = 0{,}01$. В табл. 2.2 представлены вероятности работы данного кольца защиты.

Табл. 2.2. *Вероятностные характеристики кольца защиты*

i	Комбинация сработавших МЗ	Δp_i	$\overline{\Delta p_i}$	$\frac{\Delta p_i}{\overline{\Delta p_i}}$
0	0 0 0	0,0009	0,7128	0,0013
1	0 0 1	0,0891	0,0072	12,3750
2	0 1 0	0,0021	0,1782	0,0118
3	0 1 1	0,2079	0,0018	115,5000
4	1 0 0	0,0021	0,0792	0,0265
5	1 0 1	0,2079	0,0008	259,8750
6	1 1 0	0,0049	0,0198	0,2475
7	1 1 1	0,4851	0,0002	2425,5000

Расставив в табл. 2.2 комбинации сработавших средств обнаружения в порядке убывания отношений $\frac{\Delta p_i}{\overline{\Delta p_i}}$, получим табл. 2.3.

Время обнаружения ВП данного кольца защиты $T^{об}$ будет равно $T_З$ $\left(T^{об} = T_З\right)$. Но если значение $T^{об}$ не будет удовлетворять ограниче-

нию $T^{ОБ} \le T^{Д}$, где $T^{Д}$ – допустимые временные затраты на обнаружения ВП кольцом защиты, то можно выбрать другой алгоритм.

В принципе предлагаемая схема формирования алгоритмов логической обработки дает возможность синтеза (в данном случае) семи различных алгоритмов, когда общий сигнал тревоги подается при появлении первой комбинации ($i = 1$), первой или второй ($i = 1$ или $i = 2$) и т.д. При этом каждый из 7 алгоритмов отличается вероятностью и временем обнаружения ВП и обеспечивает минимальную вероятность «ложной тревоги».

Табл. 2.3. *Комбинации сработавших СрО кольца защиты в порядке убывания*

i	Комбинация сработавших МЗ	$\frac{\Delta p_i}{\overline{\Delta p_i}}$
1	1 1 1	2425,5000
2	1 0 1	259,8750
3	0 1 1	115,5000
4	0 0 1	12,3750
5	1 1 0	0,2475
6	1 0 0	0,0265
7	0 1 0	0,0118
8	0 0 0	0,0013

Достоинством предложенного алгоритма является большое число вариантов построения решающего правила (по сравнению с тремя традиционными схемами: «И», «ИЛИ», «К из N»), что обеспечивает большую гибкость при выборе конкретного алгоритма.

Недостатки алгоритма: усложненный вид и неудобства для практической реализации.

Алгоритм обнаружения вредоносной программы «Весовые коэффициенты МЗ».

Пусть для каждого средства обнаружения, образующего кольцо защиты, известны вероятности обнаружения p_1, p_2, …, p_N и вероятности «ложной тревоги» $\overline{p_1}$, $\overline{p_2}$, …, $\overline{p_N}$.

На выходе каждого МЗ формируется бинарный сигнал u_j $(j = 1, 2, ..., N)$, принимающий с определенной вероятностью p_j либо 1 (ВП обнаружена j-м МЗ), либо 0 (ВП не обнаружена). Эти сигналы

характеризуются плотностями распределения вероятностей их появления $f_{yj}(u_j)$ (ВП есть на ОЗ) и $f_{nj}(u_j)$ (ВП нет на ОЗ).

$$f_{yj}(u_j)=\begin{cases} p_j & при\ \ u_j=1, \\ 1-p_j & при\ \ u_j=0, \end{cases} \quad (j=\overline{1,\ N}), \tag{2.6}$$

где p_j – вероятность обнаружения ВП j-м МЗ.

$$f_{nj}(u_j)=\begin{cases} \overline{p_j} & при\ \ u_j=1, \\ 1-\overline{p_j} & при\ \ u_j=0, \end{cases} \quad (j=\overline{1,\ N}), \tag{2.7}$$

где $\overline{p_j}$ – вероятность «ложной тревоги» j-го МЗ.

По критерию Неймана – Пирсона [93] решающее правило может быть записано в виде

$$\lg\frac{f_y(u_1,u_2,...,u_N)}{f_n(u_1,u_2,...,u_N)}>c, \tag{2.8}$$

где $f_y(u_1,u_2,...,u_N)$ – совместная плотность распределения вероятностей бинарных сигналов от МЗ в условиях воздействия ВП; $f_n(u_1,u_2,...,u_N)$ – совместная плотность распределения вероятностей бинарных сигналов от МЗ в ситуации отсутствия вредоносных программ; $u_1,u_2,...,u_N$ – анализируемая совокупность бинарных сигналов от кольца защиты; c – постоянная, определяемая необходимой (минимально достаточной) вероятностью защиты (пороговое значение).

При выполнении (2.8) принимается решение о наличии ВП в системе и проводится организация мер по ее уничтожению. Оптимальность решающего правила заключается в том, что при обеспечении заданной вероятности обнаружения кольца защиты в целом (которая регулируется изменением величины c) достигается минимум вероятности «ложной тревоги». Если все МЗ работают независимо друг от друга, то бинарные сигналы статически независимы:

$$f_y(u_1,u_2,...,u_N)=\prod_{j=1}^{N} f_{yj}(u_j);$$

$$f_n(u_1,u_2,...,u_N)=\prod_{j=1}^{N} f_{nj}(u_j).$$

Тогда решающее правило (2.8) можно записать в виде

$$\sum_{j=1}^{N} lg\frac{f_{yj}(u_j)}{f_{nj}(u_j)}>c.$$

Вычитая из обеих частей неравенства одну и ту же постоянную величину $\sum_{j=1}^{N} lg\frac{1-p_j}{1-\overline{p_j}}$ и введя новое обозначение $c_1 = c - \sum_{j=1}^{N} \lg\frac{1-p_j}{1-\overline{p_j}}$, получим $\sum_{j=1}^{N} lg\frac{f_{yj}(u_j)(1-\overline{p_j})}{f_{nj}(u_j)(1-p_j)} > c_1$.

После этого можно окончательно написать решающее правило в виде

$$\sum_{j=1}^{N} V_j(u_j) > c_1, \qquad (2.9)$$

где $V_j(u_j) = lg\frac{f_{yj}(u_j)(1-\overline{p_j})}{f_{nj}(u_j)(1-p_j)}$.

Если выполняется неравенство (2.9), то формируется общий сигнал кольца защиты о наличии ВП, при этом из (2.6) и (2.7) видно:

$$V_j(u_j) = \begin{cases} q_j & при\ u_j = 1, \\ 0 & при\ u_j = 0, \end{cases} \quad (j = \overline{1, N}), \qquad (2.10)$$

где $q_j = lg\frac{p_j\left(1-\overline{p_j}\right)}{\overline{p_j}\left(1-p_j\right)}$ – постоянная величина для j-го МЗ («вес» j-го МЗ).

Таким образом, оптимальный в указанном смысле алгоритм построения кольца защиты согласно (2.9) и (2.10) заключается в формировании по сигналу тревоги от j-го МЗ с заданным значением q_j с последующим суммированием сигналов и сравнением полученной суммы с фиксированным пороговым уровнем, превышение которого приведет к формированию общего сигнала тревоги.

Значения «весов» q_j можно рассчитать заранее по вероятности обнаружения и вероятности «ложной тревоги» j-го МЗ. Чем больше вероятность обнаружения МЗ и чем меньше его вероятность «ложной тревоги», тем больше «вес» МЗ.

Поясним предложенный алгоритм на примере кольца защиты, в состав которого входят три МЗ.

Пусть заданы вероятности обнаружения каждого МЗ $p_1 = 0{,}8$; $p_2 = 0{,}6$; $p_3 = 0{,}5$ и вероятности «ложной тревоги» $\overline{p_1} = 0{,}4$; $\overline{p_2} = 0{,}2$; $\overline{p_3} = 0{,}1$.

«Вес» каждого МЗ рассчитаем по формуле $q_j = lg\frac{p_j\left(1-\overline{p_j}\right)}{\overline{p_j}\left(1-p_j\right)}$, полу-

чим $q_1 = 0{,}477$; $q_2 = 0{,}778$; $q_3 = 0{,}954$ и $\sum_{j=1}^{3} q_j = 2{,}210$. В табл. 2.4 представлены все возможные комбинации бинарных сигналов от кольца защиты.

Табл. 2.4. *Комбинации бинарных сигналов от кольца защиты*

i	Комбинация сработавших МЗ	$\sum_{j=1}^{3} V_j(u_j)$
0	0 0 0	0,000
1	0 0 1	0,954
2	0 1 0	0,778
3	0 1 1	1,732
4	1 0 0	0,477
5	1 0 1	1,431
6	1 1 0	1,255
7	1 1 1	2,210

Для реализации решающего правила (2.9) необходимо установить пороговое значение c_1, по достижению которого вырабатывается общий сигнал о наличии ВП в системе. Очевидно, что пороговое значение c_1 не должно превышать $\sum_{j=1}^{3} q_j = 2{,}210$.

Например, при $c_1 = 1$ общий сигнал тревоги подается при появлении первой из четырех комбинаций ($i = 3$, 5, 6 и 7). При этом время обнаружения ВП данного кольца защиты определяется по следующему правилу: если $i = 3$, то $T^{ОБ} = \max(T_2, T_3)$; если $i = 5$, то $T^{ОБ} = \max(T_1, T_3)$; если $i = 6$, то $T^{ОБ} = \max(T_1, T_2)$; если $i = 3$, то $T^{ОБ} = \max(T_1, T_2, T_3)$. Для обеспечения ограничения $T^{ОБ} \le T^{Д}$, где $T^{Д}$ – допустимые временные затраты на обнаружение ВП кольцом защиты, необходимо выбрать нужные номера комбинаций i.

Достоинства и отличительные особенности полученного алгоритма работы кольца защиты в соответствии с (2.9) и (2.10):

1. Алгоритм полностью идентичен алгоритму 4, однако имеет более простой вид и удобнее для практической реализации. При этом несмотря на то что общий сигнал тревоги формируется при превыше-

нии порогового значения суммой сигналов тревоги от отдельных МЗ (2.9), каждый из которых имеет свой «вес» (2.10), сохраняется логический алгоритм кольца защиты, так как при заданной величине порогового уровня c_1 превышение его могут вызвать лишь определенные комбинации сигналов тревоги от отдельных МЗ.

2. Значения q_j (2.10) определены до постоянного множителя, т.е. алгоритм не изменится, если все «веса» одновременно увеличить или уменьшить в одно и то же количество раз (изменив во столько же раз значение порога).

3. Алгоритм, определяемый (2.9) и (2.10), всегда оптимален, т.е. при заданной вероятности обнаружения обеспечивает минимально возможную вероятность «ложной тревоги».

Покажем справедливость данного утверждения.

Введем следующие обозначения:

H_1 – основная гипотеза, которая заключается в том, что вредоносной программы в системе нет;

H_2 – альтернативная гипотеза, которая означает, что ВП есть.

На практике возникает следующая альтернатива: можно решить или отвергнуть, или принять предложенную гипотезу H_1 и действовать в соответствии с этим решением. И в том и в другом случае решение может оказаться ошибочным, так как можно отвергнуть гипотезу H_1, когда она в действительности верна, и принять гипотезу, когда она ошибочна.

Пусть ошибка I рода α_1 состоит в том, что H_1 отвергается, хотя она верна. Ошибка II рода α_2 состоит в том, что H_1 принимается, в то время как верна H_2.

Для принятия решения о наличии или отсутствии ВП в системе на основе показаний N модулей защиты (кольца защиты) необходимо использовать критерий, при котором вероятность отвергнуть гипотезу H_1, если она в действительности верна, была мала, а вероятность отвергнуть H_1, когда она ошибочна, была велика. При этом из нескольких критериев, соответствующих одной и той же вероятности отвергнуть в действительности правильную гипотезу H_1, следует предпочесть тот, который дает большую вероятность отвергнуть H_1, когда эта гипотеза ошибочна [10, 93].

Назовем отношение $\dfrac{f_y(u_1,u_2,\ldots,u_N)}{f_n(u_1,u_2,\ldots,u_N)}$ отношением правдоподобия.

Критерий отношения правдоподобия (КОП):

$$\delta_c(U) = \begin{cases} H_1, \ \textit{если} \ \dfrac{f_y(u_1,u_2,...,u_N)}{f_n(u_1,u_2,...,u_N)} \le c, \\ H_2, \ \textit{если} \ \dfrac{f_y(u_1,u_2,...,u_N)}{f_n(u_1,u_2,...,u_N)} > c. \end{cases}$$

Лемма Неймана – Пирсона [93] гласит, что существует постоянная *c*, при которой критерий отношения правдоподобия является минимаксным критерием; число *c* следует выбрать так, чтобы вероятности ошибок первого и второго рода были одинаковы: $\alpha_1(\delta_c) = \alpha_2(\delta_c)$.

Выражение (2.8) соответствует КОП. В свою очередь, выполнение неравенства (2.9) тождественно выполнению (2.8). Таким образом, алгоритм, определяемый (2.9) и (2.10), является оптимальным, т.е. при заданной вероятности обнаружения он обеспечивает минимально возможную вероятность «ложной тревоги».

Алгоритм обеспечивает и максимально возможную вероятность обнаружения при заданной вероятности «ложных тревог». Иными словами, невозможно синтезировать алгоритм, который улучшил бы одну из указанных характеристик (по сравнению с алгоритмом (2.9) и (2.10)), не ухудшая одновременно другую.

4. Изменение порогового уровня c_1 (2.9) позволяет установить различные вероятности обнаружения алгоритма в целом. При этом в общем случае обеспечивается $(2^N - 1)$ различных вариаций, в то время как традиционные схемы логической обработки *K* из *N* обеспечивают только *N* различных градаций ($K = 1, 2, \ldots, N$).

Установка порогового уровня c_1 в пределах

$$\sum_{j=1}^{N} q_j - \min q_j < c_1 < \sum_{j=1}^{N} q_j$$

дает алгоритм, тождественный алгоритму «И», обеспечивающий предельно низкую вероятность «ложной тревоги», но и невысокую вероятность обнаружения.

Другое крайнее значение рассматриваемого алгоритма

$$0 < c_1 < \min q_j \ \ (j = 1, 2, \ldots, N)$$

тождественно алгоритму «ИЛИ», обеспечивающему предельно высокую вероятность обнаружения, но и высокую вероятность «ложной тревоги».

Таким образом, большое число вариаций алгоритма, определяемого (2.9) и (2.10), находится в наиболее важной для практических применений области между схемами «И» и «ИЛИ», что облегчает подбор конкретного значения порогового уровня c_1, обеспечивающий заданные характеристики кольца защиты. Причем в процессе подбора значения c_1 для заданной вероятности обнаружения минимальная вероятность «ложной тревоги» будет обеспечена автоматически.

То же самое относится и к возможности регулировки характеристик кольца защиты в условиях эксплуатации (например, в связи с изменением тактической обстановки) путем изменения порогового уровня c_1 в пределах $0 < c_1 < \sum_{j=1}^{n} q_j$, обеспечивающего оптимальность алгоритма для любого значения c_1.

5. Алгоритм кольца защиты, определяемый (2.9) и (2.10), является универсальным по отношению к использованию различных МЗ. Действительно, значения q_j полностью определяются значениями характеристик j-го МЗ (2.10) и не зависят от характеристик других МЗ, используемых в составе кольца защиты, т.е. значение «веса» j-го МЗ может учитываться непосредственно при формировании сигнала тревоги от j-го МЗ. В этом случае обеспечивается простота наращивания дополнительных МЗ в кольце защиты.

6. В связи с тем что алгоритм, определяемый (2.9) и (2.10), носит логический характер, он дает выигрыш по сравнению с традиционной схемой «K из N» лишь в случае объединения в кольцо защиты не менее трех МЗ.

Недостаток алгоритма: предложенный алгоритм обнаружения ВП кольцом защиты, определяемый (2.9) и (2.10), улучшает характеристики традиционных логических схем. Но так же, как и традиционные алгоритмы, он основывается на утверждении, что все МЗ работают независимо друг от друга и бинарные сигналы МЗ статически независимы. Поэтому алгоритм, определяемый (2.9) – (2.10), не учитывает возможного взаимного влияния различных модулей защиты друг на друга (например, одна антивирусная программа может исключить работу другой в одном узле защиты компьютерной системы).

Алгоритм обнаружения вредоносных программ, основанный на понятии критической области

Пусть кольцо защиты включает в себя n модулей защиты, каждый из которых вырабатывает сигнал $X_k \left(k = \overline{1, n}\right)$ о наличии ВП. Случайные величины (СВ) X_k принимают значения 0 и 1 по схеме: 1 – ВП обнаружена в системе; 0 – ВП не обнаружена. Независимые МЗ обладают разными значениями вероятности обнаружения и вероятности возникновения «ложной тревоги», данное обстоятельство будем учитывать при формировании общего сигнала кольца защиты.

Ситуацию можно трактовать так: имеется СВ X_0, которая принимает значение 1, если ВП есть, и 0 – в противном случае. Предметом внимания является распределение многомерной СВ ($X_0, X_1, \ldots, X_n$).

Введем следующие обозначения:

x_0 – показатель, принимающий значения 0 или 1 (реализация X_0);

$x = (x_1, x_2, \ldots, x_n)$ – система показателей, где x_k также принимает одно из двух значений;

S – множество всех наборов x, состоящее из $N = 2^n$ элементов;

S^* – критическая область угроз (КОУ) такая, что если $x \in S^*$, то ВП существует, иначе ВП отсутствует при этом $S^* \subset S$.

Статистическая функция $P = p(x_0, x_1, \ldots, x_n)$, где значения p – это относительные частоты появления кода $(x_0, x_1, \ldots, x_n)$, позволяет определить КОУ. Таким образом, $0 \le p \le 1$ и сумма $p(x_0, x_1, \ldots, x_n)$ по всем кодам равна 1.

Выборочный закон распределения СВ X_0, в частности, имеет вид: значению $X_0 = 0$ соответствует вероятность q_0, значению $X_0 = 1$ – вероятность p_0, где $p_0 = \sum_{x \in S} p(1; x);\ q_0 = 1 - p_0$.

Одним из основных является вопрос: как на основании показаний модулей защиты X_k определить, есть ВП или нет? В рамках традиционного подхода он может быть решен следующим образом [93]. Пусть, например, основная гипотеза H_0 заключается в том, что ВП нет ($X_0 = 0$), тогда H_1 – альтернативная гипотеза, означает, что ВП есть ($X_0 = 1$). Тогда если $x \in S^*$, то гипотеза H_0 отвергается.

Ошибка I рода α состоит в том, что H_0 отвергается, хотя она верна. Ошибка α вычисляется по формуле

$$\alpha = \frac{1}{q_0} \sum_{x \in S^*} p(0; x). \qquad (2.11)$$

Ошибка II рода β состоит в том, что H_0 принимается, в то время как верна H_1, и вычисляется по следующей формуле:

$$\beta = 1 - \frac{1}{p_0} \sum_{x \in S^*} p(1; x). \qquad (2.12)$$

Величину αq_0 может быть интерпретирована как вероятность «ложной тревоги» кольца защиты, βp_0 – как вероятность «необнаруженной ВП» кольца защиты.

Задача построения критической области угроз кольца защиты состоит в том, чтобы при фиксированном уровне значимости α за счет выбора S^* минимизировать β. Данная трактовка соответствует задаче (2.2).

Задача построения КОУ может быть решена в рамках следующего алгоритма.

Алгоритм построения критической области угроз

Шаг 1. Пронумеровать элементы множества S так, чтобы величины $\frac{p(1; x_a)}{p(0; x_a)}$ не возрастали $(a = \overline{1, N})$.

Шаг 2. Построить последовательность расширяющихся подмножеств $S_a^* \subset S$, а именно: $S_0^* = \varnothing$, $S_1^* = \{x_1\}$, $S_2^* = \{x_1, x_2\}$ и т.д. Если найдутся наборы элементов *x* с частотой *p(0; x) = 0*, то такие наборы *x* включаются в подмножество S_0^*.

Шаг 3. Рассчитать две числовые последовательности:

$$0 = \alpha_0 \le \alpha_1 \le \ldots \le \alpha_{N'} = 1,$$

$$\beta_0 \ge \beta_1 \ge \ldots \ge \beta_{N'} = 0,$$

где $N' \le N$, $\alpha_a = \frac{1}{q_0} \sum_{x \in S^*_a} p(0; x)$, $\beta_a = 1 - \frac{1}{p_0} \sum_{x \in S^*_a} p(1; x)$.

Шаг 4. Вычислить суммы соответствующих элементов: $\alpha_0 + \beta_0$, $\alpha_1 + \beta_1$ и т.д. Определить номер *a*, которому соответствует наименьшее полученное значение. Подмножество S_a^* будет являться КОУ. Вычислить значения вероятностей $\alpha_a q_0$ и $\beta_a p_0$ кольца защиты. Конец алгоритма.

Предлагаемый алгоритм обнаружения вредоносных программ включает следующие этапы:

Этап 1. Формирование критической области угроз S^* для выбранных модулей защиты, образующих кольцо защиты. Необходимые вероятностные характеристики кольца защиты могут быть представлены разработчиками или получены экспериментально.

Этап 2. Кольцо защиты, состоящее из n модулей защиты, во время своей работы генерирует сигналы $x = (x_1, x_2, \ldots, x_n)$. При выполнении $x \in S^*$ принимается решение о наличии ВП в системе и производится организация мер по ее уничтожению. При этом время $T^{ОБ}$ зависит только от характеристик выбранного кольца защиты и может быть улучшено за счет смены средства обнаружения.

Поясним предложенный алгоритм построения критической области угроз на конкретных данных. Рассмотрим кольцо защиты, включающее антивирусные программы Касперского Personal 5.0.372, McAfee 9.0., Norton Antivirus 2005. Для построения КОУ было проведено экспериментальное исследование вероятностных характеристик данных антивирусных программ [29].

Цели исследования

1. Получить динамическую характеристику вероятности выявления ВП различными модулями защиты.

2. Получить относительные частоты p появления кода $(x_0, x_1, \ldots, x_n)$, т.е. вероятности обнаружения и вероятности «ложной тревоги» кольца защиты, включающего n модулей защиты. В рассматриваемом исследовании $n = 3$.

Методика эксперимента

1. Формирование сканируемого набора и заражение случайно выбранных из него файлов.

2. Многократные сеансы сканирования каждой антивирусной программой. Длительность каждого сеанса строго фиксирована и по истечении времени процесс останавливается независимо от результатов.

3. Весь сеанс сканирования разбивается на равные отрезки времени, на каждом из которых фиксируется количество вирусов и количество предупреждений о возможном наличии ВП.

Результаты исследования

1. Сравнительная характеристика антивирусных программ в идеальных условиях работы операционной системы (рис. 2.3).

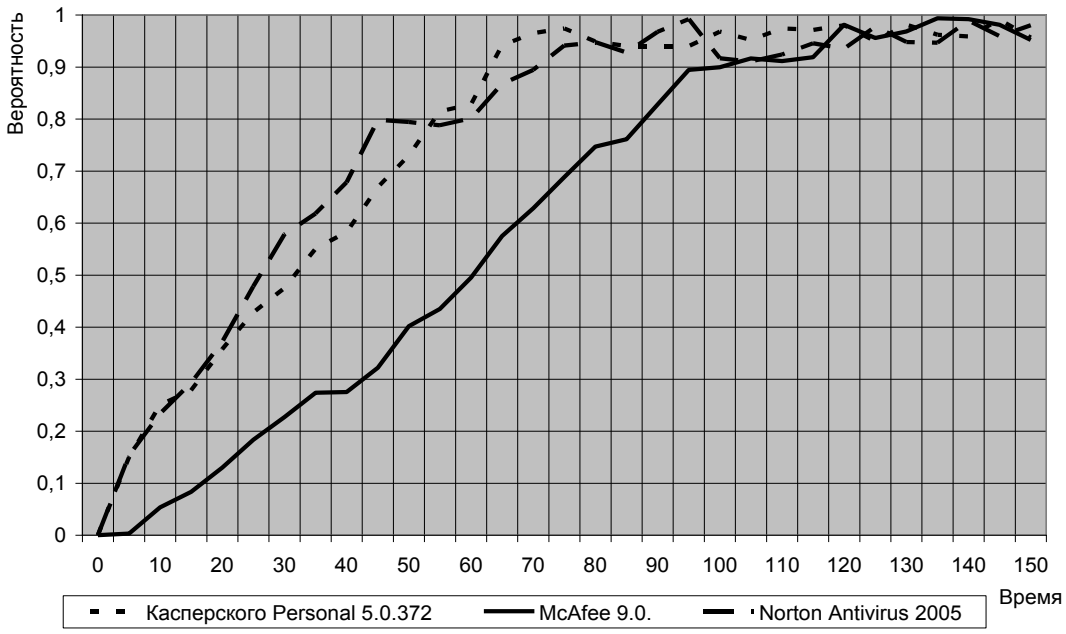


Рис. 2.3. Динамика вероятности выявления ВП антивирусными программами в идеальных условиях работы ОС

2. Сравнительная характеристика антивирусных программ в реальных условиях работы операционной системы (рис. 2.4).

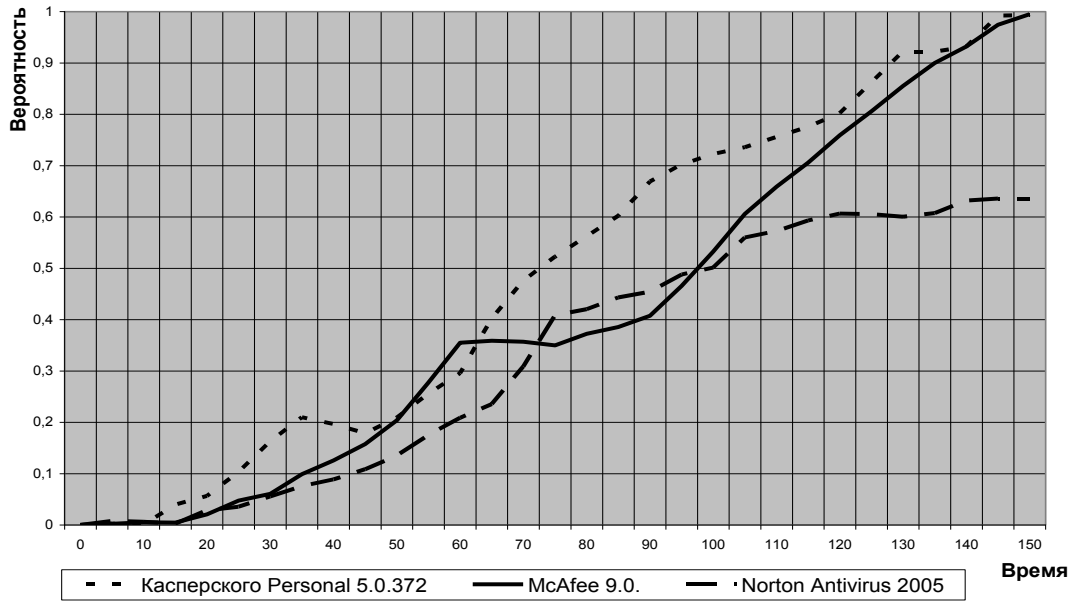


Рис. 2.4. Динамика вероятности выявления ВП антивирусными программами в реальных условиях работы ОС

3. Относительные частоты p появления кода $(x_0, x_1, \ldots, x_n)$, т.е. вероятности обнаружения и вероятности возникновения «ложной тревоги» кольца защиты (табл. 2.5).

Табл. 2.5. *Вероятностные характеристики кольца защиты, включающего 3 антивирусные программы*

x_0	x_1	x_2	x_3	$p(x_0, x)$
1	0	0	0	0,03
1	0	0	1	0,02
1	0	1	0	0,10
1	0	1	1	0,20
1	1	0	0	0,05
1	1	0	1	0,15
1	1	1	0	0,02
1	1	1	1	0,03
0	0	0	0	0,08
0	0	0	1	0,04
0	0	1	0	0,02
0	0	1	1	0,10
0	1	0	0	0,09
0	1	0	1	0,02
0	1	1	0	0,00
0	1	1	1	0,05

Произведем необходимые вычисления алгоритма построения КОУ кольца защиты [26].

1. Вычислим значения вероятностей p_0 и q_0:

$p_0 = 0,03 + 0,02 + 0,1 + 0,2 + 0,05 + 0,15 + 0,02 + 0,03 = 0,6;$

$q_0 = 1 – 0,6 = 0,4.$

В данном случае встретился набор x, относительная частота появления которого равна 0. Из этого следует, что $S_0^* \neq \varnothing$.

2. Пронумеруем элементы множества s так, чтобы величины $\frac{p(1;x_a)}{p(0;x_a)}$ не возрастали, и соответственно этому построим последовательность расширяющихся подмножеств $S_a^* \subset S$.

3. Вычислим величины соотношений вида $\frac{p(1;x)}{p(0;x)}$ для каждого набора показателей x

a	0	1	2	3	4	5	6	7
p (1; x)	0,02	0,15	0,10	0,20	0,30	0,05	0,02	0,03
p (0; x)	0,00	0,02	0,02	0,10	0,05	0,09	0,04	0,08

4. Вычислим ошибки I и II рода для *a = 0, 1, .., 7*

α_a	0,00	0,05	0,10	0,35	0,48	0,70	0,80	1,00
β_a	0,97	0,72	0,55	0,22	0,17	0,08	0,05	0,00

Для выбора критической области S^* и окончания алгоритма условимся выбирать min($\alpha_a + \beta_a$). В данном случае min($\alpha_a + \beta_a$) = 0,55 при $\alpha_3 = 0{,}35$ и $\beta_3 = 0{,}22$, что соответствует подмножеству $S_3 = \{x_0, x_1, x_2, x_3\}$.

В КОУ рассматриваемого кольца защиты входят следующие наборы показателей *x*: (1, 1, 0); (1, 0, 1); (0, 1, 0) и (0, 1, 1).

Время обнаружения $T^{ОБ}$ вредоносной программы по сравнению с рассмотренными ранее логическими алгоритмами обработки сигналов кольца защиты сократилось минимум вдвое, при этом вероятность «ложной тревоги» $\alpha q_0 = 0{,}14$, а вероятность «необнаруженной ВП» $\beta p_0 = 0{,}13$.

Достоинства полученного алгоритма работы кольца защиты:

1. Алгоритм, основанный на применении критической области угроз, обеспечивает оптимальное соотношение ошибок I рода (2.11) и II рода (2.12) [93]. Таким образом данный алгоритм позволяет решить задачу в постанове (2.2): добиться оптимальности вероятности «ложной тревоги» $(P = \alpha q_0)$ и вероятности «необнаруженной ВП» кольца защиты $(\overline{P} = \beta p_0)$.

2. Предложенный алгоритм обнаружения ВП кольцом защиты учитывает возможное взаимное влияние различных МЗ друг на друга, так как в основе его работы лежит КОУ, построенная на вероятностных характеристиках общего сигнала кольца, а не отдельных модулей защиты [22].

3. Существенное уменьшение времени обнаружения ВП $T^{ОБ}$ по сравнению с традиционными алгоритмами обнаружения вредоносных программ кольцом защиты [16, 64].

Недостатком полученного алгоритма работы кольца защиты является сложность изменения структуры кольца защиты, так как при добавлении новых модулей защиты или при удалении используемых МЗ необходимо строить новую критическую область угроз. Для построения КОУ необходимо знать и новую статистическую функцию $P = p(x_0, x_1, \ldots, x_n)$, где значения *p* – это относительные частоты появления кода $(x_0, x_1, \ldots, x_n)$.

Модель III. Кольца защиты

Рассмотрим модель организации защитных механизмов в РТКС [21], которую для наглядности представим в виде ориентированного графа (рис. 2.5). Вершины графа – объекты защиты (защищаемые ресурсы и процессы РТКС, множество *O*) и модули защиты (множество M). Дуги (связи) графа – возможные пути распространения ВП в системе.

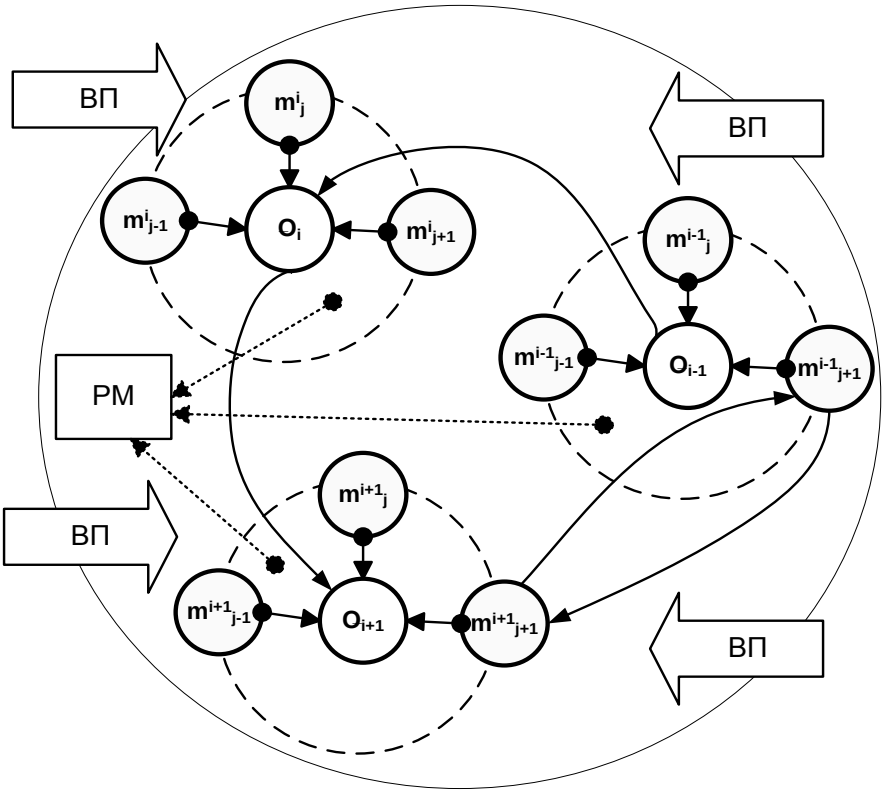


Рис. 2.5. Модель организации защитных механизмов в РТКС с несколькими объектами

Для каждого кольца защиты должно быть выбрано решающее правило наличия или отсутствия ВП в системе. Кольца защиты различных объектов могут работать и по различным схемам обнаружения ВП. Выбор алгоритма обнаружения ВП зависит от состава и количества модулей защиты, образующих кольцо защиты, от допустимых временных затрат на обнаружение ВП кольцом защиты [20]. Сигналы от каждого кольца защиты могут обрабатываться общим решающим модулем, который также должен работать по одному из рассмотренных алгоритмов обнаружения ВП [16, 64].

Выводы

Показано, что задача построения системы защиты объектов РТКС заключается в подборе модулей защиты, совокупность которых смогла бы обеспечить за ограниченное время не только максимальную вероятность обнаружения ВП, но и минимальную вероятность «ложной тревоги». Для ее решения предложена новая модель организации защитных механизмов в РИВС, реализация которой позволит учесть индивидуальные особенности и характеристики МЗ.

Для реализации модели предложены алгоритмы обнаружения ВП, устраняющие недостатки традиционных логических схем [18, 19, 28]. Одним из практических результатов внедрения предложенной модели в РТКС будет являться сокращение времени обнаружения ВП.

Глава 3

Исследование моделей противодействия атакам вредоносных программ в распределенной телекоммуникационной системе

√ Модель противодействия на основе механизмов эволюции взаимодействующих биологических видов (трофическая модель взаимодействия)

√ Исследование трофической модели противодействия

√ Физическая модель противодействия распространению вредоносных программ

Рассмотрены модели противодействия атакам вредоносных программ в распределенной телекоммуникационной системе, основанные на результатах теории нелинейных динамических систем. Модели учитывают системные параметры, характеристики вредоносных программ и программ информационной защиты. Приводятся результаты теоретического исследования разработанных моделей. Анализируются возможности прогнозирования всплесков деструктивной активности в распределенной системе

Введение

Современная РТКС представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый ее компонент может подвергнуться воздействию вредоносных программ.

В результате таких атак под контролем злоумышленников оказываются вычислительные ресурсы РТКС, что в пределе может привести к блокированию деятельности организации. Таким образом, возникает необходимость в определении особенностей появления и распространения ВП, изучении моделей противодействия вирулентному коду для предотвращения тотальных эпидемий и, следовательно, обеспечения безопасной работы организации.

Целью исследования являлось изучение моделей противодействия атакам вредоносных программ в распределенной информационно-вычислительной системе, механизмов и факторов, влияющих на их распространение по компьютерам системы, объектом исследования – совокупность процессов, протекающих в РТКС под воздействием вирулентного кода.

Теоретической основой данного исследования послужила современная теория нелинейных динамических систем, развитая в работах В. И. Арнольда [4 – 6], Г. Николиса [68, 112], И. Пригожина [70], Томпсона [114, 115] и др. Результаты теории, на взгляд авторов, открывают перспективные возможности в решении задач информационной безопасности.

В главе описываются две модели противодействия. Первая имеет аналогом биологическую модель трофического взаимодействия особей, вторая – так называемую физическую модель противодействия динамических систем.

3.1. Модель противодействия на основе механизмов эволюции взаимодействующих биологических видов (трофическая модель взаимодействия)

Противодействие в трофических экосистемах описывают классические уравнения Лотки – Вольтерра [107]. Дифференциальные уравнения, определяющие рост, упадок и общую эволюцию взаимо-

действующих биологических видов, аналогичны по структуре и форме уравнениям, которые встречались в химической кинетике. В простой экосистеме типа «хищник-жертва» могут возникнуть колебания, похожие на устойчивые колебания маятника без затухания.

Применим данную модель к процессам противодействия атакам вредоносных программ системы информационной защиты.

Пусть анализируемая РТКС состоит из N узлов (компьютеров). Распространение вредоносной программы (ВП) в данной системе происходит по закону

$$x(t) = f(x_0), \tag{3.1}$$

где x_0 – начальная «заражённость» РТКС, определяемая числом компьютеров с ВП в начальный момент времени ($t = t_0$); $x(t)$ – число компьютеров, заражённых в момент времени $t \geq t_0$.

Предположим, что при наличии ВП в РТКС компьютеры заражаются со скоростью

$$\frac{dx(t)}{dt} = k_1 a x(t), \tag{3.2}$$

где k_1 – постоянная; a – параметр, определяющий среднюю скорость заражения компьютеров в системе (будем полагать, что с точки зрения «поражаемости» вредоносной программой компьютеры РИВС идентичны).

Из формулы (3.2) следует, что чем больше компьютеров в системе заражено, тем с большей скоростью происходит заражение остальных компьютеров. Однако в пригодной для практического применения модели важно учесть следующий факт: если компьютер заразился один раз, он уже не может заразиться повторно, т.е. когда число заражённых компьютеров достигнет определённого порога, общая скорость заражения в РТКС должна упасть.

Скорость заражения компьютеров будем определять исходя из следующих рассуждений. Вредоносные программы размножаются самостоятельно, сканируя адресное пространство, и рассылают свои копии по другим компьютерам. Тогда формула для скорости заражения (распространения ВП) будет иметь следующий вид:

$$a = v_{\text{скан ВП}} \frac{N}{l_{\text{адр}}}, \tag{3.3}$$

где $v_{сканВП}$ – скорость сканирования вредоносной программой РИВС; $I_{адр}$ – размер системного адресного пространства.

Усложним модель. Определим понятие «вакцина» как программный код, служащий для нейтрализации, защиты и устранения вредных последствий вредоносных программ. Под это понятие в данной модели также можно отнести действия системного администратора по установке дополнительных обновлений программ.

По аналогии с (3.2) предположим, что заражённые компьютеры будут «вакцинироваться» со скоростью

$$\frac{dx(t)}{dt} = -k_3 b x(t), \tag{3.4}$$

где k_3 – постоянная; b – параметр, определяющий среднюю скорость вакцинации компьютеров в системе (будем полагать, что с точки зрения «восстанавливаемости» вакциной компьютеры РИВС идентичны).

Скорость распространения вакцины будем определять из следующего соотношения:

$$b = v_{взаим} + v_{скан.вак} \frac{N}{I_{адр}}, \tag{3.5}$$

где $v_{скан.вак}$ – скорость сканирования вакциной компьютеров РТКС; $I_{адр}$ – размер системного адресного пространства; $v_{взаим}$ – скорость взаимодействия (вакцина может распространяться не только самостоятельно по РТКС, системные администраторы также могут обмениваться между собой копиями вакцин).

Таким образом, модель (3.2) изменяется. Теперь динамику заражения можно представить как

$$\frac{dx(t)}{dt} = k_1 a x(t) - k_3 b x(t). \tag{3.6}$$

Проанализируем составляющие модели (3.6):

а) если $k_3 b$ будет постоянно расти, но при этом $k_1 a = const$, то все компьютеры в сети будут «вылечены». Практически данная ситуация означает что вакцины поступают в компьютеры РТКС заблаговременно и вредоносных программ со временем в системе не будет;

б) если $k_1 a$ будет постоянно расти, но при этом $k_3 b = const$, то это будет обозначать, что в системе будут появляться новые ВП, ком-

пьютеры не будут успевать вакцинироваться, таким образом, число заражённых компьютеров рано или поздно достигнет максимума (так называемая «эпидемия», данное состояние наступает, когда 75 % компьютеров системы заражены).

Пусть компьютеры РТКС вакцинируются со средней скоростью в соответствии с зависимостью

$$\frac{dr(t)}{dt} = k_4 br(t), \tag{3.7}$$

где k_4 – постоянная для данного процесса; $r(t)$ – число компьютеров, вакцинированных в момент времени $t \geq t_0$.

Рассмотрим противодействие ВП и вакцин. Выделим 2 случая противодействия:

а) если компьютер уже вакцинирован и на него «нападает» ВП, то компьютер заражен не будет. Потенциально возможное количество зараженных уменьшается;

б) если компьютер заражен и поступает вакцина, то компьютер восстанавливается, т.е. рост вакцин ведет к уменьшению числа зараженных.

Выше приведенные процессы опишем следующими дифференциальными уравнениями:

$$\frac{dx(t)}{dt} = -k_2 r(t)x(t), \tag{3.8}$$

$$\frac{dr(t)}{dt} = k_2 x(t)r(t). \tag{3.9}$$

Модель (3.2) с учетом (3.8) и (3.9) преобразуется к системе

$$\begin{cases} \dfrac{dx(t)}{dt} = k_1 ax(t) - k_2 r(t)x(t), \\ \dfrac{dr(t)}{dt} = k_2 x(t)r(t). \end{cases} \tag{3.10}$$

Усложняем модель. В определённых случаях вакцинированный ранее компьютер может быть заражен. Это может произойти, например, в случае переустановки операционной системы на компьютере и потери программного кода вакцины, либо случилось какое-то упущение системного администратора. Данный процесс опишем следующей зависимостью:

$$\frac{dr(t)}{dt} = -k_3 br(t). \qquad (3.11)$$

Теперь модель будет выглядеть в виде системы

$$\begin{cases} \frac{dx(t)}{dt} = k_1 ax(t) - k_2 r(t)x(t), \\ \frac{dr(t)}{dt} = k_2 x(t)r(t) - k_3 br(t). \end{cases} \qquad (3.12)$$

По виду это классические уравнения Лотки – Вольтерра [13], описывающие динамику простой экологии типа «хищник-жертва». Их использовали в течение многих лет для моделирования основных биологических явлений, таких как биологические часы и нестационарные нейронные сети.

Уточняем модель (3.12). Во втором уравнении системы имеется величина ($k_2 x(t)r(t)$). Анализируя практический смысл данного выражения, получаем, что вакцинируются только заражённые компьютеры. Такое состояние в РТКС вполне возможно, но кажется маловероятным. Обычно вакцинируются все компьютеры – и зараженные, и вакцинированные.

Таким образом, естественно к данной величине в текущей модели добавить вакцинирование незараженных компьютеров в соответствии с (3.7). Данное некоторое усложнение ведет к следующей системе дифференциальных уравнений для описания модели:

$$\begin{cases} \frac{dx(t)}{dt} = k_1 ax(t) - k_2 r(t)x(t), \\ \frac{dr(t)}{dt} = k_4 br(t) + k_2 x(t)r(t) - k_3 br(t). \end{cases} \qquad (3.13)$$

Данную систему назовем моделью противодействия атакам вредоносных программ в РТКС.

3.2. Исследование трофической модели противодействия

Пример 1. Рассматривается модель, описываемая системой (3.13), со следующими значениями параметров: $k_1 = 10^8$; $k_2 = 1$; $k_3 = 4 \cdot 10^9$; $k_4 = 3 \cdot 10^9$; $N = 10$; $I_{адр} = 2^{32}$; $v_{скан.ВП} = 10$; $v_{скан.вак} = 1$; $v_{взаим} = 10^{-9}$; $X_0 = 1$; $R_0 = 2$ ($a = 2.328 \cdot 10^{-8}$; $b = 2.428 \cdot 10^{-9}$).

Рассмотрим динамику распространения ВП. График зависимости *x(t)* от *r(t)* представлен на рис. 3.1. Фазовый портрет системы

представляет собой концентрически замкнутую кривую, окружающую одну стационарную точку (центр).

Процесс изменения численности вакцин и вредоносных программ (рис. 3.2) имеет колебательный характер. Данные колебания зависят от начальных условий, имеют определённый период. После каждого периода система возвращается в начальную точку.

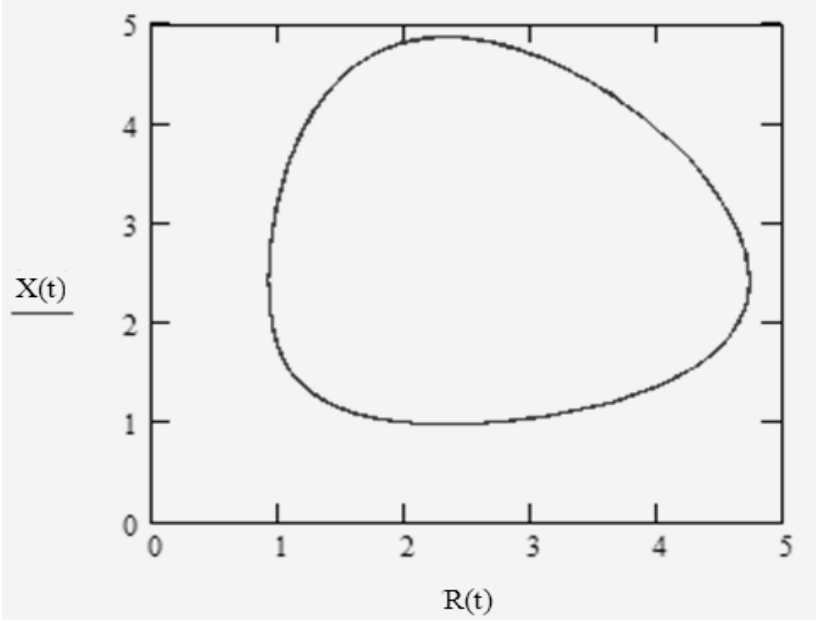


Рис. 3.1. Зависимость количества ВП в РТКС от числа вакцин (трофическая модель)

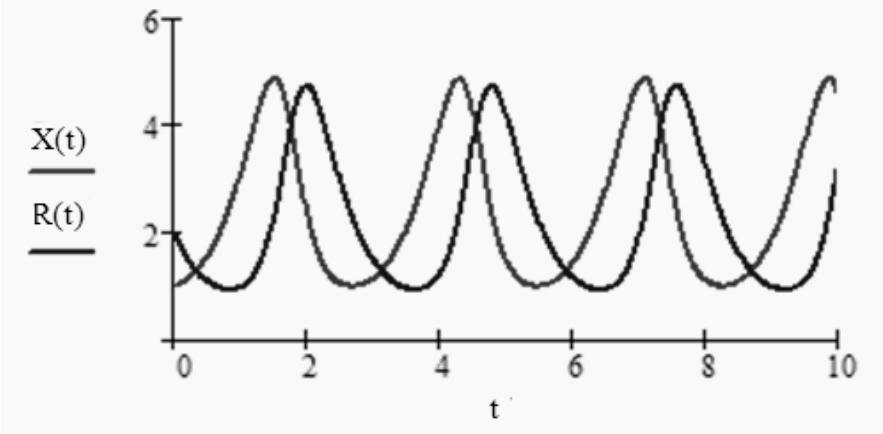


Рис. 3.2. Динамика изменения числа ВП и вакцин в РТКС (трофическая модель)

Такое поведение РТКС практически объясняется следующим образом. При начальном соотношении числа ВП и вакцин 1:2 количе-

ство зараженных компьютеров (и соответственно вредоносных программ) начинает неуклонно расти. Вскоре количество ВП в РТКС начинает превышать число вакцин. Через некоторый промежуток времени количество вакцин начинает увеличиваться. Связано это с реакцией системы на увеличение количества ВП. В определённый момент времени рост численности ВП замедляется (вакцина начинает действовать). В итоге количество ВП сокращается. По достижению определённого значения число вакцин перестаёт расти, и их количество уменьшается с течением времени в связи с сокращением числа ВП в системе. Система возвращается в начальное состояние. А далее всё начинается заново. Этими процессами и объясняется синусоидальная форма кривых изменения численности ВП и вакцин в РТКС с течением времени.

Также объясняется форма зависимости численности ВП от числа вакцин в системе в виде замкнутой кривой. Ее неэллиптичность отражает негармонический характер колебаний. Если бы в начальный момент система находилась в стационарной точке, то количество вредоносных программ и вакцин не изменялось бы с течением времени, т.е. осталось бы постоянным. Остальные начальные состояния приводят к периодическому колебанию решений.

Пример 2. Рассматривается модель (3.13) с использованием поправки на ригидность.

Как видно из графика, представленного на рис. 3.2, процесс изменения численности ВП и вакцин в РТКС носит колебательный характер. Период колебаний и амплитуда постоянны. Однако на практике система стремится к стабильному состоянию, т.е. наблюдается сравнительно постоянное количество ВП и вакцин, несмотря на то что ВП постоянно размножаются. Для того чтобы рассмотреть данный случай, необходимо внести дополнительную переменную для управления затуханием колебаний (коэффициент системной ригидности), что должно привести систему в состояние равновесия.

Модель будет иметь следующий вид:

$$\begin{cases} \dfrac{dx(t)}{dt} = k_1 a x(t) - k_2 r(t) x(t) - \chi x^2(t), \\ \dfrac{dr(t)}{dt} = k_4 b r(t) + k_2 x(t) r(t) - k_3 b r(t) - \chi r^2(t), \end{cases} \tag{3.14}$$

где χ – параметр затухания в системе (коэффициент ригидности).

Моделируется процесс со следующими значениями параметров: $k_1 = 10^8$; $k_2 = 1$; $k_3 = 4 \cdot 10^9$; $k_4 = 3 \cdot 10^9$; $N = 10$; $l_{адр} = 2^{32}$; $v_{скан.ВП} = 10$; $v_{скан.вак} = 1$; $v_{взаим} = 10^{-10}$; $X_0 = 1$; $R_0 = 2$; $\chi = 0.05$ ($a = 2{,}328 \cdot 10^{-8}$; $b = 2{,}428 \cdot 10^{-9}$).

Фазовый портрет системы (рис.3.3) представляет собой кривую, окружающую одну стационарную точку (аттрактор), к которому стремится решение системы уравнений.

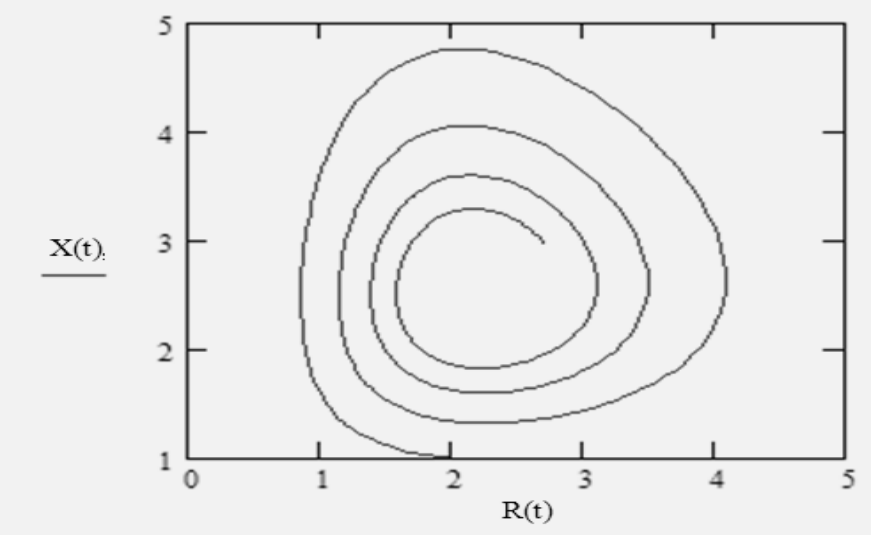


Рис. 3.3. Зависимость количества ВП в РТКС от числа вакцин (трофическая модель с поправкой на ригидность)

Таким образом, можно сделать вывод о том, что количество ВП и вакцин в РТКС будет стремиться к какому-то определённому значению и в конечном счете система придёт в равновесие.

Кривые изменения численности ВП и вакцин представлены на рис. 3.4 в виде затухающих колебаний. Амплитуда колебаний уменьшается. Можно сделать вывод о том, что количество ВП и вакцин в РТКС будет стремиться к какому-то определённому значению и в конечном счете система придёт в равновесие.

Фазовый портрет системы при данном значении χ приобретает устойчивый фокус. Однако при $\chi < 0$ фокус неустойчивый и колебания начинают нарастать. В это время как бы ни было близко начальное состояние к стационарному с течением времени состояние РТКС будет сильно отличаться от стационарного.

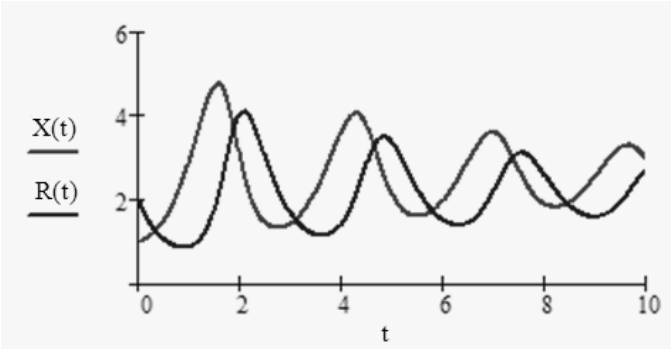


Рис. 3.4. Изменение числа вакцин и ВП (модель с поправкой на ригидность)

Изменение начальных значений *X(t)* и *R(t)* (рис. 3.5 и 3.6) не меняют вид зависимостей изменения числа вакцин и ВП в РТКС. Система также стремится к состоянию равновесия, кривые на графиках с течением времени сохраняют форму синусоиды.

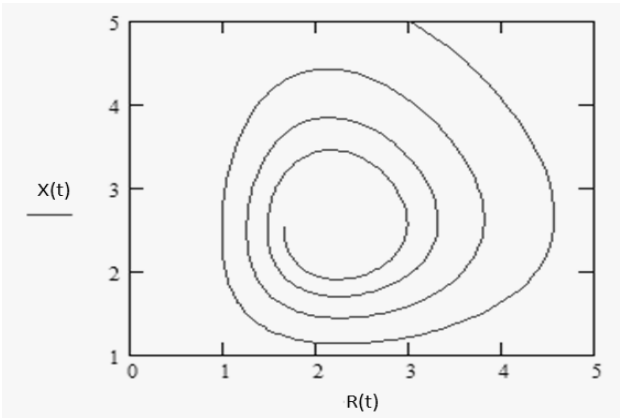


Рис. 3.5. Зависимость количества ВП в РТКС от числа вакцин при $X_0 = 5$, $R_0 = 3$

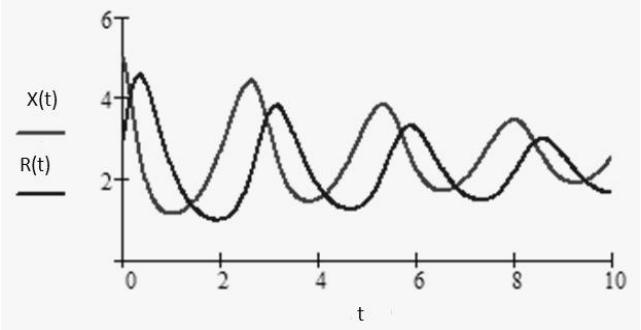


Рис. 3.6. График изменения числа вакцин и ВП в РТКС с течением времени при $X_0 = 5$, $R_0 = 3$

Пример 3. Рассматривается модель (3.14). Изменяются начальные значения коэффициентов k_1 и k_3.

Моделируется процесс со следующими значениями параметров: $k_1 = 10^7$; $k_2 = 1$; $k_3 = 4 \cdot 10^6$; $k_4 = 3 \cdot 10^9$; $N = 10$; $l_{адр} = 2^{32}$; $v_{скан.ВП} = 10$; $v_{скан.вак} = 1$; $v_{взаим} = 10^{-10}$; $X_0 = 1$; $R_0 = 2$; $\chi = 0{,}05$ ($a = 2{,}328 \cdot 10^{-8}$; $b = 2{,}428 \cdot 10^{-9}$).

Графики моделируемого процесса представлены на рис. 3.7 и 3.8.

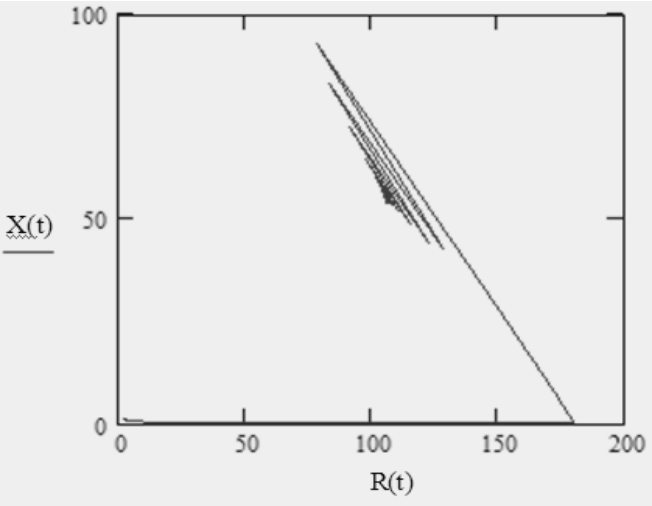


Рис. 3.7. Зависимость количества ВП в РТКС от числа вакцин ($k_1 = 10^7$; $k_3 = 4 \cdot 10^6$)

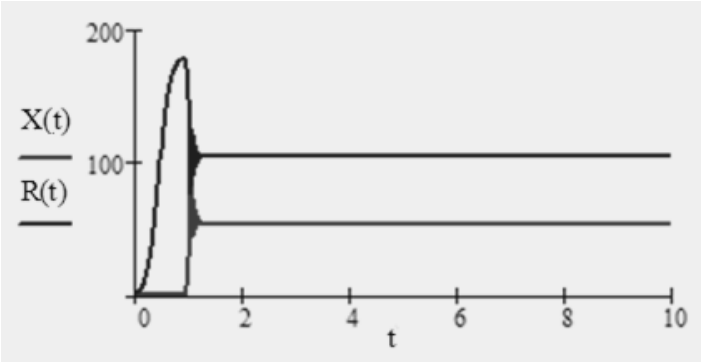


Рис. 3.8. Изменение числа вакцин и ВП в РТКС с течением времени ($k_1 = 10^7$; $k_3 = 4 \cdot 10^6$)

Как мы видим из рис. 3.8, вначале происходит увеличение количества вакцин, связано это с значениями параметров k_3 и k_4. Так как значение k_4 во много раз превосходит значение k_3, то можно судить о том, что число вновь появившихся вакцин во много раз превышает значение вакцин, которые перестали действовать, например, вследствие переустановки операционной системы, либо ошибок в программном обеспечении, или в каких-либо иных случаях.

Далее происходит сокращение численности вакцин в системе. Связано это с соотношением между числом вакцин и вредоносных программ. Так как число вакцин более чем в 100 раз превышает число ВП, можно сказать, что эпидемии ВП нет. Таким образом, число вакцин начинает уменьшаться. Через определённый промежуток времени происходит резкое возрастание числа инфицированных компьютеров, однако вакцины успевают подавить инфекцию. Отсюда можно сделать вывод о том, что если вакцины распространяются быстрее, чем ВП, то можно избежать эпидемии. Таким образом, количество ВП уменьшается, и система стремится к состоянию равновесия, это представлено на рис. 3.7.

Пример 4. Рассматривается модель (3.14). Изменяются значения параметров k_1 k_2 k_3 k_4 .

Моделируется процесс со следующими значениями параметров: $k_1 = 100$; $k_2 = 0.5$; $k_3 = 10^8$; $k_4 = 3 \cdot 10^3$; $N = 10$; $I_{адр} = 2^{32}$; $v_{скан.ВП} = 1$; $v_{скан.вак} = 10$; $v_{взаим} = 10^{-9}$; $X_0 = 1$; $R_0 = 2$; $\chi = 0.05$ ($a = 2.328 \cdot 10^{-8}$; $b = 2.428 \cdot 10^{-9}$).

Графики исследуемого процесса представлены на рис. 3.9 и 3.10. Как видно из графиков, численность ВП и вакцин сокращается с течением времени, однако число вакцин уменьшается с большей скоростью. Таким образом, можно сказать о том, что вакцины не успевают «справиться» со всеми ВП. Количество ВП со временем сокращается, но с очень низкой скоростью. Система стремится к устойчивому состоянию.

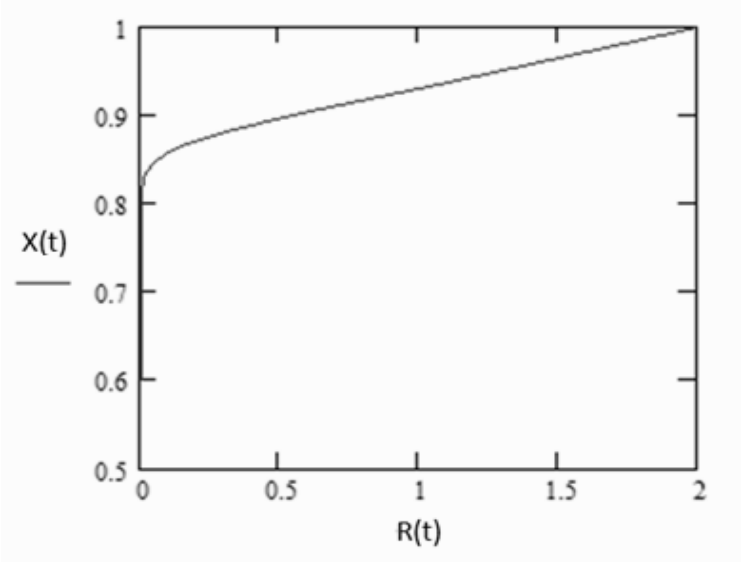


Рис. 3.9. Зависимость количества ВП в РИВС от числа вакцин ($k_1 = 100$; $k_2 = 0{,}5$; $k_3 = 10^8$; $k_4 = 3 \cdot 10^3$)

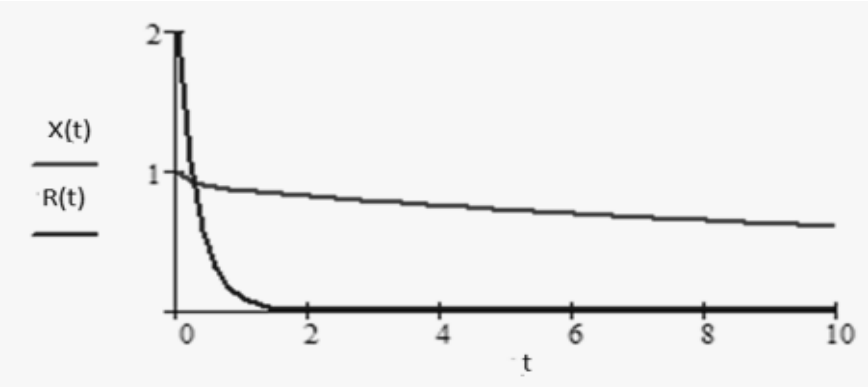


Рис. 3.10. Изменение числа вакцин и ВП в РИВС с течением времени (k_1 = 100; k_2 =0,5; $k_3 = 10^8$; $k_4 = 3 \cdot 10^3$)

Можно сделать следующий вывод: при скорости распространения вакцин в сети, меньшей скорости распространения ВП эпидемии избежать можно, однако количество инфицированных компьютеров будет уменьшаться постепенно с очень малой скоростью. Связано это также с тем, что система стремится к устойчивому состоянию.

Пример 5. Оставим начальные условия такими же, как и в примере 4. Однако резко увеличим k_1.

Графики моделируемого процесса представлены на рис. 3.11 и 3.12. Как видно из графиков, происходит резкое увеличение числа вредоносных программ в РТКС, число вакцин вначале начинает сокращаться, однако после резкого увеличения количества ВП начинает увеличиваться. Вследствие этого сокращается численность вредоносных программ. Однако скорости распространения вакцин недостаточно для того, чтобы справиться с ВП. Система стремится к устойчивому состоянию, к аттрактору, положение которого в центре (рис. 3.11).

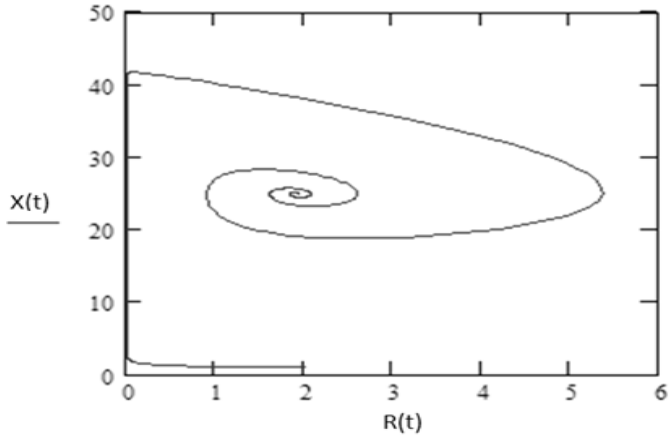


Рис. 3.11. Зависимость количества ВП в РТКС от числа вакцин ($k_1 = 10^9$)

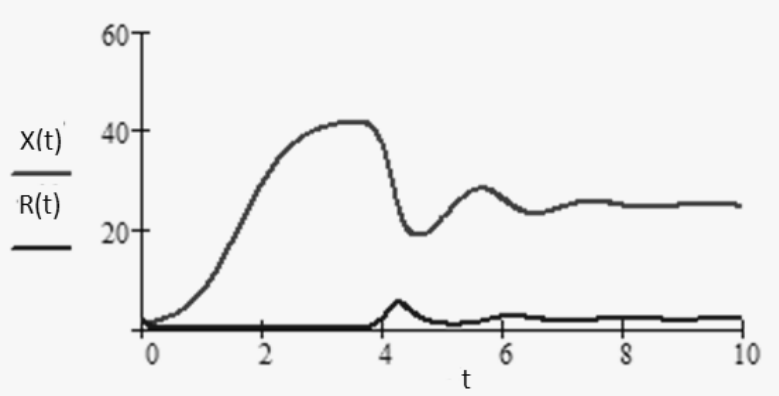


Рис. 3.12. Изменение числа вакцин и ВП в РТКС
с течением времени ($k_1 = 10^9$)

По результатам примеров 1 – 5 сделаем предварительные выводы:

1) процесс изменения численности вакцин и ВП носит колебательный характер. При применении модели с поправкой на ригидность кривые изменения числа ВП и вакцин имеют вид кривой затухающих колебаний;

2) в данной модели основную роль играют коэффициенты k_1 – k_4. Они определяют скорость распространения вакцин и ВП в системе;

3) если скорость распространения вакцин в системе достаточно велика, то гарантированно можно избежать эпидемии.

3.3. Физическая модель противодействия распространению вредоносных программ

Рассмотрим РТКС, состоящую из N компьютеров. В сети распространяется ВП. $N_з$ компьютеров заражены (содержат вредоносную программу).

Заражение будет происходить со скоростью

$$V = V_0 + \alpha t, \tag{3.15}$$

где V – скорость заражения в момент t; V_0 – начальная скорость заражения; α – ускорение заражения.

Заражённые компьютеры будут воздействовать на РИВС с силой

$$F = N_з \alpha. \tag{3.16}$$

Рассматривая F как управляемый параметр, будем исследовать изменение устойчивости РТКС по мере изменения F.

Состояние покоя (устойчивости) РИВС будем оценивать по «неувеличению» числа зараженных компьютеров с течением времени.

Потеря устойчивости связана с возрастанием во времени количества зараженных компьютеров. Графически данный процесс представляет рис. 3.13. θ – степень заражения компьютеров, на графике определяется углом наклона прямой изменения числа заражённых компьютеров к прямой, характеризующей состояние покоя, $0 \le \theta \le \pi / 2$.

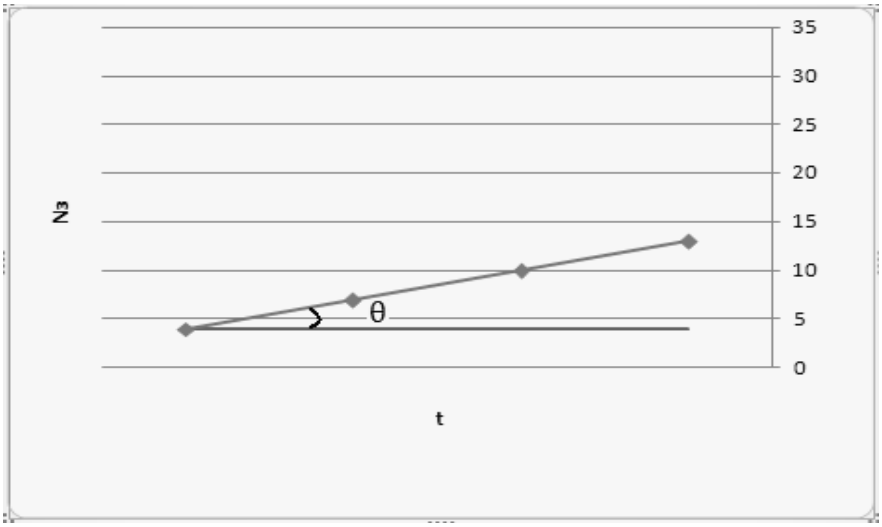


Рис. 3.13. Увеличение числа заражённых компьютеров
в РИВС (физическая модель противодействия)

РТКС противодействует процессу заражения. Пусть в системе возникает противодействующая сила $F_{пр}$, определяемая следующим образом:

$$F_{пр} = a_{пр}(N - N_з), \tag{3.17}$$

где $a_{пр}$ – ускорение противодействия.

Практически противодействующая (заражению) сила определяется операционной системой, типом и способом настройки антивирусной программы, качеством работы системного администратора и администратора безопасности, т.е. техническими и человеческими факторами.

Определим энергию противодействия по формуле

$$E_{пр} = \frac{1}{2} k\theta^2. \tag{3.18}$$

В РТКС изменение числа заражённых компьютеров приводит к изменению степени заражения компьютеров (данное изменение представлено на рис. 3.14). Изменение числа заражённых компьютеров также можно определить по формуле

$$\Delta N_з = N(1 - \cos\theta). \tag{3.19}$$

Общая (потенциальная) энергия системы будет равна

$$V = E_{пр} - F\Delta N_з = \frac{1}{2}k\theta^2 - N(1-\cos\theta). \quad (3.20)$$

Уравнение равновесия будет иметь следующий вид:

$$V' = \frac{dV}{d\theta} = k\theta - FN\sin\theta = 0, \quad (3.21)$$

или

$$F = \frac{k\theta}{N\sin\theta}. \quad (3.22)$$

Устойчивость равновесных состояний определяется по формуле:

$$V'' = \frac{d^2V}{d\theta^2} = k - FN\cos\theta. \quad (3.23)$$

При $\theta = 0$ коэффициент устойчивости будет определяться по формуле $V_f'' = k - FN$. При $V_f'' = 0$, т.е. в критическом состоянии, получаем

$$k = F_c N \quad (3.24)$$

и соответственно

$$F_c = \frac{k}{N}. \quad (3.25)$$

Таким образом, чтобы РТКС находилась в устойчивом состоянии, необходимо выполнение условия $F < F_c$, т.е. равнодействующая сил становится отличной от нуля и будет направлена к положению равновесия.

РТКС будет находиться в состоянии безразличного равновесия, если равнодействующая сил, приложенных к системе, останется равной нулю.

Пример 6. Моделируется процесс противодействия ВП в РТКС. Исходные значения параметров модели: N = 40, $N_з$ = 10, a = 10, $a_{пр}$ = 10, k = 1000.

График, представленный на рис. 3.14, иллюстрирует процесс изменения энергии противодействия РТКС, связанный с возрастанием степени заражения. При отсутствии ВП противодействия нет.

На рис. 3.15 приведен график скорости изменения энергии противодействия.

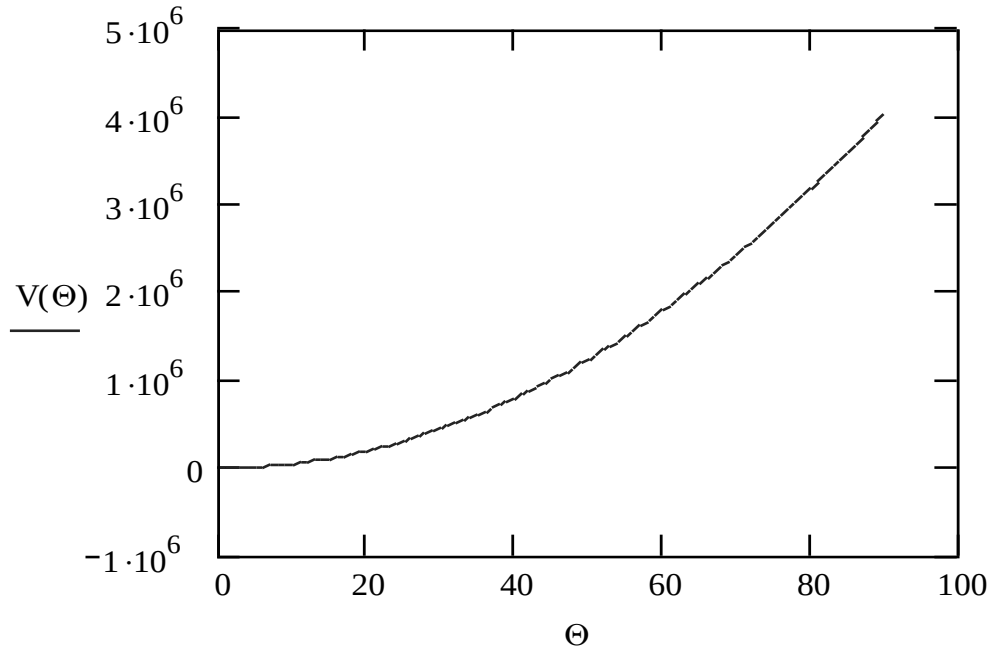


Рис. 3.14. Изменение энергии противодействия от увеличения степени заражённых компьютеров в РТКС (физическая модель $N = 40$; $N_з = 10$; $a = 10$; $a_{пр} = 10$; $k = 1000$)

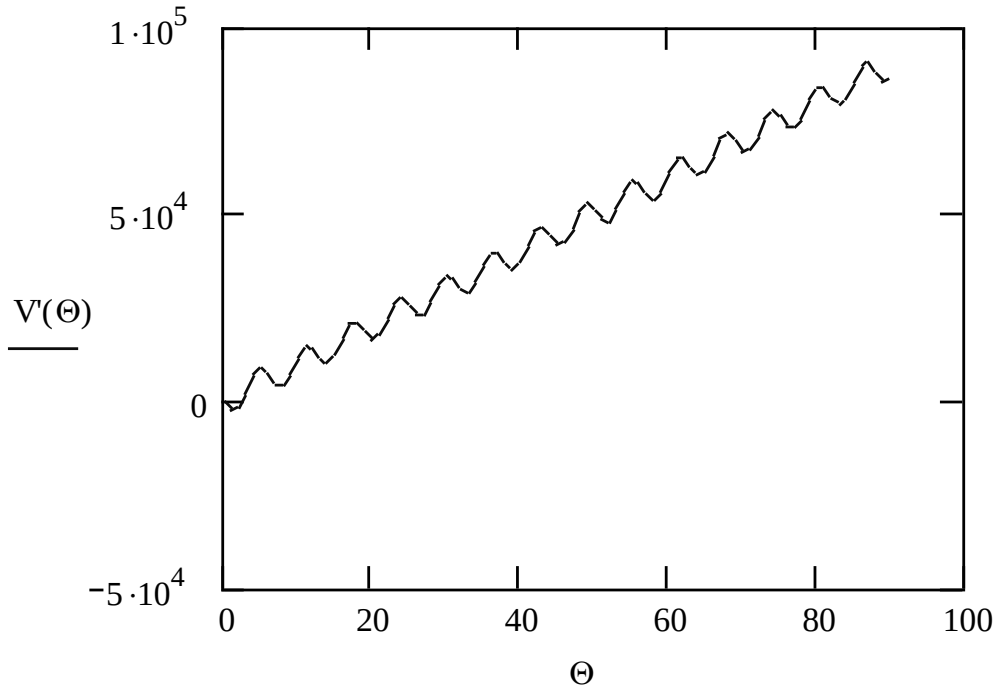


Рис. 3.15. Динамика скорости изменения энергии противодействия РТКС (физическая модель противодействия)

При возрастании числа компьютеров в РТКС кривая *V(θ)* несколько меняет форму (рис. 3.16).

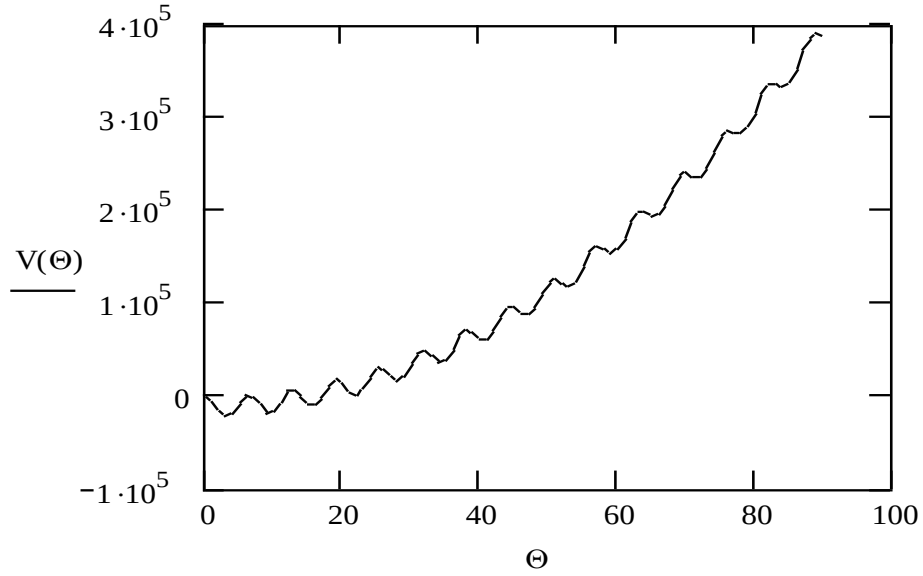


Рис.3.16. Изменение энергии противодействия от увеличения степени заражённых компьютеров при значениях (физическая модель противодействия, N = 114; k = 100)

На графике более отчётливо видны колебания вследствие большего изменения значений производной энергии противодействия (рис. 3.17).

Графики, представленные на рис. 3.18, 3.19, иллюстрируют изменение значения силы воздействия ВП в зависимости от степени заражения компьютеров в РТКС и разных исходных параметров модели.

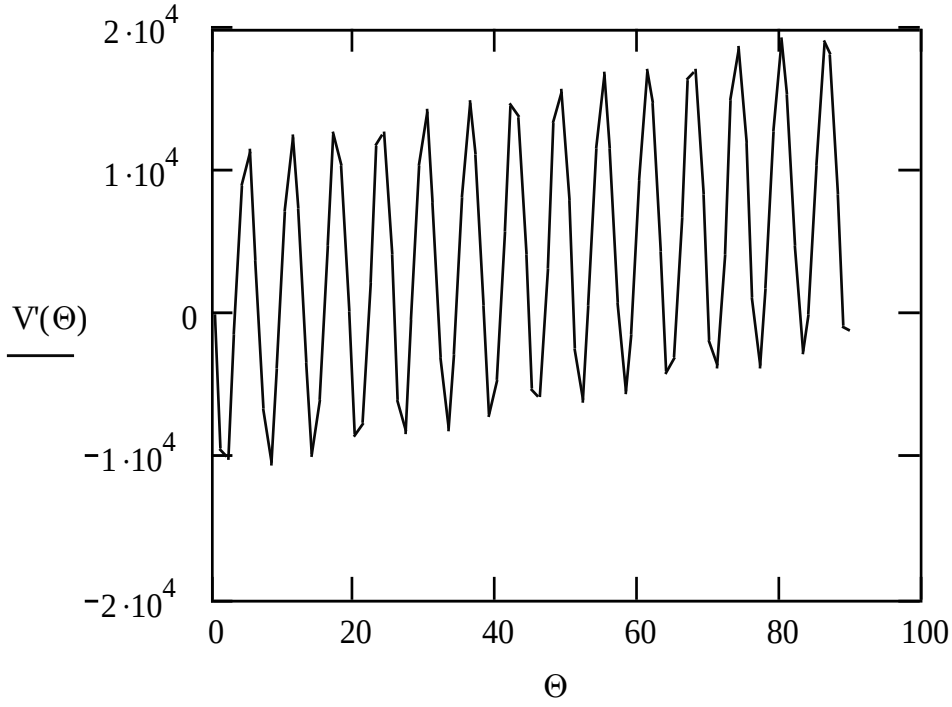


Рис. 3.17. Динамика скорости изменения энергии противодействия РТКС (физическая модель противодействия, N = 114; k = 100)

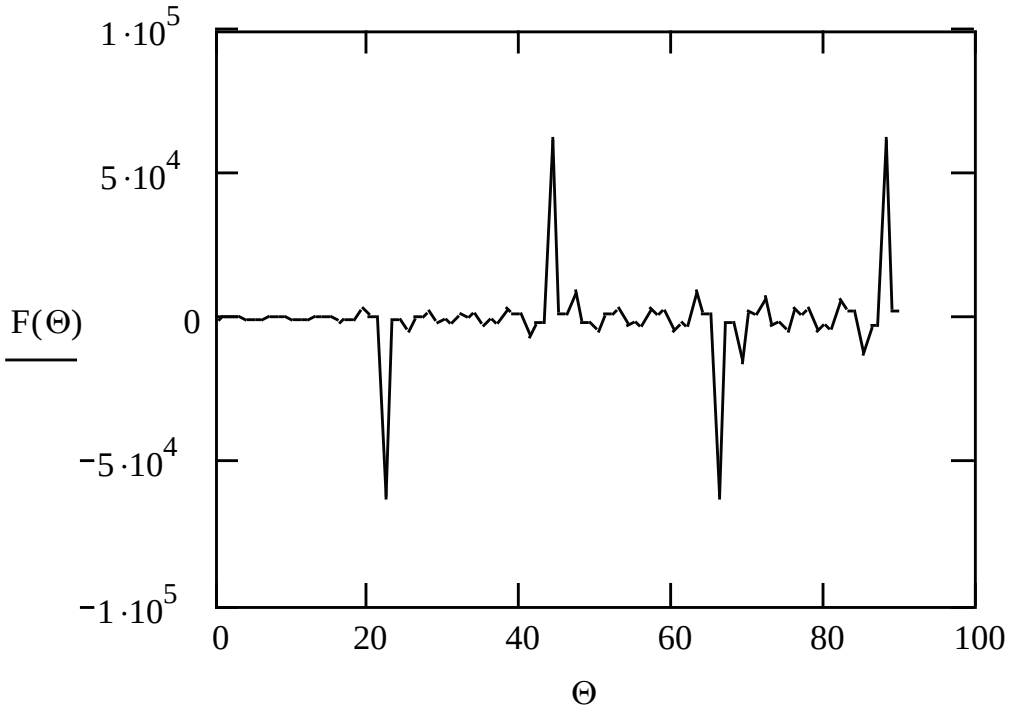


Рис. 3.18. Изменение силы воздействия ВП от степени заражения компьютеров в РТКС (физическая модель противодействия, $N = 40$, $N_з = 10$; $a = 10$; $a_{пр} = 10$; $k = 1000$)

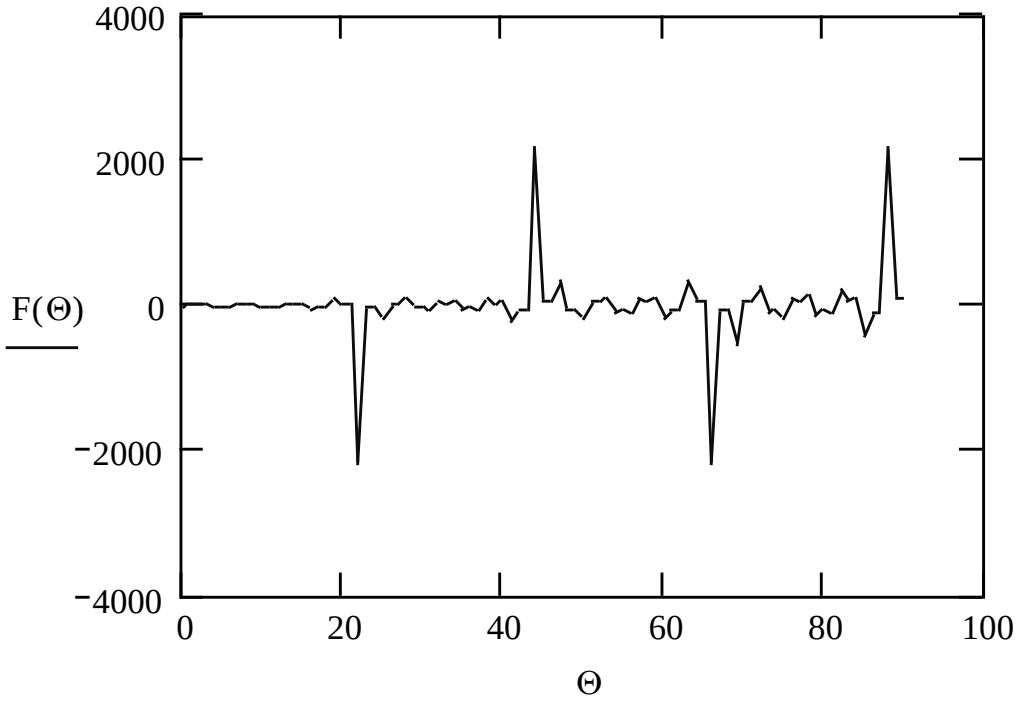


Рис. 3.19. Изменение силы воздействия ВП от степени заражения компьютеров в РТКС (физическая модель противодействия, $N = 114$; $N_з = 10$; $a = 10$; $a_{пр} = 10$; $k = 100$)

Значения силы воздействия, при которых наблюдаются пики (всплески), представлены в таблице.

Точки резкого изменения значения силы воздействия вредоносных программ на компьютеры в РТКС

Степень заражения θ	Сила воздействия вредоносных программ $F(\theta)$	
	$N = 40,\ N_з = 10,\ a = 10,$ $a_{пр} = 10,\ k = 1000$	$N = 114,\ N_з = 10,\ a = 10,$ $a_{пр} = 10,\ k = 100$
22	$-6{,}214 \cdot 10^4$	$-2{,}180 \cdot 10^3$
44	$6{,}214 \cdot 10^4$	$2{,}180 \cdot 10^3$
66	$-6{,}214 \cdot 10^4$	$-2{,}180 \cdot 10^3$
88	$6{,}215 \cdot 10^4$	$2{,}180 \cdot 10^3$

Всплески изменения значения силы наблюдаются с определённым периодом, приблизительно равным 22 для θ. Значения $V(\theta)$ повторяются с периодом, равным 44, а с периодом, равным 22, изменяется знак (с положительного на отрицательный, и наоборот).

Отсюда можно сделать вывод, что поведение (воздействие) ВП в РТКС неоднородно, т.е. их влияние то возрастает, то снижается. Так как это повторяется через определённый промежуток времени, то это даёт потенциальную возможность спрогнозировать следующую (очередную) вспышку активности ВП.

График зависимости F от V'' представлен на рис. 3.20.

На графике видно, что система практически всё время находится в стабильном состоянии и, несмотря на деструктивный потенциал ВП, большую часть времени она не будет испытывать разрушительных воздействий. На данном графике видны пики $F(\theta)$, равные $\pm 6{,}214 \cdot 10^4$. В это время РИВС будет находиться в нестабильном состоянии.

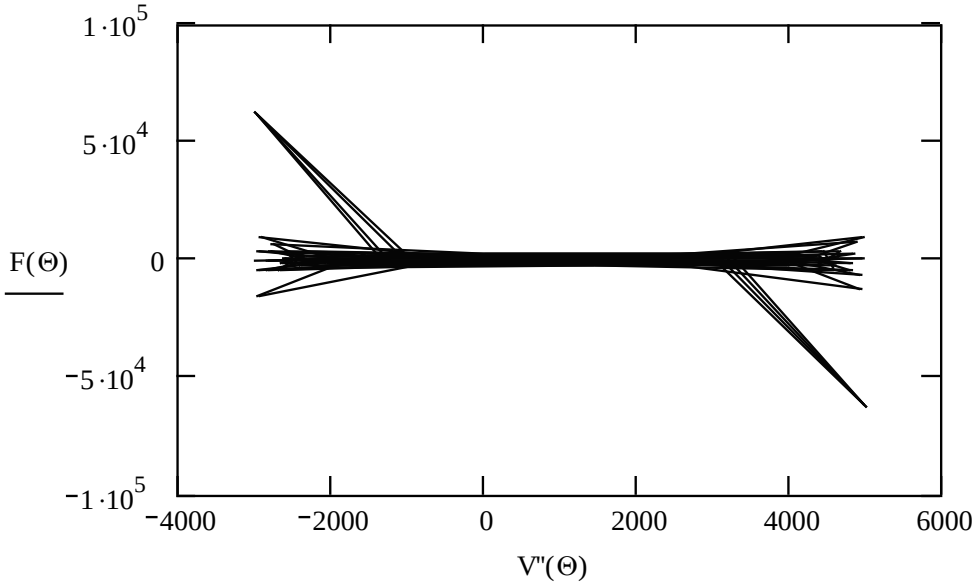


Рис. 3.20. Динамика скорости изменения потенциальной энергии противодействия РИВС в зависимости от силы воздействия заражённых компьютеров (физическая модель противодействия, $N = 40$; $N_з = 10$; $a = 10$; $a_{пр} = 10$; $k = 1000$)

При изменении значений параметров N и k (рис. 3.21) график не изменяет своего вида, по-прежнему наблюдаются четыре пика. Изменяются лишь предельные значения F и V''.

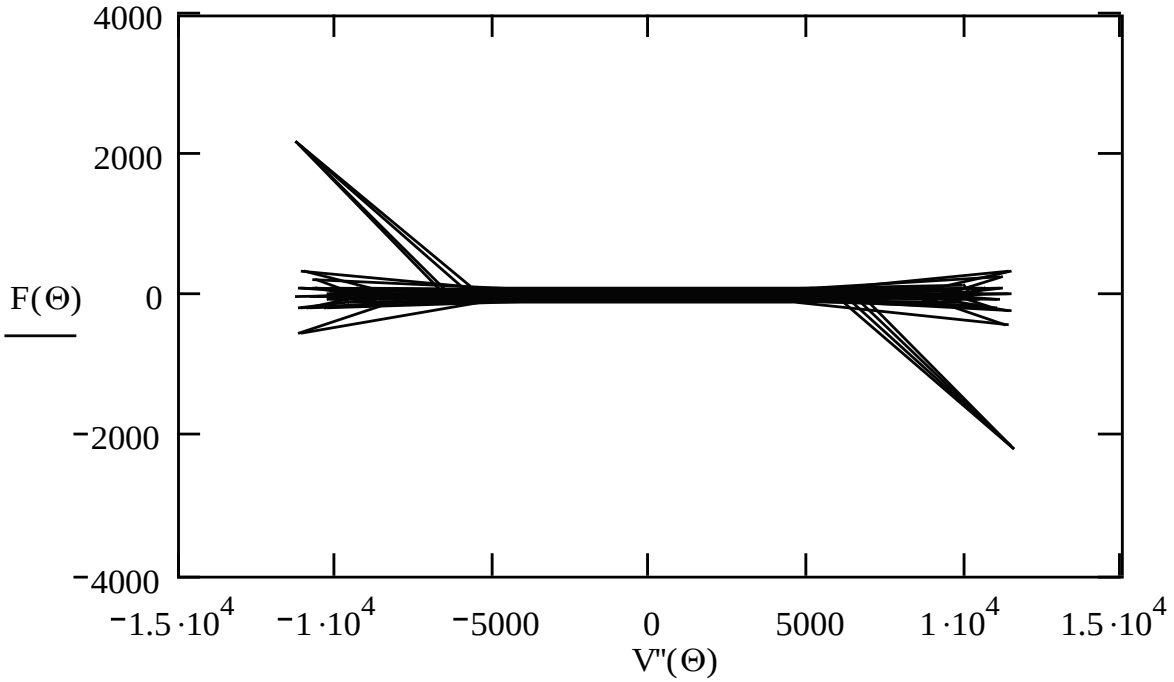


Рис. 3.21. Динамика скорости изменения потенциальной энергии противодействия РТКС в зависимости от силы воздействия заражённых компьютеров (физическая модель противодействия, $N = 114$; $N_з = 10$; $a = 10$; $a_{пр} = 10$; $k = 100$)

Проанализируем динамику скорости изменения потенциальной энергии противодействия в зависимости от скорости изменения силы воздействия заражённых компьютеров в РТКС. Данный график представлен на рис. 3.22. Видно, что энергия изменяется скачками. Если принять во внимание график изменения силы воздействия ВП в зависимости от степени заражения компьютеров, то отчётливо видно, что в период усиления воздействия ВП изменяется и энергия.

Исходя из значений вышеприведенной таблицы, можно сделать вывод о том, что система реагирует на усиление воздействия вредоносных программ. Происходит увеличение изменения энергии противодействия. То есть при резком изменении значения силы резко изменяется значение энергии.

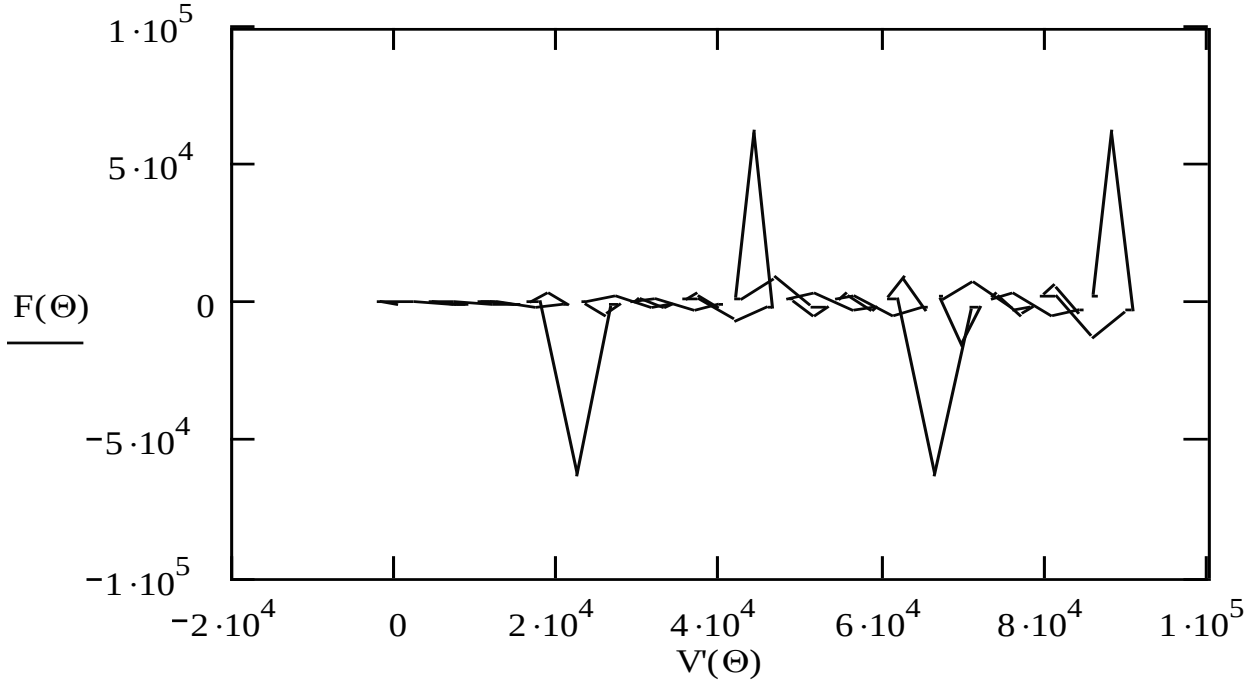


Рис. 3.22. Динамика скорости изменения энергии противодействия в зависимости от скорости изменения силы воздействия ВП в РТКС (физическая модель противодействия, N = 114; $N_з$ = 10; a = 10; $a_{пр}$ = 10; k = 100)

График $V''(\theta_i) = f\{V''(\theta_{i-1})\}$ (т.е. зависимость текущих значений от предыдущих) представлен на рис. 3.23.

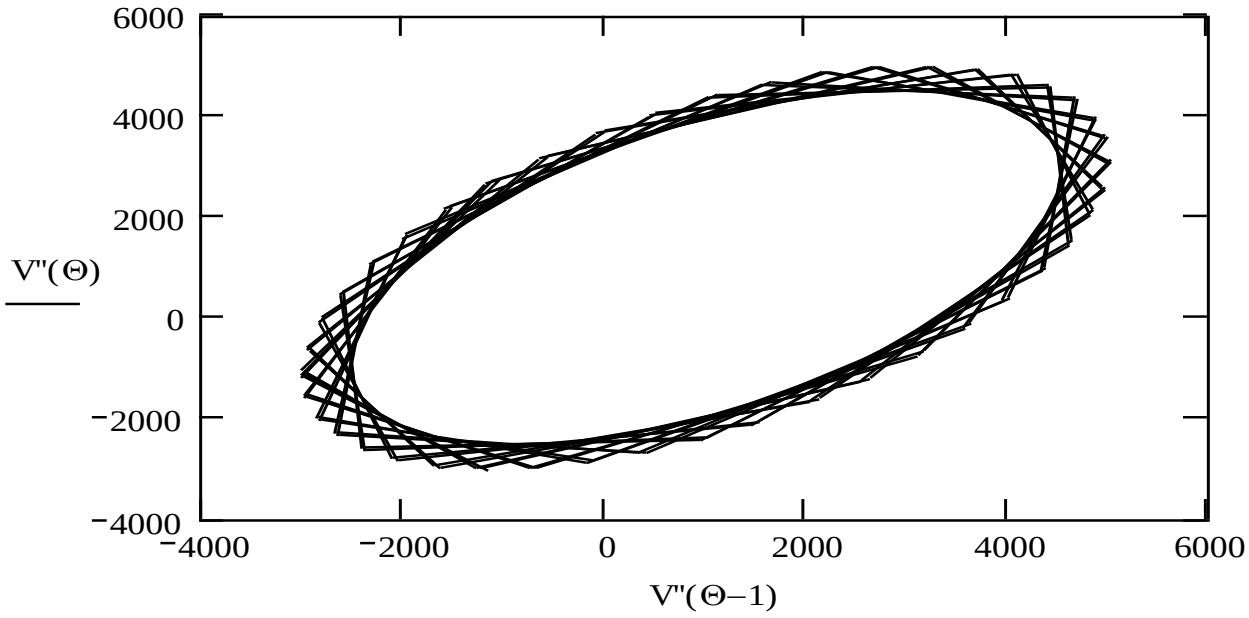


Рис. 3.23. График зависимости значения $V''(\theta_i)$ от $V''(\theta_{i-1})$ (физическая модель противодействия, N = 40; $N_з$ = 10; a = 10; $a_{пр}$ = 10; k = 1000)

При анализе графика можно сделать вывод о том, что система стремится к устойчивому состоянию. Таким образом, возникает определённая проблема: если мы не видим резкого изменения в системе, то становится сложным определение наличия ВП в системе, т.е. вредоносная программа латентизируется.

График, представленный на рис. 3.24, иллюстрирует динамику скорости изменения энергии противодействия в зависимости от скорости изменения энергии в РТКС (второй производной процесса противодействия от первой производной).

На данном графике видно, что при воздействии ВП на систему сначала происходит увеличение ускорения изменения энергии, в связи с чем увеличивается и скорость изменения энергии. Далее ускорение уменьшается и изменяет свой знак, в итоге уменьшается скорость изменения энергии. Далее при очередном воздействии ВП снова увеличивается ускорение изменения энергии. Таким образом система реагирует на каждое воздействие ВП.

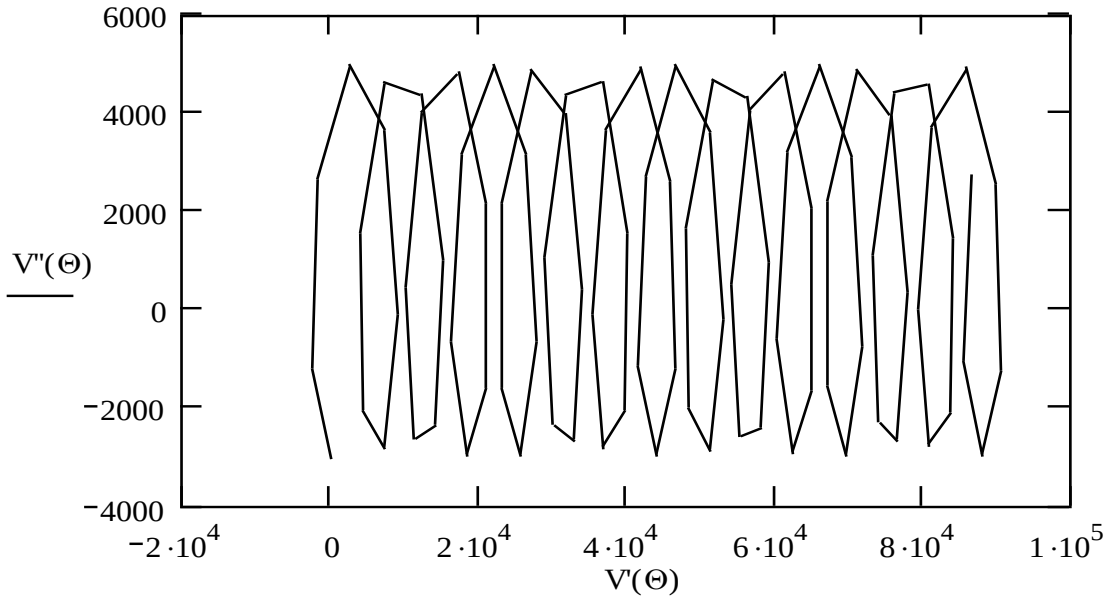


Рис. 3.24. Зависимость значения V'' от V' (физическая модель противодействия, N = 40; $N_з$ = 10; a = 10; $a_{пр}$ = 10; k = 1000)

График зависимости $V'(\theta_i) = f\{V'(\theta_{i-1})\}$ (текущих значений от предыдущих) (рис. 3.25) показывает постоянное изменение скорости изменения энергии в системе. Так как поведение ВП неоднородно (воздействие то увеличивается, то уменьшается), скорость изменения энергии также увеличивается и уменьшается. Система стремится к стабильному состоянию.

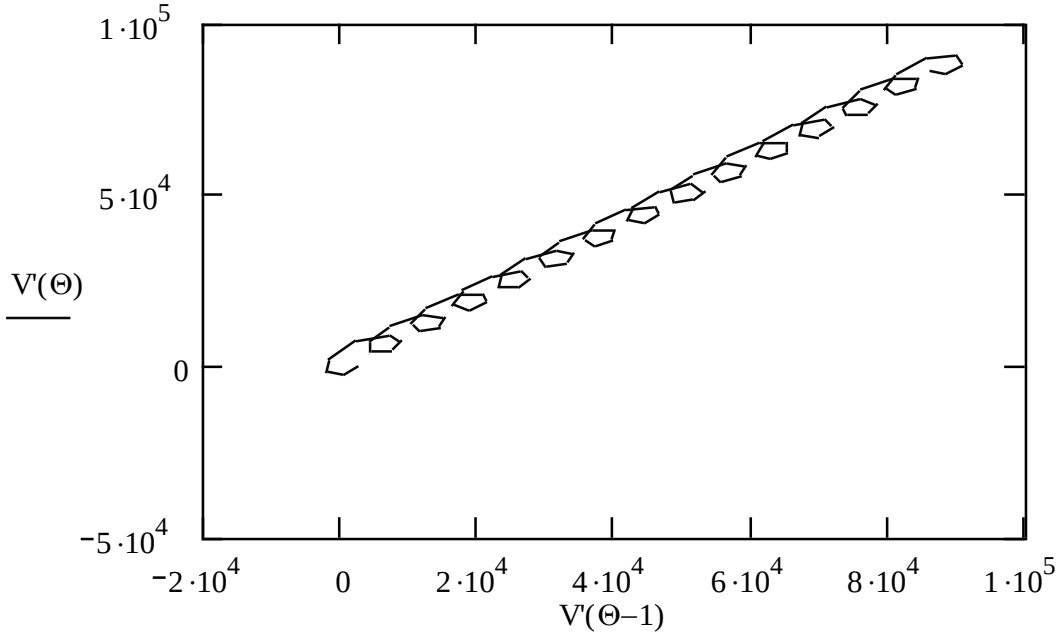


Рис. 3.25. График зависимости значения $V'(\theta_i)$ от $V'(\theta_{i-1})$ (физическая модель противодействия, N = 40; $N_з$ = 10; a = 10; $a_{пр}$ = 10; k = 1000)

При изменении значений исходных параметров модели в связи с тем, что ускорение изменения энергии при данных начальных значениях выше, график (рис. 3.26) несколько изменился. Также наблюдаются изменение скорости энергии в зависимости от воздействия на систему и стремление системы к стабильному состоянию.

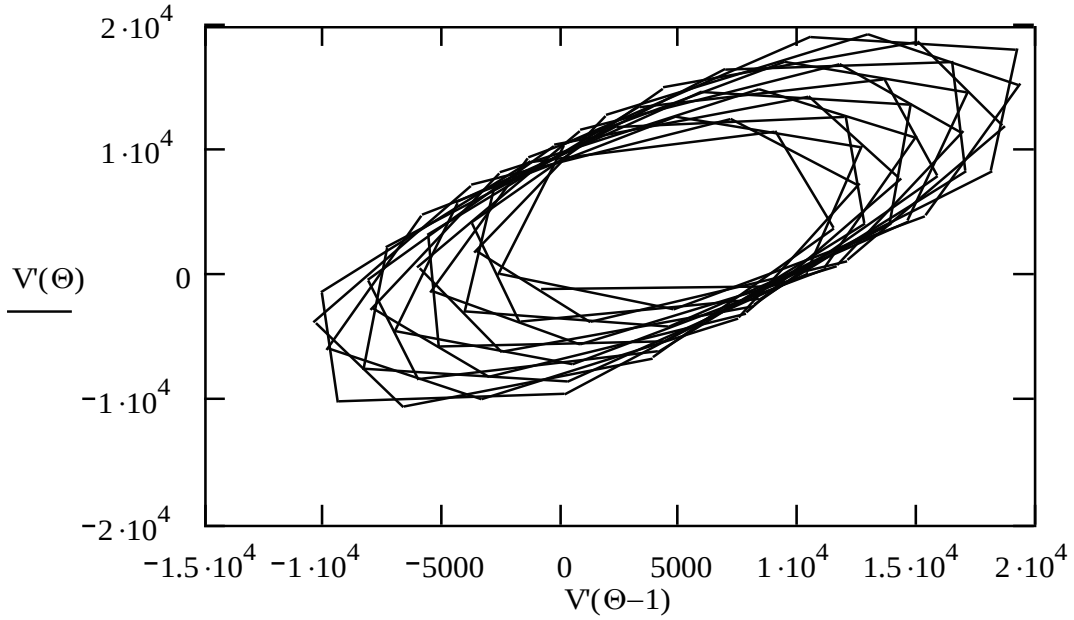


Рис. 3.26. График зависимости значения $V'(\theta_i)$ от $V'(\theta_{i-1})$ (физическая модель противодействия, N = 114; $N_з$ = 10; $a_{пр}$ = 10; k = 100)

Рассмотрим график зависимости $V''(\theta)$ (рис. 3.27).

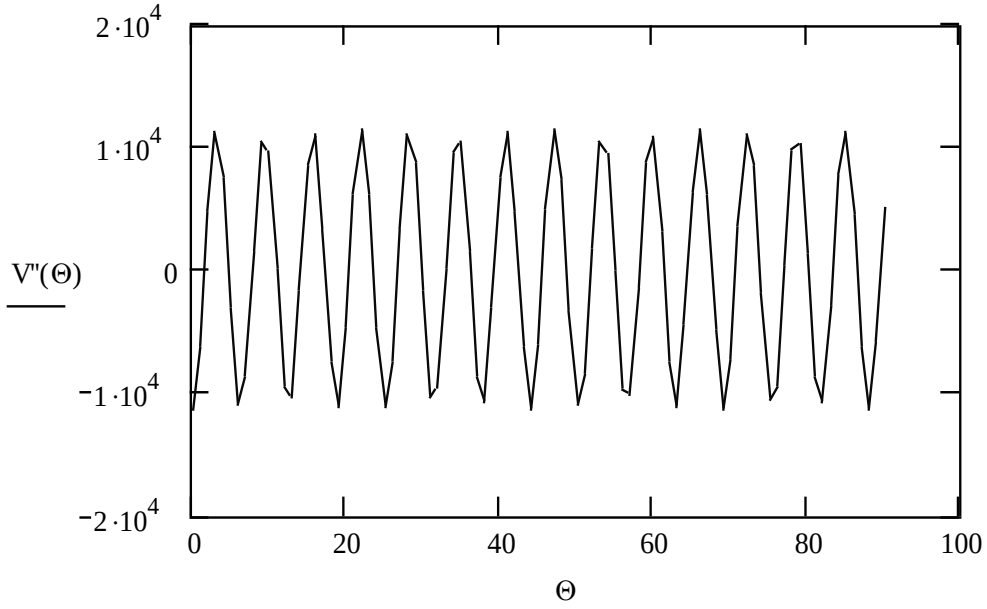


Рис. 3.27. Зависимость ускорения энергии противодействия от степени заражения РТКС (физическая модель противодействия)

Вид кривой близок к виду кривой гармонических колебаний. По мере увеличения деструктивного воздействия вредоносной программы значение $V''(\theta)$ начинает изменяться. Сначала увеличивается, после чего система стремится к стабильному состоянию, и значение $V''(\theta)$ начинает уменьшаться. Происходит это с определённым периодом.

В результате исследования данной модели отчётливо видна возможность прогнозирования всплесков деструктивной активности в РТКС. Их сила и периодичность во многом зависят от типа вредоносной программы и системных характеристик самой РТКС, включая подсистему информационной защиты.

Выводы

Трофическая модель противодействия вредоносным программам, учитывающая характеристики РТКС (включая механизмы информационной защиты) и особенности ВП, позволяет оценить динамику распространения ВП по компьютерам системы, выбрать адекватные атакам механизмы защиты. Процесс изменения численности вакцин и ВП в РТКС носит колебательный характер. При применении модели с поправкой на ригидность кривые изменения числа ВП и вакцин имеют вид кривой затухающих колебаний. Если скорость распространения вакцин в системе достаточно велика, то гарантированно можно избежать эпидемии.

Физическая модель противодействия выявила периодические «всплески» деструктивной активности вредоносных программ в РТКС, что позволяет прогнозировать эпидемии в системе и, следовательно, формировать адекватную информационную защиту.

Глава 4

Исследование призводительности распределенной телекоммуникационной системы в условиях воздействия вредоносных программ

√ Объект исследования – РТКС под воздействием вредоносных программ

√ Аналитические модели оценки производительности

√ Имитационная модель оценки производительности

Рассмотрены аналитические и имитационные модели оценки производительности распределенной телекоммуникационной системы в условиях воздействия вредоносных и антивирусных программ. Предложены методики и алгоритмы расчета локальных временных и безразмерных характеристик производительности. Приводятся результаты экспериментального и модельного исследования влияния вредоносных программ на характеристики распределенной системы

Введение

Анализ производительности распределенной телекоммуникационной системы (РТКС) особенно в условиях вредоносного информационного воздействия, приводящего, возможно, к ее непредсказуемому функционированию, является задачей весьма непростой [1, 15, 33, 46, 62, 74, 82]. Причина тому – усложнение структуры и режимов функционирования РТКС, что затрудняет применение классических методов теории систем массового обслуживания (СМО) ввиду возрастающей размерности решаемых задач.

Одним из возможных путей преодоления противоречия является использование моделей в форме сетей массового обслуживания (СеМО) [12, 14, 32, 73, 74, 78, 81, 95, 105, 106, 116]. СеМО используют для определения системных характеристик, таких как средняя задержка в передаче пакетов сообщений, время доставки пакетов, вероятность потери сообщений и блокировки в узлах, области допустимых значений нагрузки, при которых обеспечивается требуемое качество обслуживания, и др. В качестве моделей протекающих в СеМО процессов наиболее часто используют марковские (экспоненциальные) и полумарковские.

В настоящее время известен ряд теоретических и прикладных работ, посвященных анализу и синтезу РТКС с использованием аппарата СеМО [9, 12, 38, 87 – 89], в них в основном исследуются идеальные сетевые модели. Работ, в которых оценивались бы характеристики производительности в зависимости от типа и интенсивности вредоносного информационного воздействия, практически нет.

Многочисленные эксперименты авторов настоящей монографии по моделированию программных сетевых атак и средств противодействия им [17 – 24, 47 – 52, 54 – 56, 63, 65, 67] показали, что их функционирование в значительной степени ухудшает производительность РТКС, делая иной раз ее вообще неработоспособной. В главе представлена методика, основанная на систематизации характеристик производительности информационно-вычислительных систем аналитического и имитационного моделирования РТКС, функционирующей в условиях воздействия вредоносных программ.

4.1. Объект исследования – РТКС под воздействием вредоносных программ

Любая РТКС обладает двумя важными свойствами – работоспособностью и эффективностью. Работоспособность состоит в правильном выполнении заданных функций, эффективность – в ограниченности или минимальности разного рода затрат. Анализ эффективности осуществляется путём оценки показателей эффективности, т.е. величин, характеризующих затраты на эксплуатацию РТКС.

Показатели, характеризующие затраты времени на получение системой каких-либо полезных результатов, называются показателями производительности. К их числу относятся, например, средние значения времени ответа системы на разные типы запросов, средние числа задач разного типа, решаемых в единицу времени, коэффициенты загрузки устройств РТКС и др.

Многие (если вообще не все) показатели эффективности РТКС могут быть сведены к форме показателей производительности [66]. Имея это в виду, термин «производительность» в настоящей работе будем отождествлять с термином «эффективность».

Эффективность (производительность) РТКС может быть охарактеризована совокупностью параметров и характеристик.

В качестве параметров производительности РТКС выделим: 1) структурные параметры, описывающие ее состав и структуру; 2) функциональные параметры, описывающие стратегию управления передачей данных в системе; 3) нагрузочные параметры, описывающие ее взаимодействие с внешней средой.

Среди характеристик производительности РТКС определим две группы: качественные и количественные. К качественным отнесем ее операционные возможности, масштабируемость и совместимость. Количественные характеристики обычно делят на глобальные (оперативность, живучесть, надёжность, устойчивость) и локальные (описывают эффективность функционирования узлов и каналов связи, узлов обработки данных, отдельных сегментов РТКС), которые, в свою очередь, удобно делить на временные и безразмерные.

Типовые временные локальные характеристики производительности РТКС: время ожидания передачи данных в узлах, время доставки (задержки) сообщения, время ожидания освобождения ресурсов узлов, время пребывания данных в различных узлах и др.

Среди безразмерных локальных характеристик производительности наиболее значимы коэффициенты загрузок узлов и каналов связи, число запросов, находящихся в состоянии ожидания, общее число сообщений, находящихся в узлах, и др.

К вредоносным программам (ВП) относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие заведомый вред компьютерам РТКС.

В силу большого разнообразия не существует единой классификации ВП. Поэтому наиболее удобным для данной работы будет классифицировать ВП по их назначению и способам распространения одновременно, так как это позволит связать их с воздействием на те или иные характеристики производительности РТКС [8, 52]. По такому принципу классификации выделим 4 типа ВП: сетевые черви, классические вирусы, троянские программы, прочие.

1. Сетевые черви – ВП, распространяющие свои копии по локальным и/или глобальным сетям с целью проникновения на удаленные компьютеры, запуска своей копии и дальнейшего распространения на другие компьютеры.

2. Классические вирусы – ВП, распространяющие свои копии по ресурсам локального компьютера с целью последующего запуска своего кода при каких-либо действиях пользователя.

3. Троянские программы – ВП, осуществляющие различные несанкционированные пользователем действия: сбор и передачу информации злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

4. Другие ВП. К данной категории относятся разного вида организаторы DoS атак, флудеры, Spyware- и Adware-программы.

В табл. 4.1 представлена общая статистика воздействия ВП на характеристики РТКС [8].

С целью противодействия негативному воздействию вредоносных программ разрабатывается система информационной защиты, составной частью которой нередко становится антивирусная программа (АП) [99 – 101].

Ее работу в РТКС нельзя оценивать однозначно. Зачастую АП тем или иным образом ограничивает функциональные возможности прикладного программного обеспечения, установленного на ЭВМ. Для эффективной работы АП требуется постоянное обновление ее баз данных, что может создавать дополнительную нагрузку на подсистему передачи данных РТКС. Считается, что среднестатистическая современная антивирусная программа может использовать до 20 % ресурсов компьютера.

Табл. 4.1. *Воздействие ВП на характеристики РТКС*

Воздействие	Процент влияния на характеристики
Потеря производительности	75
Компьютеры были недоступны	69
Повреждения файлов	62
Потеря доступа к файлам	49
Потеря данных	47
Потеря доверия пользователей	33
Закрытие доступа	18
Ненадежность прикладного ПО	13
Трудности с чтением файлов	12
Трудности с сохранением файлов	9
Падение системы	9
Трудности с выводом на печать	7

Влияние на характеристики производительности РТКС разных АП неодинаково. В этом авторы убедились, выполнив экспериментальные исследования по оцениванию влияния различных АП на характеристики производительности ЭВМ.

В качестве испытательного стенда использовался ПК (процессор Intel Core 2 Duo T7600, 2,33 ГГц; память: 2048 Мб, DDR2-533; видео NVIDIA GeForce Go 7600, 256 Мб; жёсткий диск 320 (160 +160 RAID) Гб; дисплей: 17"TFT WUXGA; звуковая карта TruSurround XT, Harman Kardon; оптические устройства HD DVD-RW; порты PCMCIA Type II; 4xUSB 2.0; VGA; S-Video; IEEE 1394. Устройства связи: FM 56K, LAN 10/100, Wi-Fi, Bluetooth, ТВ-тюнер). Программное обеспечение, учитываемое при тестировании Windows XP Media Center Edition, 3DMark05, COSBI OpenSourceMark 1.0 beta 7a, Microsoft Bootvi (измерение времени загрузки ОС).

Перед инсталляцией каждой АП средствами утилиты System Restore производился откат конфигурации ОС в изначальное состояние, а сами тесты прогонялись десятки и сотни раз. Конкретные результаты зависят от конфигурации ЭВМ, но общая тенденция, как правило, сохраняется.

Проводимые тесты:

– измерение времени загрузки ОС средствами утилиты Bootvis;

– измерение времени копирования одиночных файлов разного размера (100 и 1000 Мб) средствами бенчмарк-пакета COSBI OpenSourceMark 1.0;

– оценочный анализ (в баллах) быстродействия системы при выполнении таких операций, как архивирование данных, кодирование мультимедийных файлов в формат MP3 и загрузка веб-страниц, хранящихся на жёстком диске компьютера (для проведения тестов использовался инструмент COSBI OpenSourceMark 1.0).

Результаты экспериментального исследования сведены в табл. 4.2.

Результаты достаточно показательны. К примеру, отчётливо видно, как велико влияние АП на время загрузки ОС: практически все они оттянули ее старт на десять секунд и более. В основном АП оказывают нагрузку на процессор и оперативную память.

Табл. 4.2. *Влияние АП на характеристики ЭВМ*

Антивирусная программа	Время загрузки системы, с	Копирование файла 100 Мб, с	Копирование файла 1000 Мб, с	Сжатие ZIP, балл	Загрузка веб-страниц, балл
Без антивируса	45,62	2,69	25,75	984	1745
Антивирус Касперского 7.0 (настройки по умолчанию)	62,23	2,8	28,14	956	1541
Антивирус Касперского 7.0 (максимальная защита)	63,35	2,4	31,07	964	1525
Trend Micro Internet Sec Pro	58,96	3,15	46	942	1414
Trend Micro Internet Sec Pro (максимальная защита)	57,13	5,05	59,28	775	1424
Dr.Web 4.44 (настройки по умолчанию)	51,63	2,84	41,95	978	1663
Dr.Web 4.44 (макс)	58,28	2,93	42,91	620	1655
Panda Antivirus 2008 (настройки по умолчанию)	55,56	3,03	43,69	946	1705
Panda Antivirus 2008 (макс)	54,84	3,05	43,55	839	1707
Eset NOD32 Antivirus (настройки по умолчанию)	50,82	3,23	41,53	948	1701
Eset NOD32 Antivirus (максимальная защита)	52,11	3,24	41,58	943	1705
avast! 4 Home Edition (настройки по умолчанию)	66,95	3	43,62	937	1665
avast! 4 Home Edition (макс)	70,44	3,23	42,7	926	1668
Norton Antivirus 2008 (настройки по умолчанию)	62,37	3,16	43,56	937	1559
Norton Antivirus 2008 (макс)	73,02	3,4	43	978	1575
Антивирус Stop! 4.10 Pro Edition	46,67	3,4	42,88	941	1699
AVG Anti-Virus 7.5 (настройки по умолчанию)	55,82	3,3	43,14	942	1711
AVG Anti-Virus 7.5	55,7	3,5	43,21	937	1702
CA Anti-Virus 8.1	95,35	3,2	41,91	939	1701

4.2. Аналитические модели оценки производительности

Модель замкнутой системы

Пусть РТКС представляет собой замкнутую сеть из K СМО (рис. 4.1), в которой циркулирует фиксированное число заявок, а внешний их источник отсутствует. N– количество пакетов, циркулирующих в сети, часть из них N^* – пакеты вредоносных программ; $P_R=(p_{ji})$ – маршрутная матрица; m_i – количество обрабатывающих конвейеров в i-м узле; τ_i – среднее время обработки пакета в одном конвейере i-го узла ($\forall i = \overline{1, K}$), зависящее (кроме остальных условий и характеристик обработки) от наличия в данном узе ВП и возможностей противодействия ей.

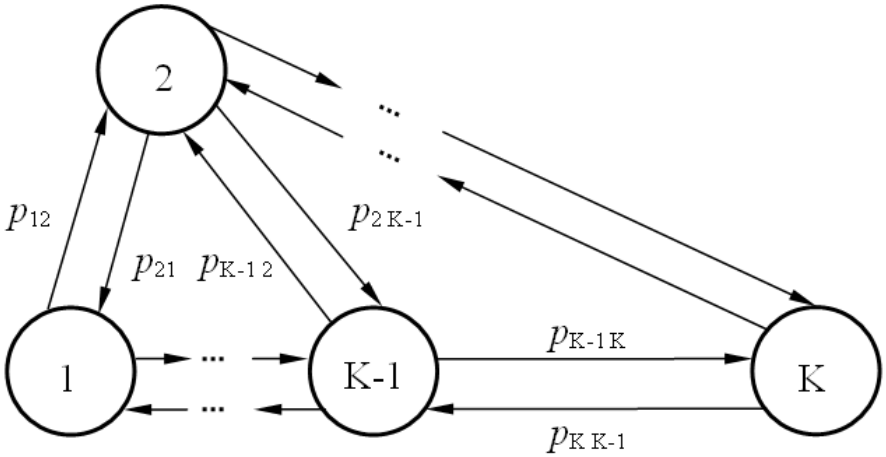


Рис. 4.1. Граф замкнутой сети

Требуется найти все возможные состояния сети в целом и состояния каждого узла в отдельности; рассчитать вероятности этих состояний $P_i(n_i)$; определить характеристики производительности – среднее число пакетов в узле L_i; интенсивности потоков поступающих пакетов λ_i; среднее время пребывания пакета в узле T_i и среднее время цикла V_i.

В общем случае сеть задается стохастической маршрутной матрицей

$$P_R = \begin{pmatrix} p_{11} & p_{12} \dots p_{1K} \\ p_{21} & p_{22} \dots p_{2K} \\ \dots\dots\dots\dots & \\ p_{K1} & p_{K2} \dots p_{KK} \end{pmatrix}, \qquad (4.1)$$

где p_{ij} – вероятность пересылки пакета из i-го узла в j-й узел, причём

$$\sum_{j=1}^{K} p_{ij} = 1 \quad \forall i = \overline{1, K}.$$

В соответствии с подходом, предложенным в [12], обозначим $\lambda_i = e_i \Lambda$ интенсивность потока пакетов, поступающих в i-й узел, где e_i – передаточные коэффициенты, Λ – интегральный сетевой трафик.

Описывая интенсивность потока пакетов ВП пуассоновским процессом с экспоненциальным распределением времени их передачи, учитывая независимость данного потока (в первом приближении) от остальных, положим, что $\lambda_i = \lambda_i^0 + \lambda_i^{ВП}$, где λ_i^0 – интенсивность «полезного» потока, включая интенсивность потока АП (например, обновление баз сигнатур), а $\lambda_i^{ВП}$ – интенсивность вредоносного потока. Учитывая, что $\lambda_i = e_i \Lambda$, получим

$$\lambda_j = \sum_{i=1}^{K} (\lambda_i^0 + \lambda_i^{ВП}) p_{ij} = \sum_{j=1}^{K} (e_j^0 \Lambda^0 + e_j^{ВП} \Lambda^{ВП}) p_{ij}. \qquad (4.2)$$

Для простоты анализа будем считать вредоносный поток постоянным и непревышающим полезный: $\Lambda^{ВП} = \xi \Lambda^0, \xi < 1$, где коэффициент ξ представляет вредоносный поток как часть от полезного.

Таким образом,

$$\begin{aligned} \lambda_j = \sum_{i=1}^{K} (\lambda_i^0 + \lambda_i^{ВП}) p_{ij} &= (1+\xi) \sum_{j=1}^{K} (e_j^0 + e_j^{ВП}) \Lambda^0 p_{ij} = \\ &= \Lambda^0 (1+\xi) \sum_{j=1}^{K} (e_j^0 + e_j^{ВП}) p_{ij}. \end{aligned} \qquad (4.3)$$

Для стационарного режима интенсивность потока, входящего в узел, равна интенсивности исходящего. Составим систему уравнений

$$\lambda_j = \sum_{i=1}^{K} \lambda_i p_{ij} \quad \forall i = \overline{1, K}$$

Учитывая, что $\lambda_i = e_i \Lambda$ и $\lambda_j = e_j \Lambda$, сократим на Λ: $e_j = \sum_{i=1}^{K} e_i p_{ij}$, или в развернутом виде

$$\begin{cases} (p_{11} - 1)(e_1^0 + e_1^{ВП}) + p_{12}(e_2^0 + e_2^{ВП}) + \ldots + p_{K1}(e_K^0 + e_K^{ВП}) = 0, \\ p_{12}(e_1^0 + e_1^{ВП}) + (p_{22} - 1)(e_2^0 + e_2^{ВП}) + \ldots + p_{K2}(e_K^0 + e_K^{ВП}) = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ p_{1K}(e_K^0 + e_K^{ВП}) + p_{2K}(e_2^0 + e_2^{ВП}) + \ldots + (p_{KK} - 1)(e_K^0 + e_K^{ВП}) = 0. \end{cases} \qquad (4.4)$$

Система линейных уравнений (4.4) в матричной форме: $P_1 E = 0$, где матрица P_1 получена путем транспонирования матрицы (4.1) и уменьшением элементов главной диагонали на 1:

$$P_1 = \begin{pmatrix} p_{11}-1 & p_{21} & \dots & p_{K1} \\ p_{12} & p_{22}-1 & \dots & p_{K2} \\ \dots & \dots & \dots & \dots \\ p_{1K} & p_{2K} & \dots & p_{KK}-1 \end{pmatrix} \text{ и } E = \begin{pmatrix} e_1 \\ e_2 \\ \dots \\ e_K \end{pmatrix}.$$

Чтобы получить единственное решение, положим e_1=1. Тогда сложим 1-ю строку матрицы P_1 почленно с $k-$й, где $k = \overline{2, K}$, и получим

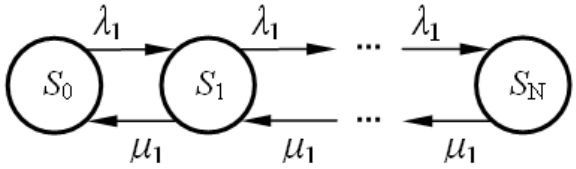
$$P_2 E = Q, \qquad (4.5)$$

где

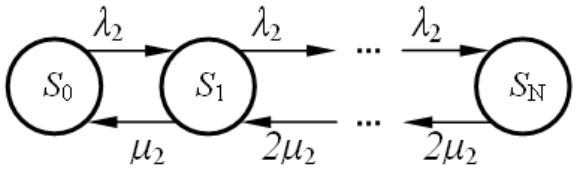
$P_2 = \begin{pmatrix} p_{21}+p_{22}-1 & \dots & p_{K1}+p_{K2} \\ p_{21}+p_{23} & \dots & p_{K1}+p_{K3} \\ \dots & \dots & \dots \\ p_{21}+p_{2K} & \dots & p_{K1}+p_{KK}-1 \end{pmatrix}$ – матрица размерностью $K-1$ и

$Q = \begin{pmatrix} p_{11}-1+p_{12} \\ p_{11}-1+p_{13} \\ \dots \\ p_{11}-1+p_{1K} \end{pmatrix}$.

Применив Метод Гаусса к (4.5), найдем передаточные коэффициенты $e_2, e_3, \dots, e_K$. Рассмотрим узлы замкнутой сети по отдельности (рис. 4.2).



M/M/1



M/M/2

Рис. 4.2. Схемы узлов замкнутой сети

Обозначим $\mu_i = 1/\tau_i$ – интенсивность обработки пакетов в i-м узле, где τ_i – среднее время обработки пакета в i-м узле, распреде-

лённое по экспоненциальному закону $P(t) = \mu e^{-\mu t}$, $t \geq 0$. Среднее время обработки в общем случае зависит от длительности непосредственной обработки пакета в узле (τ_i^0 – расшифровка пакета, формирование запроса к БД и т.п.), от длительности функционирования ВП ($\tau_i^{ВП}$ – запуск своего кода при каких-либо действиях пользователя, «пустое» или «разрушающее» использование ресурсов узла и т.п.) и длительности функционирования АП ($\tau_i^{АП}$ – поиск ВП, противодействие, обновление и т.п.):

$$\tau_i = \Phi(\tau_i^0, \tau_i^{ВП}, \tau_i^{АП}). \qquad (4.6)$$

Вид данной функциональной зависимости не определен. Отметим лишь, что величина τ_i пропорциональна τ_i^0 и имеет тенденцию к увеличению при возрастании $\tau_i^{ВП}$ по сложной динамической нелинейной зависимости. К увеличению длительности обработки в узле ведет и величина $\tau_i^{АП}$, которая в общем плане зависит от интенсивности ВП (т.е., по сути, от $\tau_i^{ВП}$).

Возможные состояния 1-го узла (1 конвейер) $\{S_k\} = \{S_0, S_1, S_2, \ldots, S_N\}$, где k– число пакетов (обрабатывающихся или ожидающих) в узле. Процесс блуждания по этим состояниям будет Марковским процессом гибели и размножения. Вероятность нахождения 1-го узла при стационарном режиме в состоянии S_k обозначим как $P_1(k)$. Выразим вероятности этих состояний через $P_1(0)$:

$P_1(1) = \frac{\lambda_1}{\mu_1} P_1(0)$, $P_1(2) = \frac{\lambda_1^2}{\mu_1^2} P_1(0)$, $P_1(3) = \frac{\lambda_1^3}{\mu_1^3} P_1(0)$ и т.д., причём $\sum_{n=0}^{N} P_1(n) = 1$.

Выражения для числителя получаются перемножением интенсивностей поступления пакетов (размножение), для знаменателя – интенсивностей их обслуживания (гибель). $P_1(0)$ пока остаётся неизвестным.

Рассмотрим 2-й узел с двумя конвейерами. Если в узле 2 конвейера, то узел начинает обрабатывать пакеты с удвоенной интенсивностью (задействованы оба конвейера), когда в нем находится 2 пакета и более.

$P_2(1) = \frac{\lambda_2}{\mu_2} P_2(0)$, $P_2(2) = \frac{{\lambda_2}^2}{2{\mu_2}^2} P_2(0)$, $P_2(3) = \frac{{\lambda_2}^3}{4{\mu_2}^3} P_2(0)$ и т.д., причём $\sum_{n=0}^{N} P_2(n) = 1$.

В общем случае вероятность нахождения i-го узла в состоянии s_k:

$$P_i(n) = \frac{\lambda_i^n}{\mu_i^n \beta_i(n)} P_i(0), \ \forall i = \overline{1, K}, \tag{4.7}$$

где $\beta_i(n) = \begin{cases} n!, n \le m \\ m!\, m^{n-m}, n > m \end{cases}$, m – число конвейеров в i-м узле.

Рассмотрим все возможные состояния сети $\vec{n} = (n_1, n_2, \ldots, n_K)$: $n_1 + n_2 + \ldots + n_K = N$, где n_i – число пакетов в узле. Обозначим множество всех состояний сети как $S(N,K)$. По теореме декомпозиции (Джексона) в стационарном режиме состояние всей сети определяется состоянием её узлов

$$P(\vec{n}) = \frac{\prod_{i=1}^{K} P_i(n_i)}{\sum_{\vec{n}' \in S(N,K)} \prod_{i=1}^{K} P_i(n_i')} \quad \forall \vec{n} = (n_1, n_2, \ldots, n_K) \in S(N,K),$$

где $P_i(n_i)$ – вероятность нахождения i-го узла в состоянии s_{n_i}, а суммирование проводится по всему множеству состояний сети $S(N,K)$. Подставим сюда выражения для $P_i(n_i)$, сократим дробь на $P_1(0), P_2(0), \ldots, P_K(0)$.

Подставляя сюда выражения для λ_i и учитывая, что $n_1 + n_2 + \ldots + n_K = N$, сократим дробь на Λ^N. В результате получаем

$$P(\vec{n}) = \frac{\prod_{i=1}^{K} \frac{e_i^{n_i}}{\mu_i^{n_i} \beta_i(n_i)}}{\sum_{\vec{n}' \in S(N,K)} \prod_{i=1}^{K} \frac{e_i^{n_i'}}{\mu_i^{n_i'} \beta_i(n_i')}} \quad \forall \vec{n} = (n_1, n_2, \ldots, n_K) \in S(N,K). \tag{4.8}$$

Когда все величины известны, можно рассчитать вероятности всех состояний сети $S(N,K)$. Можно убедиться, что

$$\sum_{\vec{n} \in S(N,K)} P(\vec{n}) = 1.$$

Найдём также $P_i(k)$ – все вероятности нахождения каждого i-го узла в состоянии S_k:

$$P_i(k) = \sum_{\substack{\vec{n}' \in S(N,K): \\ n_i' = k}} P(\vec{n}') \quad \forall i = \overline{1, K}, \ \forall k = \overline{0, N}.$$

Здесь суммирование проводится только по тем состояниям из множества $S(N,K)$, для которых в i-м узле находится ровно k пакетов. Убедимся, что $\sum_{n=0}^{N} P_i(n) = 0 \quad \forall i = \overline{1, K}$.

Среднее число пакетов в i-м узле находится как математическое ожидание количества пакетов в i-м узле: $L_i = \sum_{n=0}^{N} n P_i(n) \quad \forall i = \overline{1, K}$.

Можно убедиться, что $\sum_{i=1}^{K} L_i = N.$

Интенсивность λ_i входящего в i-й узел потока в стационарном режиме будет равна интенсивности выходящего потока. Эта величина находится как математическое ожидание интенсивности потока обработанных пакетов: $\lambda_i = \sum_{n=0}^{N} \mu_i(n) P_i(n) \quad \forall i = \overline{1, K}$, где $\mu_i(n)$ – общая интенсивность обработки n пакетов в i-м узле:

$$\mu_i(n) = \begin{cases} n\mu_i, n \le m \\ m\mu_i, n > m \end{cases}, \quad m \text{ – число конвейеров в } i\text{-м узле.}$$

Можно убедиться, что $\frac{\lambda_1}{e_1} = \frac{\lambda_2}{e_2} = \ldots = \frac{\lambda_K}{e_K}$. Теперь среднее время пребывания пакета в i-м узле можно рассчитать по теореме Литтла: $T_i = \frac{L_i}{\lambda_i} \quad \forall i = \overline{1, K}$. Найдём также среднее время цикла V_i – среднее время между моментом выхода пакета из i-го узла до момента первого поступления этого пакета в тот же узел:

$$V_i = \sum_{\substack{j=1 \\ j \ne i}}^{K} \frac{e_j}{e_i} T_j \qquad \forall i = \overline{1, K},$$

где $\frac{e_j}{e_i}$ – среднее число посещений j-го узла между двумя последовательными посещениями i-го узла. Учитывая, что $\frac{\lambda_i}{e_i} = \frac{\lambda_j}{e_j}$, $L_j = T_j \lambda_j$ и $\sum_{\substack{j=1 \\ j \ne i}}^{K} L_j = N - L_i$, получаем $V_i = \frac{N - L_i}{\lambda_i}, \ \forall i = \overline{1, K}.$

Алгоритм расчета характеристик производительности РТКС (замкнутая сеть)

Шаг 1. Задать начальные значения характеристик сети:

1) K – количество узлов в сети;

2) N – количество пакетов, циркулирующих в сети, включая N^* – вредоносные пакеты;

3) маршрутную матрицу P_R;

4) количество обрабатывающих конвейеров в каждом узле: m_1, m_2, …, m_K;

4) среднее время обработки пакета в одном конвейере каждого узла с учетом (4.6): $\tau_1, \tau_2,..., \tau_K$.

Шаг 2. Получить систему линейных уравнений в матричной форме (3.3).

Шаг 3. Применить метод Гаусса к (4.5), найти передаточные коэффициенты $e_2, e_3, \ldots, e_K$.

Шаг 4. Найти множество $S(N,K)$ всех состояний сети.

Шаг 5. Получить возможные состояния $\{S_k\}=\{S_0, S_1, S_2, \ldots, S_N\}$ для каждого узла, где k – число пакетов (обрабатывающихся или ожидающих) в узле и рассчитать вероятности $P_i(n)$ этих состояний.

Шаг 6. Рассчитать среднее число пакетов как математическое ожидание количества пакетов в i-м узле: $L_i = \sum_{n=0}^{N} n P_i(n) \quad \forall i = \overline{1, K}$.

Шаг 7. Рассчитать интенсивность входящего в каждый узел потока с учетом (4.6): $\lambda_i = \sum_{n=0}^{N} \mu_i(n) P_i(n) \quad \forall i = \overline{1, K}$, где $\mu_i(n)$ – общая интенсивность обработки n пакетов в i-м узле: $\mu_i(n) = \begin{cases} n\mu_i, n \le m \\ m\mu_i, n > m \end{cases}$, m – число конвейеров в i-м узле.

Шаг 8. Рассчитать среднее время пребывания пакета в i-м узле: $T_i = \frac{L_i}{\lambda_i} \quad \forall i = \overline{1, K}$. Конец алгоритма.

Пример 1. Рассматривается оценка характеристик производительности РТКС по аналитической модели замкнутой сети. В РИВС каждый узел имеет линию связи с любым другим узлом данной системы (рис. 4.3).

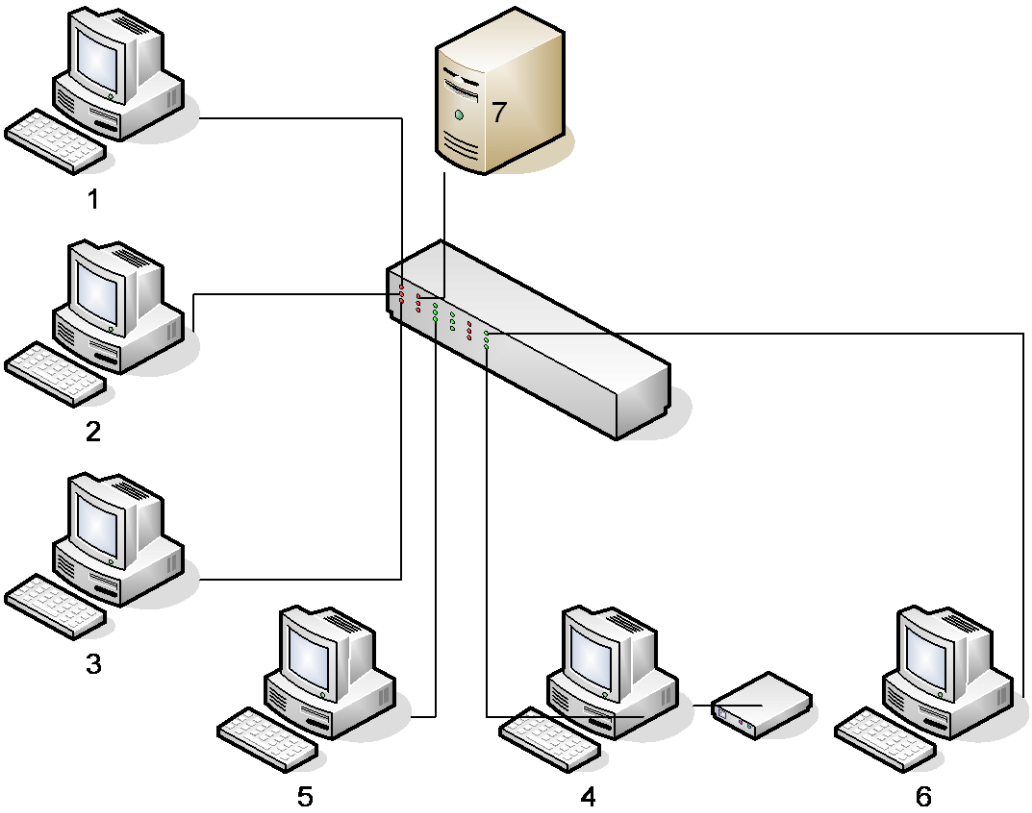


Рис. 4.3. Исследуемая РТКС

Исходные данные: K = 7 (6 персональных компьютеров и сервер); N = 16 (число «полезных» пакетов равно числу «вредоносных» – по 8); маршрутная матрица

$$P_R = \begin{pmatrix} 0,1 & 0,2 & 0,1 & 0,3 & 0 & 0,1 & 0,2 \\ 0,1 & 0,1 & 0,3 & 0,2 & 0,1 & 0,1 & 0,1 \\ 0,2 & 0,1 & 0 & 0,1 & 0,1 & 0,4 & 0,1 \\ 0,1 & 0,2 & 0,1 & 0 & 0,1 & 0,1 & 0,4 \\ 0,1 & 0,1 & 0,1 & 0,1 & 0,4 & 0,1 & 0,1 \\ 0,2 & 0,3 & 0 & 0,1 & 0 & 0,3 & 0,1 \\ 0,2 & 0,1 & 0,1 & 0,1 & 0,2 & 0,2 & 0,1 \end{pmatrix}.$$

m_j = 1; τ_1^0 =0,5ус, τ_2^0 = 0,5ус, τ_3^0 =0,7ус, τ_4^0 =0,7ус, τ_5^0 =1ус, τ_6^0 =1ус, τ_7^0 =0,3ус ($\tau_i^{АП} \approx 0.2\tau_j^0$ – получено экспериментально); ус – условная единица времени – «условная секунда».

А. Моделирование РТКС в условиях отсутствия ВП и АП (табл. 4.3).

Табл. 4.3. *Характеристики производительности РТКС в условиях отсутствия ВП и АП*

Среднее число пакетов в узле	Интенсивность входящего в узел потока, $ус^{-1}$	Среднее время пребывания пакета в узле, ус
$L_1 = 0{,}552$	$\lambda_1 = 0{,}727$	$T_1 = 0{,}759$
$L_2 = 0{,}675$	$\lambda_2 = 0{,}829$	$T_2 = 0{,}815$
$L_3 = 0{,}561$	$\lambda_3 = 0{,}525$	$T_3 = 1{,}069$
$L_4 = 0{,}821$	$\lambda_4 = 0{,}666$	$T_4 = 1{,}232$
$L_5 = 1{,}290$	$\lambda_5 = 0{,}596$	$T_5 = 2{,}167$
$L_6 = 3{,}801$	$\lambda_6 = 0{,}924$	$T_6 = 4{,}111$
$L_7 = 0{,}300$	$\lambda_7 = 0{,}777$	$T_7 = 0{,}386$

Б. Моделирование РТКС под воздействием только ВП (табл. 4.4).

Табл. 4.4. *Характеристики производительности РИВС под воздействием ВП*

Среднее число пакетов в узле	Интенсивность входящего в узел потока, $ус^{-1}$	Среднее время пребывания пакета в узле, ус
$L_1 = 0{,}643$	$\lambda_1 = 0{,}784$	$T_1 = 0{,}820$
$L_2 = 0{,}804$	$\lambda_2 = 0{,}893$	$T_2 = 0{,}900$
$L_3 = 0{,}654$	$\lambda_3 = 0{,}566$	$T_3 = 1{,}156$
$L_4 = 1{,}004$	$\lambda_4 = 0{,}718$	$T_4 = 1{,}399$
$L_5 = 1{,}755$	$\lambda_5 = 0{,}642$	$T_5 = 2{,}734$
$L_6 = 10{,}804$	$\lambda_6 = 0{,}997$	$T_6 = 10{,}842$
$L_7 = 0{,}335$	$\lambda_7 = 0{,}837$	$T_7 = 0{,}400$

В. Моделирование РИВС под воздействием только АП (табл. 4.5) ($\tau_1 = 0{,}625$ ус, $\tau_2 = 0{,}625$ ус, $\tau_3 = 0{,}874$ ус, $\tau_4 = 0{,}874$ ус, $\tau_5 = 1{,}250$ ус, $\tau_6 = 1{,}250$ ус, $\tau_7 = 0{,}375$ ус).

Табл. 4.5. *Характеристики производительности РИВС воздействием только АП*

Среднее число пакетов в узле	Интенсивность входящего в узел потока, $ус^{-1}$	Среднее время пребывания пакета в узле, ус
L_1 = 0,552	λ_1 = 0,582	T_1 = 0,949
L_2 = 0,676	λ_2 = 0,663	T_2 = 1,019
L_3 = 0,561	λ_3 = 0,420	T_3 = 1,334
L_4 = 0,819	λ_4 = 0,533	T_4 = 1,537
L_5 = 1,291	λ_5 = 0,476	T_5 = 2,708
L_6 = 3,802	λ_6 = 0,740	T_6 = 5,140
L_7 = 0,300	λ_7 = 0,622	T_7 = 0,481

Среднее время обработки запроса в узле в условиях отсутствия вредоносных и антивирусных программ составляет приблизительно 1.5 ус, под воздействием только ВП ≈ 2.607 ус, под воздействием только АП ≈ 1.9 ус.

Следовательно, вредоносные программы, число пакетов которых сопоставимо с числом пакетов прикладных и системных программ в РТКС, в отсутствии средств противодействия и не «размножаясь», ведут к падению производительности примерно на 42 %. В отсутствии ВП функционирование антивирусных программ, настроенных на полное выполнение своих функций, производительность РТКС падает приблизительно на 30 %.

Модель незамкнутой сети

Пусть РТКС представляет собой незамкнутую сеть, состоящую из источника пакетов (узел 0) и K СМО M/M/m_1/∞, M/M/m_2/∞, …, M/M/m_K/∞ (рис. 4. 4). Незамкнутая сеть – это такая отрытая сеть, в которую заявки поступают из внешней среды и уходят после обслуживания из сети во внешнюю среду. Другими словами, особенностью незамкнутой СеМО является наличие одного или нескольких независимых внешних источников, которые генерируют заявки, поступаю-

щие в сеть, независимо от того, сколько заявок уже находится в сети. В любой момент времени в открытой СеМО может находиться произвольное число заявок.

Заданы $P_R=(p_{ji})$ – маршрутная матрица, μ_i – средняя интенсивность обработки пакета в одном конвейере i-го узла, λ_0 – интенсивность входящего в сеть потока пакетов. Влияние вредоносных программ и программ, которые им противодействуют, учитывается в соответствии с (4.2) и (4.6) путем нелинейного увеличения соответствующих параметров.

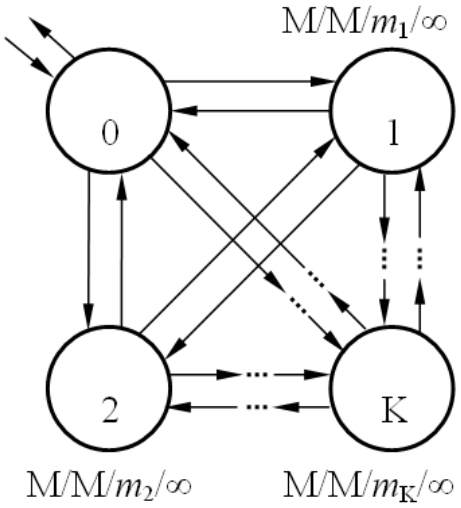


Рис. 4.4. Схема незамкнутой сети

Требуется: найти интенсивности потоков поступающих пакетов λ_i, минимально необходимое число конвейеров в каждом узле m_i, среднюю длину очереди r_i, среднее число пакетов в узле L_i, среднее время пребывания пакета в узле T_i, среднее число пакетов в сети N и среднее время пребывания пакета в сети T.

В общем случае сеть задается стохастической маршрутной матрицей

$$P_R = \begin{pmatrix} 0 & p_{01} & p_{02} & \dots & p_{0K} \\ p_{10} & p_{11} & p_{12} & \dots & p_{1K} \\ p_{20} & p_{21} & p_{22} & \dots & p_{2K} \\ p_{K0} & p_{K1} & p_{K2} & \dots & p_{KK} \end{pmatrix}, \qquad (4.9)$$

где p_{ij} – вероятность пересылки пакета из i-го узла в j-й узел, причём $\sum_{j=0}^{K} p_{ij} = 1 \;\; \forall i = \overline{0, K}$.

Обозначим как $\lambda_i = e_i \lambda_0$ интенсивность потока пакетов, поступающих в i-й узел, где e_i – передаточные коэффициенты.

Для стационарного режима интенсивность потока, входящего в узел, равна интенсивности исходящего. Составим систему уравнений

$$\lambda_i = \sum_{j=0}^{K} \lambda_j p_{ij} \quad \forall i = \overline{0, K}.$$

Учитывая, что $\lambda_i = e_i \lambda_0$ и $\lambda_j = e_j \lambda_0$, получим $e_i = \sum_{j=0}^{K} e_j p_{ij}$, или в развернутом виде

$$\begin{cases} -e_0 + p_{10}e_1 + p_{20}e_2 + \ldots + p_{K0}e_K = 0, \\ p_{01}e_0 + (p_{11} - 1)e_1 + p_{21}e_2 + \ldots + p_{K1}e_K = 0, \\ p_{02}e_0 + p_{12}e_1 + (p_{22} - 1)e_2 + \ldots + p_{K2}e_K = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ p_{0K}e_0 + p_{1K}e_1 + p_{2K}e_2 + \ldots + (p_{KK} - 1)e_K = 0. \end{cases} \quad (4.10)$$

Система линейных уравнений (4.10) в матричной форме: $P_1 E = 0$, где матрица P_1 получена путем транспонирования соответствующей стохастической маршрутной матрицы и уменьшением элементов главной диагонали на 1:

$$P_1 = \begin{pmatrix} -1 & p_{10} & p_{20} & \ldots & p_{K0} \\ p_{01} & p_{11} - 1 & p_{21} & \ldots & p_{K1} \\ p_{02} & p_{12} & p_{22} - 1 & \ldots & p_{K2} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ p_{0K} & p_{1K} & p_{2K} & \ldots & p_{KK} - 1 \end{pmatrix} \text{ и } E = \begin{pmatrix} e_0 \\ e_1 \\ e_2 \\ \ldots \\ e_K \end{pmatrix}.$$

Чтобы получить единственное решение, положим $e_0 = 1$. Тогда сложим 0-ю строку матрицы P_1 почленно с k-й, где $k = \overline{1, K}$ и получим:

$$P_2 E = Q, \quad (4.11)$$

где

$$P_2 = \begin{pmatrix} p_{10} + p_{11} - 1 & \ldots & p_{K0} + p_{K1} \\ p_{10} + p_{12} & \ldots & p_{K0} + p_{K2} \\ \ldots & \ldots & \ldots \\ p_{01} + p_{1K} & \ldots & p_{K0} + p_{KK} - 1 \end{pmatrix} \text{ и } Q = \begin{pmatrix} 1 - p_{01} \\ 1 - p_{02} \\ \ldots \\ 1 - p_{0K} \end{pmatrix}.$$

Применив Метод Гаусса к (4.11), найдем передаточные коэффициенты $e_1, e_2, \ldots, e_K$. Подставим найденные значения e_i в исходную систему и убедимся, что уравнения обращаются в верные равенства.

Теперь можем найти интенсивность потока пакетов, поступающих в i-й узел: $\lambda_i = e_i \lambda_0 \quad \forall i = \overline{1, K}$.

Рассмотрим один из узлов сети (рис. 4.5).

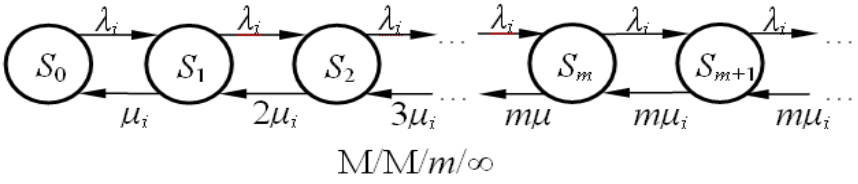


Рис. 4.5. Схема узла сети

Допустим, что он имеет m конвейеров и неограниченную очередь. Возможными состояниями этого узла будут $\{S_k\}=\{S_0, S_1, S_2, \ldots, S_m, S_{m+1}, \ldots\}$, где k – число пакетов (обрабатывающихся или ожидающих) в узле. Процесс блуждания по этим состояниям будет Марковским процессом гибели и размножения. Вероятность нахождения узла при стационарном режиме в состоянии S_k обозначим как $P_i(k)$. Выразим вероятности этих состояний через $P_i(0)$ (табл. 4.6).

Табл. 4.6. *Вероятности нахождения узла в различных состояниях*

n	$P_i(n)$	$r_i(n)$	$k_i(n)$
0	$P_i(n)$	0	0
1	$P_i(0)\frac{\lambda_i}{\mu_i}$	0	1
…	…	…	…
m	$P_i(0)\frac{{\lambda_i}^m}{m!\,{\mu_i}^m}$	0	m
m+1	$P_i(0)\frac{{\lambda_i}^{m+1}}{m!\,m{\mu_i}^{m+1}}$	1	m
m+2	$P_i(0)\frac{{\lambda_i}^{m+2}}{m!\,m^2{\mu_i}^{m+2}}$	2	m
…	…	…	…

Выражения для числителя получаются перемножением интенсивностей поступления пакетов (размножение), для знаменателя – интенсивностей их обслуживания (гибель). В общем случае

$$P_i(n)=\frac{\lambda_i^n}{\mu_i^n\beta_i(n)}P_i(0)\ \forall i=\overline{1,K}, \qquad (4.12)$$

где $\beta_i(n)=\begin{cases}n!, n\le m\\ m!\,m^{n-m}, n>m\end{cases}$, m – число конвейеров в i-м узле.

Учитывая, что $\sum_{n=0}^{\infty}p_i(n)=1$, получим

$$P_i(0)\left(+\frac{\lambda_i}{\mu_i}+\frac{{\lambda_i}^2}{2!\,{\mu_i}^2}+\ldots+\frac{{\lambda_i}^m}{m!\,{\mu_i}^m}+\frac{{\lambda_i}^{m+1}}{m!\,m\mu_i^{m+1}}+\frac{{\lambda_i}^{m+2}}{m!m^2\mu_i^{m+2}}+\ldots\right)=1.$$

Введем обозначения $\rho_i=\frac{\lambda_i}{\mu_i}$ и $\chi_i=\frac{\lambda_i}{m\mu_i}$, тогда

$$P_i(0)\left(1+\rho_i+\frac{\rho_i^2}{2!}+\ldots+\frac{\rho_i^m}{m!}+\frac{\rho_i^{m+1}}{m!m}\left(1+\chi_i+\chi_i^2+\ldots\right)\right)=1.$$

Сумма бесконечной геометрической прогрессии $\left(1+\chi_i+\chi_i^2+\ldots\right)$ будет конечной величиной при условии $\chi_i<1$. Отсюда следует, что число конвейеров m_i в i-м узле следует выбирать как минимальное целое число, удовлетворяющее условию $m_i>\frac{\lambda_i}{\mu_i}\ \ \forall i=\overline{1,K}$, иначе сеть не справится с заданным входящим потоком пакетов. Возвращаясь к $P_i(0)$, получаем

$$P_i(0)=\left(\sum_{n=0}^{m}\frac{\rho_i^n}{n!}+\frac{\rho_i^{m+1}}{m!\,m(1-\chi_i)}\right)^{-1}\ \ \forall i=\overline{1,K}$$, где m – число конвейеров в i-м узле.

Обозначим как $r_i(n)$ длину очереди в i-м узле, находящемся в состоянии S_n. В общем виде $r_i(n)=\begin{cases}0, n\le m\\ n-m, n>m\end{cases}$, где m – число конвейеров в i-м узле.

Средняя длина очереди r_i в i-м узле находится как математическое ожидание $r_i(n)$:

$$r_i=\sum_{n=0}^{\infty}r_i(n)P_i(n)=P_i(0)\frac{\lambda_i^{m+1}}{m!\,m\mu_i^{m+1}}\left(1+2\frac{\lambda_i}{m\mu_i}+\right.$$

$$\left.+3\frac{{\lambda_i}^2}{m^2{\mu_i}^2}+\ldots\right)=P_i(0)\frac{\rho_i^{m+1}}{m!\,m}\left(1+2\chi_i+3\chi_i^2+\ldots\right).$$

Здесь сумма прогрессии $\left(1+2\chi_i+3\chi_i^2+\ldots\right)$ является производной по χ_i суммы прогрессии $\left(\chi_i+\chi_i^2+\ldots\right)$, откуда следует $r_i=P_i(0)\frac{\rho_i^{m+1}}{m!\,m(1-\chi_i)^2}$ $\forall i=\overline{1,K}$, где m – число конвейеров в i-м узле.

Обозначим как $k_i(n)$ число работающих (обрабатывающих пакеты) конвейеров в i-м узле, находящемся в состоянии S_n. В общем виде

$k_i(n) = \begin{cases} n, n \le m, \\ m, n > m, \end{cases}$ где m – число конвейеров в i-м узле.

Среднее число работающих каналов k_i в i-м узле находится как математическое ожидание $k_i(n)$:

$$k_i = \sum_{n=0}^{\infty} k_i(n) P_i(n) = P_i(0) \frac{\lambda_i}{\mu_i} \times \left(1 + 2 \frac{\lambda_i}{2! \mu_i} + 3 \frac{{\lambda_i}^2}{3! {\mu_i}^2} + \ldots \right.$$

$$\left. \ldots + m \frac{{\lambda_i}^{m-1}}{m! {\mu_i}^{m-1}} + m \frac{{\lambda_i}^m}{m! m {\mu_i}^m} + m \frac{{\lambda_i}^{m+1}}{m! m^2 {\mu_i}^{m+1}} + \ldots \right) =$$

$$= P_i(0) \rho_i \left(1 + \rho_i + \frac{{\rho_i}^2}{2!} + \ldots + \frac{{\rho_i}^m}{m!} + \frac{{\rho_i}^{m+1}}{m! m} \left(1 + \chi_i + \chi_i^2 + \ldots \right) \right) =$$

$$= P_i(0) \rho_i \left(\sum_{n=0}^{m} \frac{{\rho_i}^n}{n!} + \frac{{\rho_i}^{m+1}}{m! m (1 - \chi_i)} \right)^{-1} = \rho_i .$$

Получаем $k_i = \rho_i \quad \forall i = \overline{1, K}$.

Среднее число пакетов в i-м узле находится как сумма среднего числа работающих каналов и средней длины очереди: $L_i = k_i + r_i$ $\forall i = \overline{1, K}$.

Среднее время пребывания пакета в i-м узле находится по теореме Литтла: $T_i = \frac{L_i}{\lambda_i} \quad \forall i = \overline{1, K}$. Среднее число циркулирующих в сети пакетов $N = \sum_{i=1}^{K} L_i$. Среднее время пребывания пакета в сети $T = \frac{N}{\sum_{i=1}^{K} \lambda_i}$.

Алгоритм расчета характеристик производительности РТКС (незамкнутая сеть)

Шаг 1. Задать начальные условия:

1) K – количество узлов в сети;

2) N – количество пакетов, циркулирующих в сети, включая N^* – вредоносные пакеты;

3) λ_0 – интенсивность входящего в сеть потока пакетов;

4) маршрутную матрицу P_R;

5) количество обрабатывающих конвейеров в каждом узле: m_1, m_2, …, m_K;

6) среднее время обработки пакета в одном конвейере каждого узла с учетом (4.6): $\tau_1, \tau_2,..., \tau_K$.

Шаг 2. Получить систему линейных уравнений (4.10) в матричной форме.

Шаг 3. Применить метод Гаусса к (4.11), чтобы найти передаточные коэффициенты $e_1, e_2,..., e_K$.

Шаг 4. Найти интенсивности потока пакетов, поступающих в каждый узел: $\lambda_i = e_i \lambda_0 \quad \forall i = \overline{1, K}$.

Шаг 5. Найти число конвейеров m_i – минимальное целое число, удовлетворяющее условию $m_i > \frac{\lambda_i}{\mu_i} \quad \forall i = \overline{1, K}$.

Шаг 6. Рассчитать вероятности $P_i(0)$:

$$P_i(0) = \left(\sum_{n=0}^{m} \frac{{\rho_i}^n}{n!} + \frac{{\rho_i}^{m+1}}{m!\, m(1-\chi_i)} \right)^{-1} \quad \forall i = \overline{1, K}.$$

Шаг 7. Найти:

– загруженности каждого узла по формуле $\chi_i = \frac{\lambda_i}{m\mu_i}$ и среднюю загруженность сети;

– среднюю длину очереди в каждом узле: $r_i = P_i(0) \frac{\rho_i^{m+1}}{m!\, m(1-\chi_i)^2}$ $\forall i = \overline{1, K}$;

– среднее число работающих каналов в каждом узле;

– по теореме Литтла рассчитать среднее время пребывания пакета в i-м узле: $T_i = \frac{L_i}{\lambda_i} \quad \forall i = \overline{1, K}$.

Шаг 8. Определить среднее число циркулирующих в сети пакетов $N = \sum_{i=1}^{K} L_i$ и среднее время пребывания пакета в сети $T = \frac{N}{\sum_{i=1}^{K} \lambda_i}$. Конец алгоритма.

Пример 2. Рассматривается оценка характеристик производительности РИВС (см. рис. 4.3) по аналитической модели незамкнутой сети, в РТКС каждый узел имеет линию связи с любым другим узлом данной системы.

Исходные данные: $K = 7$ (6 персональных компьютеров и сервер); $N = 16$ (число «полезных» пакетов равно числу «вредоносных» –

по 8); $\lambda_0 = 9$ пакетов в условную секунду – интенсивность входящего в сеть потока пакетов, включая и пакеты вредоносной программы; маршрутная матрица

$$P_R = \begin{pmatrix} 0,1 & 0,2 & 0,1 & 0,3 & 0 & 0,1 & 0,2 \\ 0,1 & 0,1 & 0,3 & 0,2 & 0,1 & 0,1 & 0,1 \\ 0,2 & 0,1 & 0 & 0,1 & 0,1 & 0,4 & 0,1 \\ 0,1 & 0,2 & 0,1 & 0 & 0,1 & 0,1 & 0,4 \\ 0,1 & 0,1 & 0,1 & 0,1 & 0,4 & 0,1 & 0,1 \\ 0,2 & 0,3 & 0 & 0,1 & 0 & 0,3 & 0,1 \\ 0,2 & 0,1 & 0,1 & 0,1 & 0,2 & 0,2 & 0,1 \end{pmatrix};$$

$m_1 = m_2 = m_3 = m_4 = m_5 = m_6 = m_7 = 1$; $\tau_1^0 = 0,022$ус, $\tau_2^0 = 0,022$ус, $\tau_3^0 = 0,033$ус, $\tau_4^0 = 0,033$ус, $\tau_5^0 = 0,066$ус, $\tau_6^0 = 0,066$ус, $\tau_7^0 = 0,02$ус ($\tau_i^{АП} \approx 0.2\tau_j^0$ – получено экспериментально); ус – условная единица времени – «условная секунда».

А. Моделирование РТКС в условиях отсутствия ВП и АП (табл. 4.7).

Табл. 4.7. *Характеристики производительности РИВС в условиях отсутствия ВП и АП*

Номер узла	Загруженность узла, %	Средняя длина очереди, пакеты	Среднее время обработки, ус
1	15,985	0,030	0,026
2	7,480	0,006	0,024
3	12,980	0,019	0,038
4	12,211	0,017	0,038
5	26,909	0,099	0,091
6	29,876	0,127	0,095
7	7,399	0,006	0,022

Б. Моделирование РТКС под воздействием только ВП (табл. 4.8).

Табл. 4.8. *Характеристики производительности РИВС под воздействием только ВП*

Номер узла	Загруженность узла, %	Средняя длина очереди, пакеты	Среднее время обработки, ус
1	47,955	0,442	0,043
2	22,439	0,065	0,029
3	38,941	0,248	0,055
4	36,633	0,212	0,053
5	80,726	3,381	0,346
6	89,628	7,745	0,643
7	22,198	0,063	0,026

В. Моделирование РТКС под воздействием только АП (табл. 4.9).

Табл. 4.9. *Характеристики производительности РТКС под воздействием только АП*

Номер узла	Загруженность узла, %	Средняя длина очереди, пакеты	Среднее время обработки, ус
1	19,981	0,050	0,035
2	9,350	0,010	0,031
3	12,980	0,019	0,038
4	12,211	0,017	0,038
5	33,636	0,170	0,126
6	37,345	0,223	0,133
7	9,249	0,009	0,028

Средняя длина очереди в условиях отсутствия ВП и АП 0.043 пакета, под воздействием только ВП – 1,737 пакета, под воздействием только АП – 0,071 пакета. Следовательно, под воздействием вредоносных программ, число пакетов которых сопоставимо с числом пакетов прикладных и системных программ в РИВС, средняя длина очереди в рассматриваемой РИВС увеличилась примерно в 40 раз, а под воздействием АП – примерно на 65 %.

Среднее время обработки запроса в узле в условиях отсутствия ВП и АП составило 0,047 ус, под воздействием только ВП – 0,17 ус,

под воздействием только антивирусных программ – 0,06 ус. Следовательно, под воздействием ВП среднее время обработки запроса увеличивается более чем в 2,5 раза, а под воздействием АП – на треть.

Согласно анализу данных, полученных в результате изучения состояния РТКС под воздействием только ВП, стохастический характер маршрутной матрицы, описывающей систему, может стать причиной нелинейного роста характеристик производительности в некоторых узлах сети, несмотря на то что загрузка узлов будет расти линейно. Такое явление может приводить к сбоям в работе РТКС.

4.3. Имитационная модель оценки производительности

Аналитические методы не всегда применимы для решения практических задач. Например, выдвигается предположение о простейшем потоке заявок (для разных фаз обслуживания он может быть непростейшим), однотипных устройствах и т.д. В имитационном моделировании [2, 42, 72, 97, 111, 113] большинство ограничений снимаются (например, могут использоваться произвольные законы распределения для описания временных параметров, различные схемы, дисциплины обслуживания и т.д., объекты исследуется необязательно в стационарном режиме (например, возможно изучение переходного режима, когда показатели отличаются от асимптотических значений).

В состав исследуемой РТКС (рис. 4.6) входят 4 рабочих станции (РС), сервер и сетевой коммутатор. Имеется связь с внешней локальной сетью и Интернет.

Работа РИВС формализуется в виде СМО с ограниченной очередью. Поток заявок распределен по закону Пуассона с интенсивностью λ (увеличивается при воздействии ВП), время обработки заявки распределено экспоненциально, интенсивность обработки μ (увеличивается при воздействии АП).

Моделируемый процесс – передача пакетов (заявок) от РС к серверу РТКС. Его параметры: единица времени – 1 ус (условная секунда); размер пакета 100 Мбайт; пропускная способность канала связи 100 Мбит/ус (задержка на передачу пакета по каналу связи 8 ус); РС генерируют пакеты для отправки серверу (табл. 4.10); количество обрабатывающих каналов сервера 3; емкость накопителя пакетов, поступивших на обработку, 5 (если все каналы заняты, то пакеты

встают в очередь на обработку, если очередь заполнена, то пакет получает отказ в обслуживании); время обработки пакета в сервере 110 ус.

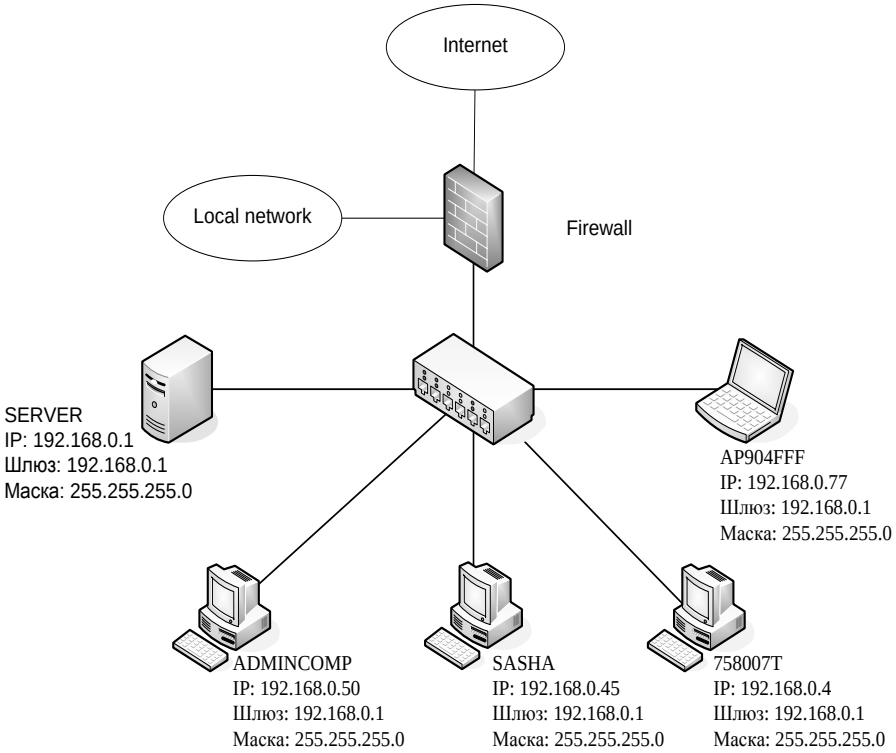


Рис. 4.6. Структура исследуемой РИВС

Табл. 4.10. *Средние интервалы времени генерации пакетов рабочими станциями*

Рабочая станция	Интервал времени, ус
PC1	23 ± 3
PC2	30 ± 2
PC3	25 ± 4
PC4	40 ± 6

Кроме того, определены изменения параметров СМО при моделировании воздействия ВП на характеристики РИВС: количество генерируемых пакетов увеличивается на 69 % (табл. 4.11); задержка на обработку пакетов сервером увеличивается на 75 %; время обработки пакета в сервере с учётом данного влияния равно 192,5 ус; возможность доступа пакетов к серверу уменьшается на 18 %, емкость накопителя пакетов с учётом данного влияния – 4.

Табл. 4.11. *Средние интервалы времени генерации пакетов РС с повышенной частотой генерации*

Рабочая станция	Интервал времени, с
PC1	7,13 ± 1
PC2	9,3 ± 0,6
PC3	7,75 ± 1,25
PC4	12,4 ± 1,85

Для имитационного моделирования воздействия АПО на характеристики РИВС экспериментально исследовались три программных продукта: антивирус Касперского 7.0; Dr.Web 4.44; Avast! 4 Home Edition [99 – 101]. В результате были определены изменения параметров РТКС под воздействием АПО (табл. 4.12): ухудшается пропускная способность канала (задержка на передачу пакета по каналу связи увеличивается), уменьшается производительность системы (задержка на обработку пакетов сервером увеличивается).

Табл. 4.12. *Изменение параметров РТКС под воздействием АПО*

Антивирусная программа	Задержка на обработку пактов, ус	Ухудшение пропускной способности канала связи, %	Задержка на передачу пакетов, ус
Антивирус Касперского 7.0	152,75	12,6	9
Dr.Web 4.44	140,5	5,15	8,4
Avast! 4 Home Edition	170	4,4	8,35

Процесс моделирования облегчает построение графической схемы имитационной модели (рис. 4.7), которая отображает логику взаимодействия блоков модели.

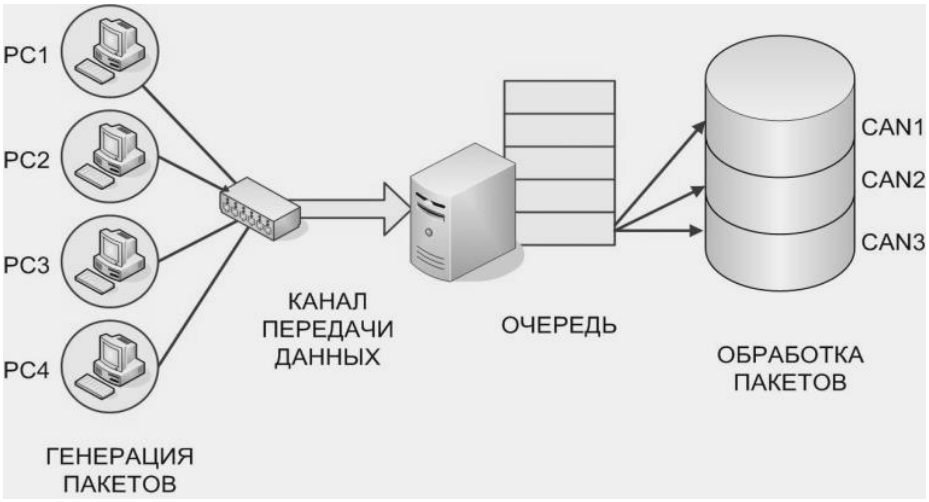


Рис. 4.7. Схема функционирования имитационной модели

Прогон модели с разными входными данными в программной среде GPSS World [39, 84, 87] позволяет получить статистические результаты, которые выводятся в виде стандартных отчётов и могут быть представлены в виде графиков и гистограмм.

В отчеты об экспериментах (рис. 4.8) включены основные показатели моделирования системы:

– о каналах обрабатывающего устройства (FACILITY) с условными именами CAN1, CAN2 и CAN3: ENTIRES – количество пакетов, прошедших через устройство, UTIL – коэффициент использования устройства, AVE._TIME – среднее время обработки одного пакета в устройстве, AVAIL – состояние готовности устройства в конце периода моделирования, OWNER – номер последнего пакета, занимавшего устройство, PEND – количество пакетов, ожидающих устройство, находящееся в режиме прерывания, INTER – количество пакетов, прерывающих устройство в данный момент, RETRY – количество пакетов, ожидающих специальных условий, зависящих от состояния устройства, DELAY – количество пакетов, ожидающих занятия или освобождения устройства;

– очереди (QUEUE) заявок на обработку с условным именем LINE1: MAX - максимальное содержимое очереди в течение периода моделирования, CONT – текущее содержимое очереди в конце периода моделирования, ENTRIES – общее количество входов в накопитель, ENTRIES(0) – общее количество входов в очередь с нулевым временем ожидания, AVE.CONT – среднее значение содержимого

очереди, AVE.TIME – среднее время, проведенное в очереди с учетом всех входов в очередь, AVE.(–0) – среднее время, проведенное в очереди без учета «нулевых» входов в очередь, ETRY – количество транзактов, ожидающих специальных условий, зависящих от состояния очереди.

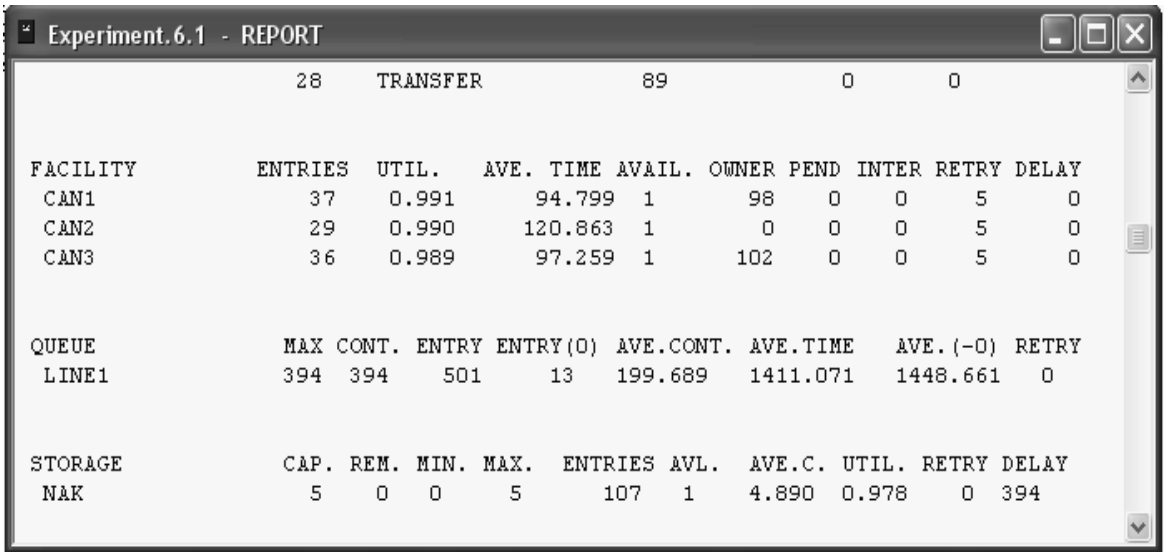


Рис. 4.8. Вывод результатов моделирования

На рис. 4.9 – 4.17 представлены гистограммы результатов моделирования, где Mean – среднее значение исследуемого параметра; S.D. – среднее квадратическое отклонение.

Ход моделирования

А. Моделирование РИВС в условиях отсутствия ВП и АП

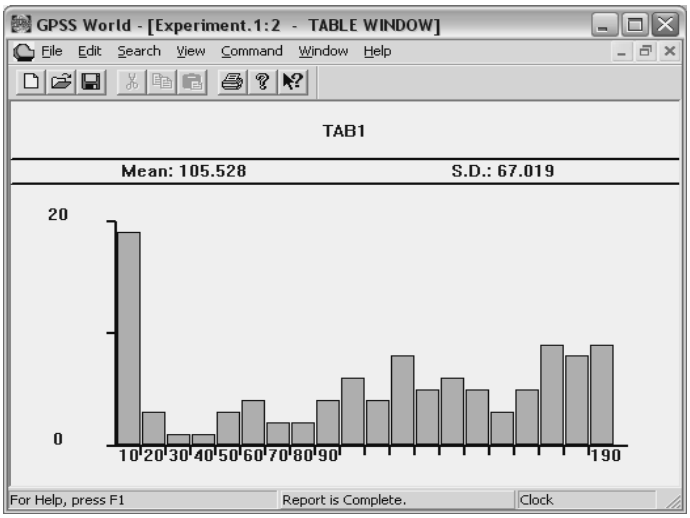


Рис. 4.9. Среднее количество пакетов в очереди

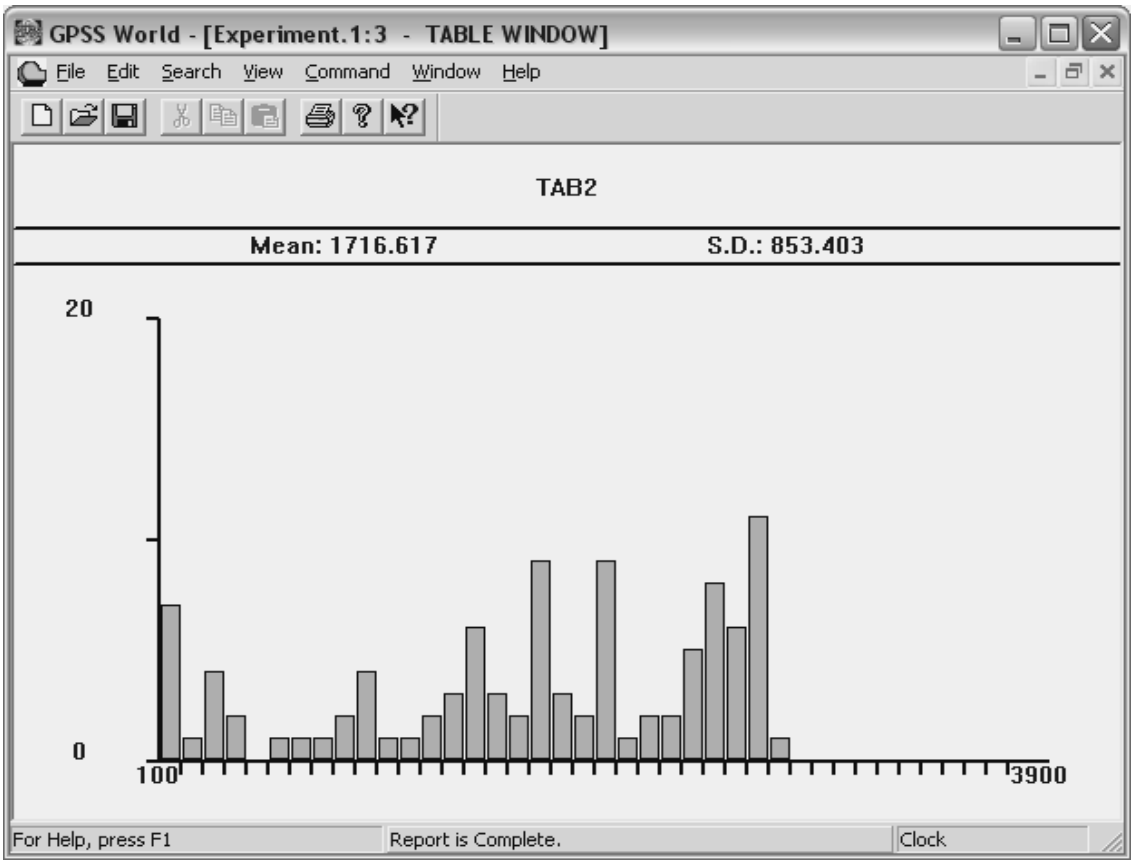


Рис. 4.10. Средняя продолжительность пребывания пакета в системе

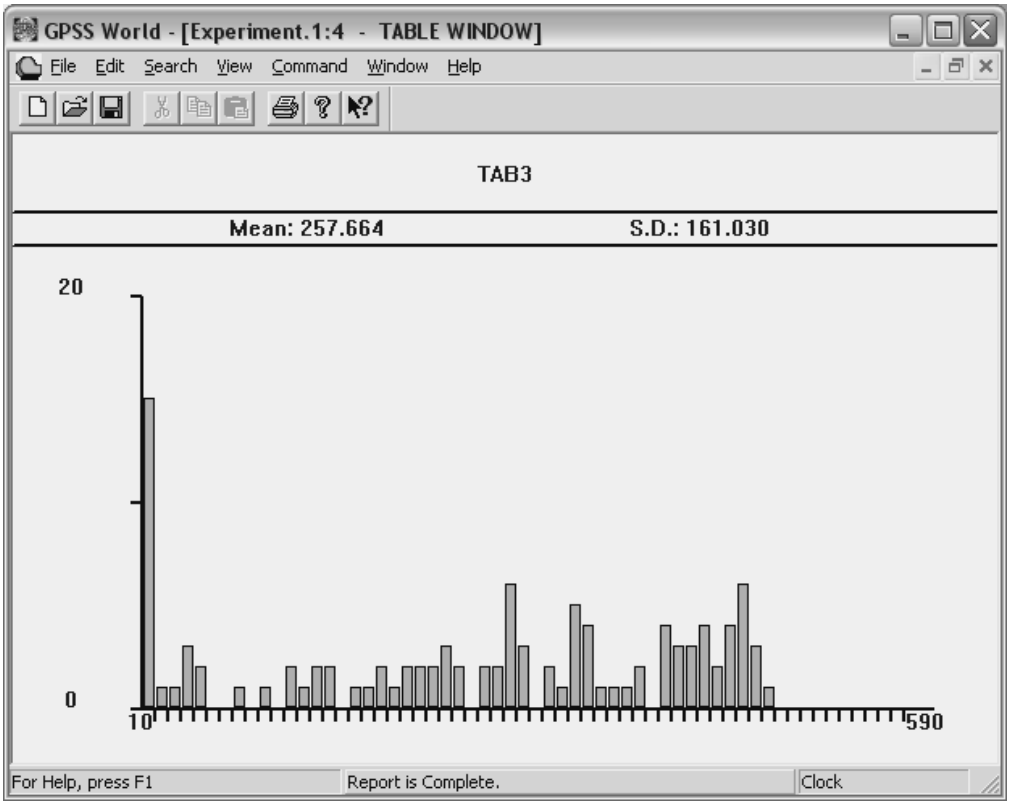


Рис. 4.11. Число пакетов, ожидавших момента обслуживания

Б. Моделирование РИВС под воздействием ВП

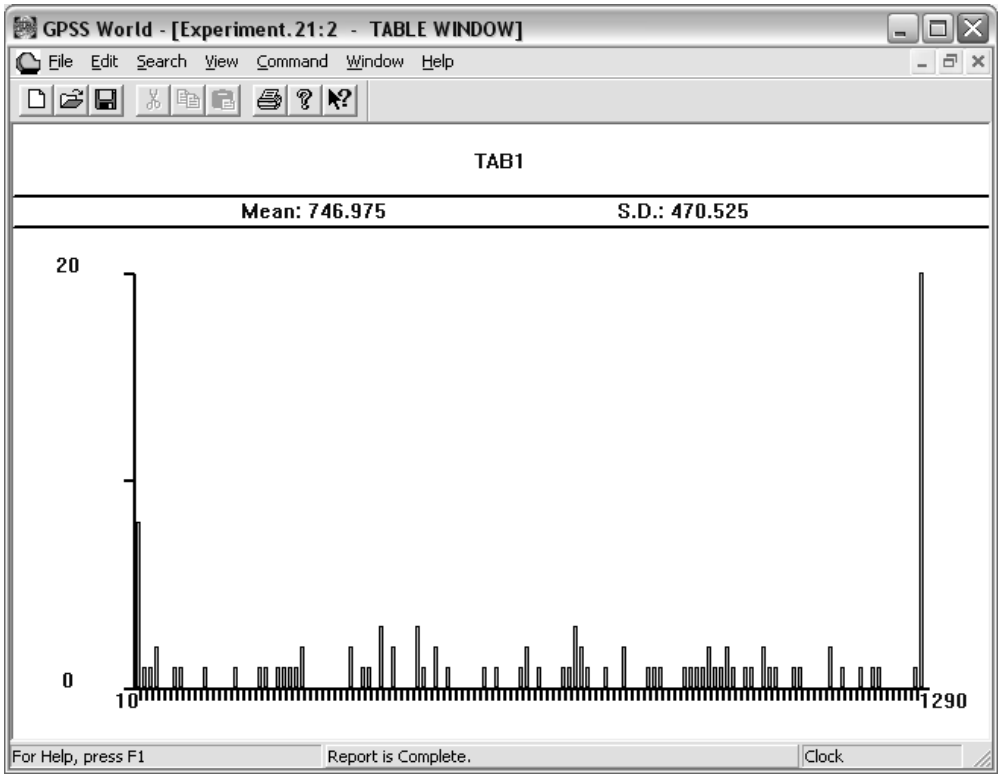


Рис. 4.12. Среднее количество пакетов в очереди

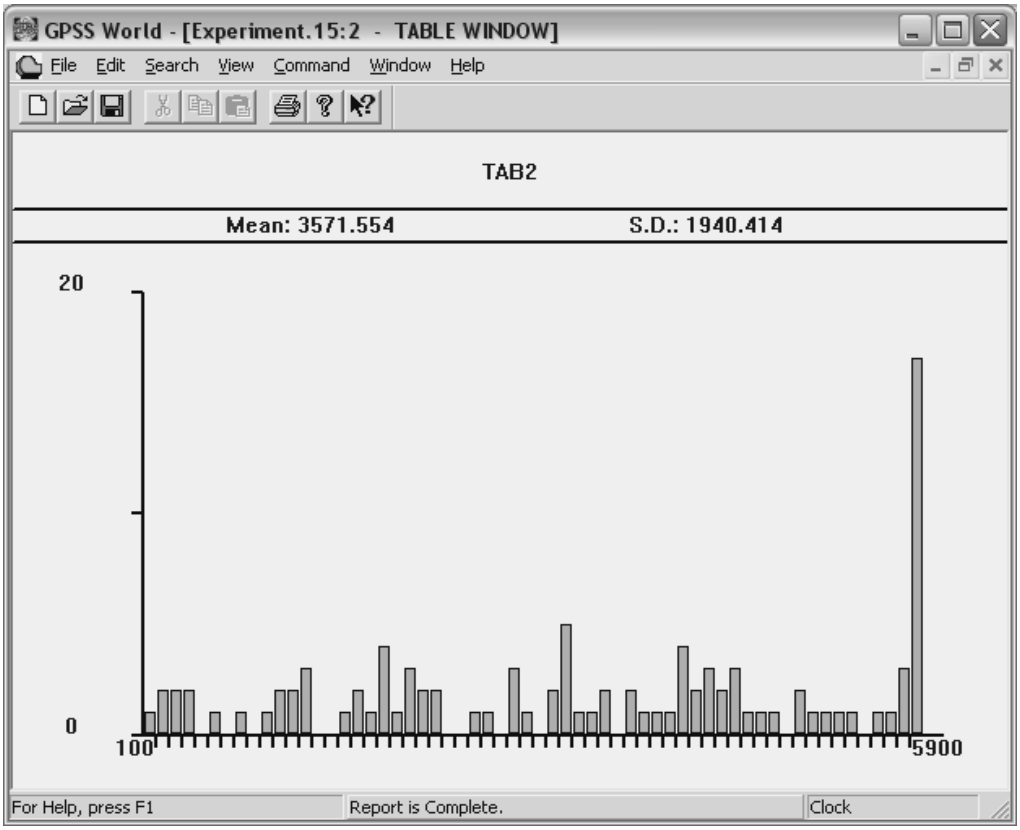


Рис. 4.13. Средняя продолжительность пребывания пакета в системе

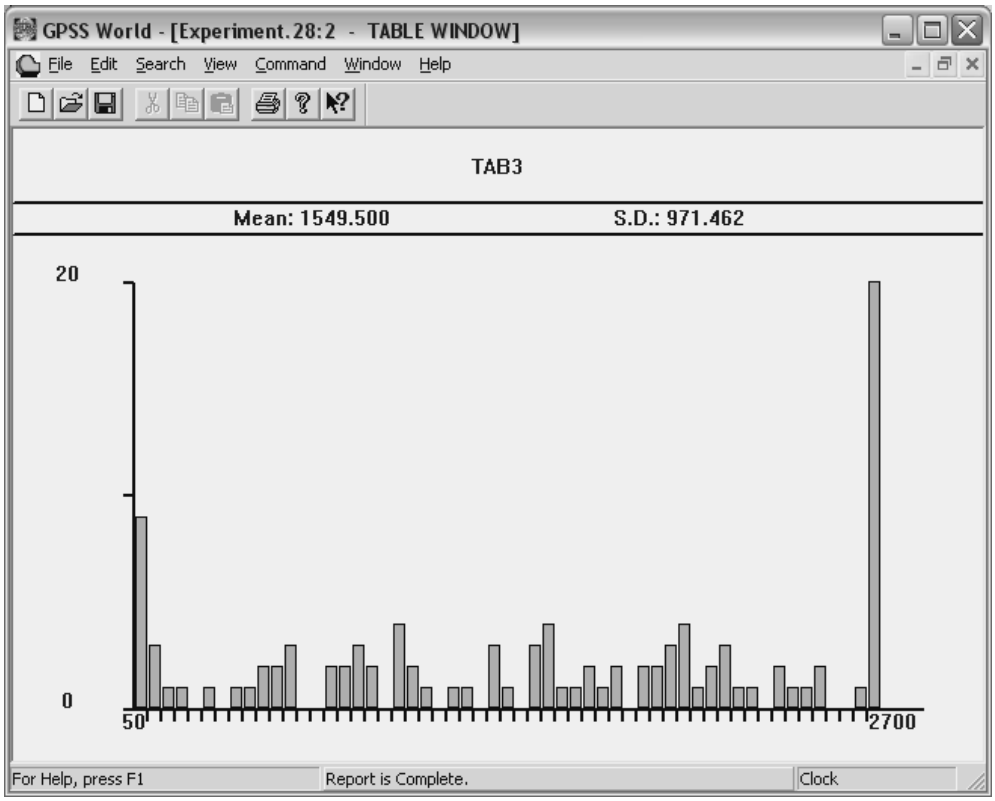


Рис. 4.14. Число пакетов, ожидавших момента обслуживания

В. Моделирование РИВС под воздействием только АП

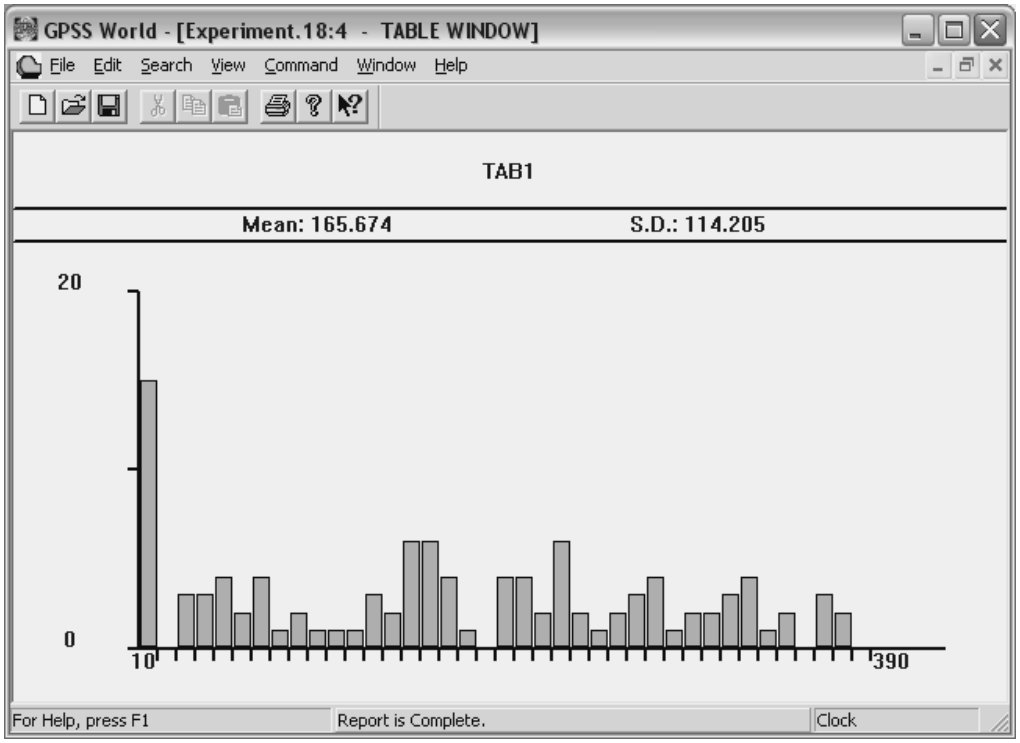


Рис. 4.15. Среднее количество пакетов в очереди

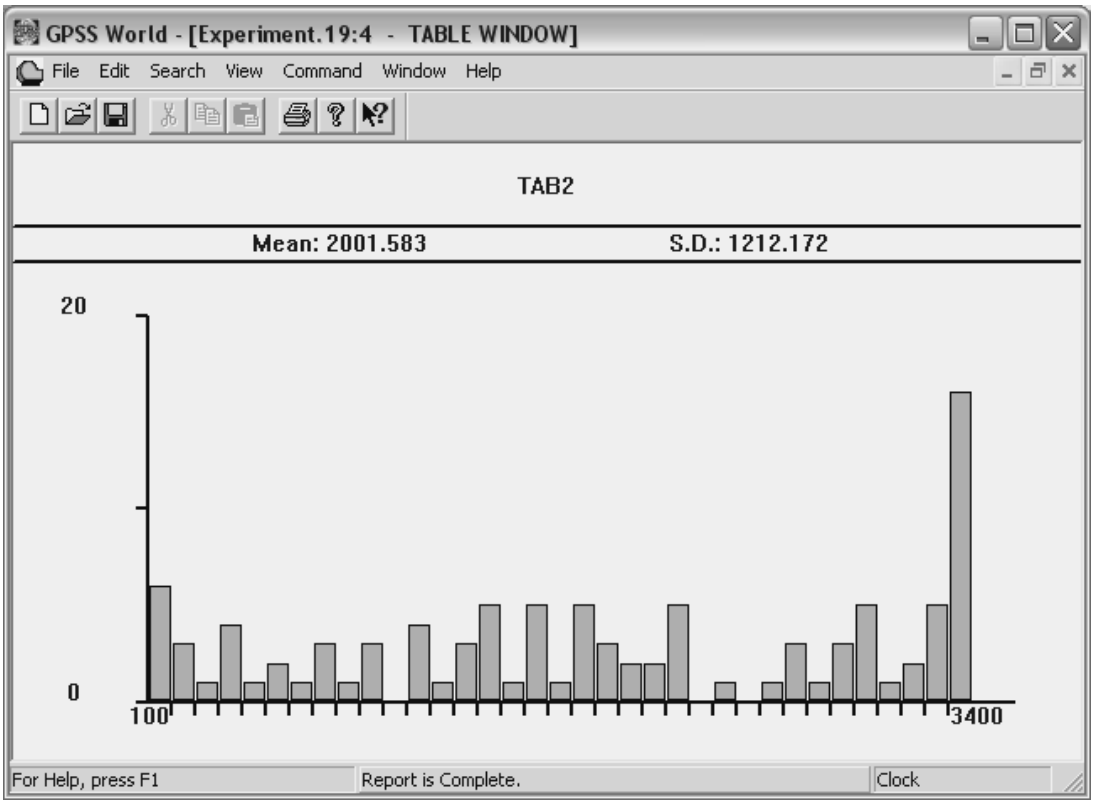


Рис. 4.16. Средняя продолжительность пребывания пакета в системе

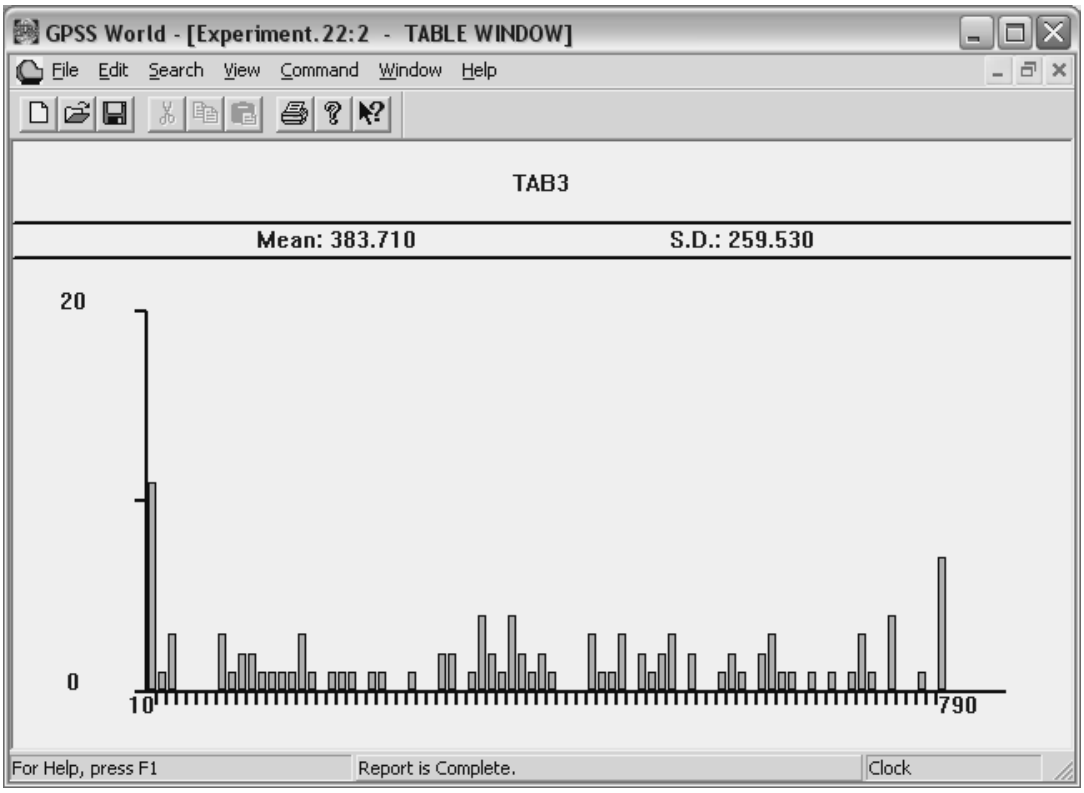


Рис.4.17. Число пакетов, ожидавших момента обслуживания

Графическое представление результатов моделирования визуально отображает увеличение загрузки канала связи и времени пребывания пакета в системе. Средние значения характеристик РИВС по проведенным экспериментам представлены в табл. 4.13.

Табл. 4.13. *Средние значения характеристик КС*

Эксперимент	Среднее количество пакетов в очереди	Средняя продолжительность пребывания пакета в РИВС, ус	Общее число пакетов, ожидавших момента обслуживания
Без влияния	105,8	1716,617	257,664
Влияние ВП	746,975	3571,554	1549,5
Влияние АПО	165,674	2001,583	383,710

Выводы

Аналитическое и имитационное моделирование позволило количественно оценить характеристики производительности РТКС в условиях воздействия вредоносных и антивирусных программ. Наиболее негативное влияние на производительность оказывают ВП (увеличивают частоту генерации пакетов, что, как минимум, перегружает очереди к узлам). Однако и действие антивирусных средств также ухудшает основные характеристики РТКС (АП увеличивают задержку пакетов в узлах, добавляют общий трафик, что замедляет обработку потока пакетов).

Исследование показывает, что при развертывании систем информационной защиты на предприятиях необходимо учитывать, что системы призваны обеспечить не только максимальную защищенность информационных ресурсов, но и не ухудшить системные характеристики РТКС.

Заключение

Сформулируем основные результаты исследования.

1. Разработана модель атаки захвата ресурса распределенной информационно-вычислительной системы вредоносными программами, включающая алгоритмы и процедуры функционирования РТКС в условиях вредоносного информационного воздействия, а также семейство аналитических зависимостей для их описания. Результаты экспериментального исследования предложенных механизмов подтвердили теоретически показанную возможность предсказания состояния РТКС при известных параметрах системы и характеристиках атакующей вредоносной программы.

2. Сформулирована задача построения системы информационной защиты в РТКС как процедура динамического подбора модулей защиты (обнаружения и противодействия), совокупность которых смогла бы за ограниченное время обеспечить максимальную эффективность обнаружения вредоносной программы и противодействия её атаке. Для решения задачи предложена новая модель организации защитных механизмов в РТКС, включающих алгоритмы обнаружения вредоносных программ, устраняющие недостатки традиционных логических схем и позволяющие существенно сократить время обнаружения.

3. Синтезирована модель противодействия вредоносным программам в РТКС, учитывающая нелинейную динамику распространения вредоносных программ. Показано, что процесс изменения численности вакцин и вредоносных программ в РТКС носит колебательный характер. Выявлены механизмы повышения противодействия вредоносным программам и условия, при которых гарантированно можно избежать эпидемии (катастрофы) системы. Разработанная «физическая» модель противодействия выявила периодические

«всплески» деструктивной активности вредоносных программ в РТКС, что позволяет прогнозировать эпидемии в системе и, следовательно, формировать адекватную информационную защиту.

4. Разработано семейство аналитических и имитационных моделей, позволяющих количественно оценить характеристики производительности РТКС в условиях воздействия вредоносных и противодействующих им (антивирусных) программ. Результаты экспериментов показали, что наиболее негативное влияние на производительность оказывают вредоносные программы, увеличивающие частоту генерации пакетов и перегружая очереди к узлам. Исследования показывают, что при развертывании систем информационной защиты необходимо помнить о том, что они не должны ухудшить системные характеристики РТКС.

Список использованных информационных источников*

1. *Абросимов, Л. И.* Основные положения теории производительности вычислительных сетей / Л. И. Абросимов // Вестн. МЭИ. – 2001. – № 4. – С. 70 – 75.

2. *Аверилл, М. Лоу* Имитационное моделирование / М. Лоу Аверилл, В. Дэвид Кельтон. – СПб. : Питер, издат. группа BHV, 2004. – 848 с. – ISBN 5-94723-981-7.

3. *Алексеев, В. В.* Влияние фактора насыщения на динамику системы хищник-жертва / В. В. Алексеев // Биофизика. – 1973. – Т. 18. – Вып. 5. – С. 922 – 926.

4. *Арнольд, В. И.* Лекции о бифуркациях и версальных семействах / В. И. Арнольд. – УМН, 1972. – Т. 27 (176). – Вып 5. – С. 119 – 184.

5. *Он же.* Теория катастроф / В. И. Арнольд. – 3-е изд., доп. – М. : Наука, 1990. – 128 с.

6. *Он же.* Теория катастроф. Современные проблемы математики. Фундаментальные направления / В. И. Арнольд. – М. : ВИНИТИ, 1986. – Т. 5. – С. 219 – 277.

7. *Базыкин, А. Д.* Математическая биофизика взаимодействующих популяций / А. Д. Базыкин. – М. : Наука, 1985. – 182 с.

8. *Биячуев, Т. А.* Безопасность корпоративных сетей : учеб. пособие / Т. А. Биячуев ; под ред. Л. Г. Осоветского. – СПб. : СПбГУ ИТМО, 2004. – 161 с.

9. *Боровков, А. А.* Вероятностные процессы в теории массового обслуживания / А. А. Боровков. – М. : Наука, 1972. – 367 с.

10. *Васильева, А. Б.,* Асимптотические методы в теории сингулярных возмущений / А. Б. Васильева, В. Ф. Бутузов. – М. : Высш. шк., 1990. – 208 с.

11. *Вентцель, А. Д.* Курс теории случайных процессов / А. Д. Вентцель. – М. : Наука, 1972. – 320 с.

* Приводится в авторской редакции.

12. *Вишневский, В. М.* Теоретические основы проектирования компьютерных сетей / В. М. Вишневский. – М. : Техносфера, 2003. – 512 с. – ISBN 5-94836-011-3.

13. *Вольтерра, В.* Математическая теория борьбы за существование / В. Вольтерра ; пер. с фр. ; под ред. Ю. М. Свирежева. – М. : Наука, 1976. – 288 с.

14. *Груздева, Л. М.* Имитационное моделирование корпоративной сети в условиях вредоносного информационного воздействия / Л. М. Груздева // Имитационное моделирование. Теория и практика : сб. докл. Четвертой всерос. науч.-практ. конф. – СПб., 2009. – Т. 2. С. 60 – 64.

15. *Она же.* Модель оценки трудоемкости обнаружения вредоносных программ в компьютерных системах / Л. М. Груздева // Математические методы в технике и технологиях. – ММТТ-23. : сб. тр. XXIII Междунар. науч. конф. – Саратов, 2010. – Т. 9. – С. 160 – 162.

16. *Она же.* Алгоритм оптимизации функционирования распределенной системы защиты / Л. М. Груздева, М. Ю. Монахов // Вестн. Костром. гос. ун-та им. Н. А. Некрасова : науч.-метод. журн. (Сер. Технические и естественные науки. Системный анализ. Теория и практика.). – 2008. – № 2. – Т. 14. – С. 80 – 82.

17. *Она же.* Алгоритм раннего обнаружения атак на информационные ресурсы АСУП / Л. М. Груздева, М. Ю. Монахов // Автоматизация в промышленности. – 2008. – № 3. – С. 12 – 14.

18. *Она же.* Алгоритмы обнаружения угрозы информационной безопасности / Л. М. Груздева [и др.] // Автоматизированная подготовка машиностроительного производства, технология и надежность машин, приборов и оборудования : материалы Междунар. науч.-техн. конф. – Вологда : ВоГТУ, 2005. – Т. 2. – С. 153 – 156.

19. *Она же.* Алгоритмы работы комплекса средств обнаружения угроз информационной безопасности / Л. М. Груздева, М. Ю. Монахов // Информационные системы и технологии в образовании и экономике : сб. тр. науч.-практ. конф. – М. – Покров: МГПУ им. М. А. Шолохова, 2007. – С. 50 – 51.

20. *Груздева, Л. М.* К вопросу оценки эффективности систем информационной защиты предприятия / Л. М. Груздева // Системы и методы обработки и анализа информации : сб. науч. ст. / под ред. С. С. Садыкова, Д. Е. Андрианова. – М. : Горячая линия – Телеком, 2005. – С. 285 – 293.

21. *Она же.* Модель распределенной антивирусной защиты информационной системы предприятия / Л. М. Груздева // Современные проблемы экономики и новые технологии исследований : межвуз. сб. науч. тр. В 2 ч. Ч. 1 / филиал ВЗФЭИ в г. Владимире. – Владимир, 2006. – С. 157 – 158.

22. *Она же.* О задаче построения критической области угроз информационной безопасности / Л. М. Груздева [и др.] // Математические методы в технике и технологиях : сб. тр. XIX Междунар. науч. конф. Т. 10. Секция 11 / ВГТА. – Воронеж, 2006. – С. 194 – 196.

23. *Она же.* Исследование SIR-модели динамики распространения вредоносных программ / Л. М. Груздева // Математические методы в технике и технологиях – ММТТ-21 : сб. тр. XXI Междунар. науч. конф. Т. 5. – Саратов : Сарат. гос. техн. ун-т, 2008. – С. 242 – 244.

24. *Она же.* Подход к достоверному обнаружению угроз информационной безопасности / Л. М. Груздева [и др.] // Комплексная защита объектов информатизации : материалы науч.-техн. семинара. – Владимир : Ред.-издат. комплекс ВлГУ, 2005. – С. 88 – 90.

25. *Она же.* Подход к обеспечению надежности работы АСУП / Л. М. Груздева [и др.] // Краеведение и регионоведение : межвуз. сб. науч. тр. Вып. 2. – Владимир : ВЗФИ, 2006. – С. 144 – 148.

26. *Она же.* Пример формирования критической области в задаче достоверного обнаружения угроз информационной безопасности / Л. М. Груздева, А. Ю. Казарин // Комплексная защита объектов информатизации : материалы науч.-техн. семинара. – Владимир : Ред.-издат. комплекс ВлГУ, 2005. – С. 91 – 92.

27. *Она же.* Проблема защиты информации в АСУП / Л. М. Груздева // Краеведение и регионоведение : межвуз. сб. науч. тр. Вып. 2. – Владимир : ВЗФИ, 2006. – С. 142 – 143.

28. *Груздева, Л. М.* Типовые алгоритмы работы комплекса средств обнаружения угроз информационной безопасности / Л. М. Груздева, А. Ю. Казарин, М. Ю. Монахов // Комплексная защита объектов информатизации : материалы науч.-техн. семинара. – Владимир : Ред.-издат. комплекс ВлГУ, 2005. – С. 58 – 60.

29. *Она же.* Исследование влияния вредоносных и антивирусных программ на характеристики открытой компьютерной сети / Л. М. Груздева // Математические методы в технике и технологиях – ММТТ-22 : сб. тр. XXII Междунар. науч. конф. – Иваново : Изд-во ИГХТУ, 2009. – С. 208 – 210.

30. *Гукенхеймер, Дж.* Нелинейные колебания, динамические системы и бифуркации векторных полей / Дж. Гукенхеймер, П. Холмс. – М. : УРСС, 2002. – 560 с.

31. *Домрачев, А. А.* Общие проблемы информационной безопасности и программа создания ИТКС / А. А. Домрачев // Конфидент. – 1995. – № 3. – С. 3 – 6.

32. *Ивченко, Г. И.* Теория массового обслуживания / Г. И. Ивченко, В. А. Каштанов, И. Н. Коваленко. – М. : Высш. шк., 1982. – 256 с.

33. Информационная безопасность государственных организаций и коммерческих фирм **:** справ. пособие / А. В. Волокитин [и др.] ; под общ. ред. Л. Д. Реймана. – М. : НТЦ "ФИОРД-ИНФО", 2002. – 270 с. – (Современные информационные технологии для управленческого персонала). – ISBN 5-206-00604-1.

34. *Калмыков, М. С.* Основные проблемы защиты от коллективных распределенных атак на вычислительные ресурсы информационных систем / М. С. Калмыков, М. Ю. Монахов // Труды LX науч. сессии, посвященной Дню радио. Т. 1. – М. : Изд-во ЛКИ, 2005. – С. 157 – 158.

35. *Он же.* Распределенные коллективные атаки на вычислительные ресурсы информационных систем / М. С. Калмыков, М. Ю. Монахов // Тр. LX науч. сессии, посвященной Дню радио. Т. 1. – М. : Изд-во ЛКИ, 2005. – С. 161 – 162.

36. *Калмыков, М. С.* Распределенные коллективные атаки на вычислительные ресурсы объектов информатизации и методы защиты от них / М. С. Калмыков, М. Ю. Монахов // Теоретические и прикладные аспекты защиты объектов информатизации : монография ; под ред. Е. М. Сухарева. – М. : Радиотехника, 2007. – 207 с. – ISBN 5-88070-120-4.

37. *Кислицын, А. С.* Распределенный интеллект сети как средство обеспечения информационной безопасности за счет введения динамической составляющей архитектуры вычислительных систем / А. С. Кислицын, А. В. Пружинин, И. В. Бочкарев // Обеспечение информационной безопасности в экономической и телекоммуникационной сферах : монография ; под ред. Е. М. Сухарева. – Кн. 2. – М. : Радиотехника, 2003. – 216 с.

38. *Колбанев, М. О.* Модели и методы оценки характеристик обработки информации в интеллектуальных сетях связи : монография / М. О. Колбанев, С. А. Яковлев. – СПб. : Изд-во СПбГУ, 2002. – 230 с. – ISBN 5-288-03061-8.

39. *Кудрявцев, Е. М.* GPSS World. Основы имитационного моделирования различных систем / Е. М. Кудрявцев. – М. : ДМК Пресс, 2004. – 320 с. – ISBN 5-94074-219.

40. *Кузнецов, С. П.* Динамический хаос / С. П. Кузнецов. – М. : Физматгиз, 2001. – 296 с.

41. *Кульба, В. В.* Задачи анализа и синтеза систем защиты и контроля при обработке данных в АСУ / В. В. Кульба, В. П. Пелихов. – М. : ИПУ, 1980. – 47 с.

42. *Кутузов, О. И.* Имитационное моделирование сетей массового обслуживания : учеб. пособие / О. И. Кутузов, В. Н. Задорожный, С. И. Олзоева. – Улан-Удэ : Изд-во ВСГТУ, 2001. – 228 с. – ISBN 5-89230-184-2.

43. *Малинецкий, Г. Г.* Современные проблемы нелинейной динамики / Г. Г. Малинецкий, А. Б. Потапов. – М. : Эдиториал УРСС, 2002. – 360 с.

44. *Мамиконов, А. Г.* Достоверность, защита и резервирование информации в АСУ / А. Г. Мамиконов, В. В. Кульба, А. Б. Шелков. – М. : Энергоатомиздат, 1986. – 304 с.

45. *Михайлов, А. В.* Метод обнаружения компьютерных вирусов / А. В. Михайлов, Л. М. Груздева // Науч.-практ. конф. «Информационные технологии в образовании и экономике». – Покров : ГОУ ВПО Покров, филиал МГПУ им. М. А. Шолохова, 2007. – С. 76 – 77.

46. *Монахов, М. Ю.* Безопасное управление ресурсами в распределенных информационных и телекоммуникационных системах : монография / М. Ю. Монахов, Ю. А. Илларионов. – Владимир, 2004. – 212 с.

47. *Он же.* Атака на информационную систему предприятия / М. Ю. Монахов, А. И. Соколов // Современные проблемы экономики и новые технологии исследований : межвуз. сб. науч. тр. В 2 ч. Ч. 1 / филиал ВЗФЭИ в г. Владимире. – Владимир, 2006. – С. 118 – 120.

48. *Монахов, Ю. М.* Математическая модель системы мониторинга вредоносного программного обеспечения / Ю. М. Монахов // Методы и технологии автоматизации обучения, компьютерной графики и информационной безопасности : сб. науч. ст. – Владимир : Изд-во Владим. гос. ун-та, 2007. – С. 63 – 65.

49. *Он же.* Проблема обнаружения вредоносной программы / Ю. М. Монахов // Алгоритмы, методы и системы обработки данных : сб. науч. ст. – М. : Центр информ. технологий в природопользовании, 2007. – С. 123 – 128.

50. *Он же.* Автоматизированная система обнаружения аномального функционирования распределенной вычислительной среды АСУ / Ю. М. Монахов, Р. И. Макаров // Системный анализ: теория и практика. – 2009. – № 3.– С. 86 – 89.

51. *Он же.* Атака на информационную систему предприятия / Ю. М. Монахов // Формирование социально-ориентированной экономики: вопросы теории и практики : межвуз. сб. науч. тр. / филиал ВЗФЭИ в г. Владимире. – Владимир, 2007. – С. 105 – 109.

52. *Он же.* Вредоносные программы в компьютерных сетях / Ю. М. Монахов, Л. М. Груздева, М. Ю. Монахов. – Владимир : Изд-во Владим. гос. ун-та, 2010. – 96 с.

53. *Монахов, Ю. М.* Динамика протокола TCP в условиях сетевых атак и перегрузок / Ю. М. Монахов // Математические методы в технике и технологиях – ММТТ-21 : сб. тр. XXI Междунар. науч. конф. В 10 т. – Саратов : Сарат. гос. техн. ун-т, 2008. Т. 7. – С. 264.

54. *Мишин, Д. В.* Информационная система обнаружения атак в сети передачи данных региональной администрации / Д. В. Мишин, Ю. М. Монахов // Алгоритмы, методы и системы обработки данных : сб. науч. ст. – М. : Центр информ. технологий в природопользовании, 2009. – С. 98 – 103.

55. *Монахов, Ю. М.* Использование FARIMA-модели для описания и предсказания поведения сети передачи данных в условиях атак типа «отказ в обслуживании» / Ю. М. Монахов // Горный информ.-аналит. бюл. – 2008. – № 10. – С. 133 – 137.

56. *Илларионов, Ю. А.* Механизм распределенных коллективных атак на ресурсы телекоммуникационных систем / Ю. А. Илларионов, Ю. М. Монахов // Информационные системы и технологии в образовании и экономике : сб. тр. науч.-практ. конф. – М. – Покров : МГПУ им. М. А. Шолохова, 2007. – С. 58.

57. *Полянский, Д. А.* Модель поиска оптимальной структуры системы защиты информации / Д. А. Полянский, Ю. М. Монахов // Информационные системы и технологии в образовании и экономике : сб. тр. науч.-практ. конф. – М. – Покров : МГПУ им. М. А. Шолохова, 2007. – С. 85 – 86.

58. *Монахов, Ю. М.* Модель с противодействием: progressivesidr / Ю. М. Монахов // Информационные системы и технологии в образовании и экономике : сб. тр. науч.-практ. конф. – М. – Покров : МГПУ им. М. А. Шолохова, 2007. – С. 80 – 81.

59. *Груздева, Л. М.* Об одной математической модели динамики распространения вредоносных программ / Л. М. Груздева, Ю. М. Монахов // Математические методы в технике и технологиях – ММТТ-20 // сб. тр. XX Междунар. науч. конф. В 10 т. Секция 12 / под общ. ред. В. С. Балакирева. – Ярославль : Изд-во Ярослав. гос. техн. ун-та, 2007. Т. 6. – С. 65 – 66.

60. *Монахов, Ю. М.* Об одной модели распространения вредоносной программы / Ю. М. Монахов // Информационные технологии в образовательном процессе и управлении : межвузов. сб. ст. / под ред. В. Н. Федосеева. – Шуя : Весть. – 2007. – С. 14 – 15.

61. *Полянский, Д. А.* Оценка безопасности информационно-вычислительной сети на основе формальных моделей / Д. А. Полянский, Ю. М. Монахов // XIX Междунар. науч. конф. «Математические методы в технике и технологиях». – Воронеж, 2006. – Т. 10. – С. 196 – 198.

62. *Монахов, Ю. М.* Оценка сетевых характеристик компьютерных сетей в условиях информационного вредоносного воздействия / Ю. М. Монахов, Л. М. Груздева, М. Ю. Монахов. – Владимир : Изд-во Владим. гос. ун-та, 2010. – 112 с.

63. *Мишин, Д. В.* Экспериментальное исследование эффективности DistributedNetwork IDS / Д. В. Мишин, Ю. М. Монахов // Алгоритмы, методы и системы обработки данных : сб. науч. ст. ; под ред. С. С. Садыкова, Д. Е. Андрианова. – М. : Центр информ. технологий в природопользовании, 2009. – С. 95 – 100.

64. *Груздева, Л. М.* Экспериментальное исследование корпоративной сети передачи данных с адаптивной системой защиты информации / Л. М. Груздева, К. Г. Абрамов, Ю. М. Монахов // Изв. высш. учеб. заведений. Приборостроение. – 2012. – Т. 55. – № 8. – С. 57 – 59.

65. *Она же.* Экспериментальное исследование производительности корпоративной телекоммуникационной сети / Л. М. Груздева, Ю. М. Монахов, М. Ю. Монахов // Проектирование и технология электронных средств. – 2009. – № 4. – С. 21 – 24.

66. *Монахов, Ю. М.* Функциональная устойчивость информационных систем. В 3 ч. Ч. 1. Надежность программного обеспечения / Ю. М. Монахов. – Владимир : Изд-во Владим. гос. ун-та, 2011. – 60 с.

67. *Мишин, Д. В.* Анализ защищенности распределенных информационных систем. Идентификация ресурсов корпоративной сети передачи данных : практикум / Д. В. Мишин, Ю. М. Монахов. – Владимир : Изд-во ВлГУ, 2012. – 96 с. – ISBN 978-5-9984-0295-1.

68. *Николис, Г.* Познание сложного / Г. Николис, И. Пригожин. – М. : Мир, 1990. – 344 с.

69. *Одум, Ю.* Экология. В 2 т. / Ю. Одум. – М. : Мир, 1986. Т. 1. – 328 с; Т. 2. – 376 с.

70. *Пригожин, И.* Время, хаос, квант: к решению парадокса времени ; пер. с англ. / И. Пригожин, И. Стенгенрс. – М. : Прогресс, 1994. – 272 с. – ISBN 5-01-003917-6.

71. *Ризниченко, Г. Ю.* Лекции по математическим моделям в биологии. В 2 ч. Ч. 1 / Г. Ю. Ризниченко. – Ижевск : НИЦ «Регулярная и хаотическая динамика», 2002. – 232 с.

72. *Рыжиков, Ю. И.* Имитационное моделирование. Теория и технологии / Ю. И. Рыжиков. – СПб. : КОРОНА-принт, 2004. – 384 с. – ISBN 5-94271-021.

73. *Советов, Б. Я.* Моделирование систем : учеб. пособие для вузов / Б. Я. Советов, С. А. Яковлев. – М. : Высш. шк., 2001. – 343 с. – ISBN 5-06-003860-2.

74. *Тарасик, В. П.* Математическое моделирование технических систем : учеб. для вузов / В. П. Тарасик. – Минск : ДизайнПРО, 1997. – 640 с. – ISBN 985-6182-10-7.

75. *Тихонов, А. Н.* О системах дифференциальных уравнений, содержащих параметры / А. Н. Тихонов. – М. : МАКС-Пресс, 2001. – С. 231 – 238.

76. *Он же.* Дифференциальные уравнения / А. Н. Тихонов, А. Б. Васильева, А. Г. Свешников. – М. : Наука, 1980. – 231 с.

77. *Трубецков, Д. И.* Введение в синергетику. Хаос и структуры / Д. И. Трубецков; – 2-е изд., испр. и доп. – М. : Эдиториал УРСС, 2004. – 240 с. – ISBN 5-354-00532-9.

78. *Филлипс, Д.* Методы анализа сетей / Д. Филлипс, А. Гарсия-Диас. – М. : Мир, 1984. – 496 с.

79. *Хоффман, Л. Дж.* Современные методы защиты информации / Л. Дж. Хоффман ; пер. с англ. – М. : Сов. радио, 1980. – 246 с.

80. *Цикритзис, Д.* Операционные системы / Д. Цикритзис, Ф. Бернстайн. – М. : Мир, 1977. – 336 с.

81. *Шелухин, О. И.* Моделирование информационных систем / О. И. Шелухин, А. М. Тенякшев, А. В. Осин. – М. : Радиотехника, 2005. – 368 с. – ISBN 5-93108-072-4.

82. *Шеннон, Р. Дж.* Имитационное моделирование систем – искусство и наука / Р. Дж. Шеннон. – М. : Мир, 1978. – 418 с.

83. *Шильников, Л. П.* К вопросу о структуре расширенной окрестности грубого состояния равновесия типа седло-фокус / Л. П. Шильников // Мат. сб. – 1970. – Т. 81 (123). – С. 92 – 103.

84. *Шрайбер, Т. Дж.* Моделирование на GPSS / Т. Дж. Шрайбер. – М. : Машиностроение, 1980. – 592 с.

85. *Aksakaya, H. R., Arditi R., Ginzburg L. R.* Ratio-dependent predation: an abstraction that works, Ecology. – 1995. – 76. – P. 995 – 1004.

86. *Arditi, R., Ginzburg L.R.* Coupling in predator-prey dynamics: ratio-dependence, J. Theor. Biol. – 1989. – 139. – P. 311 – 326.

87. *Beytuk, Yuri.* Estimation of characteristics and optimizing the structure of measuring and controlling contour for flexible technological cell on GPSS-model base. Proc. of Int. Conf. IMEKO'86 "Intelligence measurement", Jena, 10 – 14 Jun., 1986. – P. 287 – 293.

88. *Beytuk, Yuri.* GPSS-simulator of distributed control system in flexible manufacturing (статья). Proc. of the XXXI JUREMA'86, 31st Annual Gathering JUREMA, First symposium on automata and robots in process automatization, 22 – 25 Apr. 1986. – P. 401 – 405.

89. *Carson, J. S.,* Convincing User's of Model's Validity is Challenging Aspect of Modeler's Job, Industrial Engineering, June 1986. – P. 77.

90. *Chi, S.-D., Park J. S., Jung K.-C., Lee J.-S.* Network security modeling and cyber attack simulation methodology // Lecture Notes in Computer Science. Springer-Verlag, 2001. V. 2119.

91. *Chung, M, Mukherjee B., Olsson R. A., Puketza N.* Simulating Concurrent Intrusions for Testing Intrusion Detection Systems // Proceedings of the 18th NISSC. 1995.

92. *Cohen, F.* Simulating Cyber Attacks, Defenses, and Consequences. IEEE Symposium on Security and Privacy, Berkeley, CA. 1999.

93. *Крамер, Г.* Математические методы статистики / Г. Крамер ; пер. с англ.; под ред. А. Н. Колмогорова. – М. : Мир, 1975. – 648 с.

94. *Dawkins, J., Campbell, C., Hale, J.* Modeling network attacks: Extending the attack tree paradigm // Workshop on Statistical and Machine Learning Techniques in Computer Intrusion Detection, Johns Hopkins University. 2002.

95. *deRoos, A. M.* Modeling Population Dynamics. Institute for Biodiversity and Ecosystem Dynamics, Population Biology Section, University of Amsterdam, 2004.

96. *Gordon, Geoffre.* System Simulation, 2nd ed., Prentice-Hall, 1978.

97. *Harrell, Charles R., Tumay Kerim,* Simulation Made Easy, Industrial Engineering Press, 1995.

98. *Holling, C. S.* The functional response of predator to prey density and its role in mimicry and population regulation. – Mem. Entomol. Soc. Canada. – 1965. – V. 45. – P. 1 – 60.

99. Антивирус ESET NOD32. [Электронный ресурс] Режим доступа: http://www.esetnod32.ru/products/av_home.php

100. НОУ ИНТУИТ | Учебный курс | Антивирусная защита компьютерных систем [Электронный ресурс] Режим доступа: http://www.intuit.ru/department/security/antiviruskasp/5/

101. Kaspersky Anti-Virus | Kaspersky Lab RU [Электронный ресурс] Режим доступа: http://www.kaspersky.ru/kaspersky_anti-virus_7_0

102. *Iglun, K., Kemmerer R. A., Porras P. A.* State Transition Analysis: A Rule-Based Intrusion Detection System // IEEE Transactions on Software Engineering, – V.21. – No. 3. – 1995.

103. *Izhikevich, E.M.* Neural Excitability, Spiking and Bursting. International Journal of Bifurcation and Chaos . – V. 10. – № 6 (2000).

104. *Jost, C., Arino, O., Arditi, R.* About deterministic extinction in ratio-dependent predator-prey models. Bull. Math. Biol. – 1999. – 61. – P. 19 – 32.

105. *Law, Averill M.* "Designing and Analyzing Simulation Experiments", Industrial Engineering, March 1991. – P. 20 – 23.

106. *Law, Averill M. Kelton, David W.* Simulation Modeling and Analysis, McGraw-Hill, 1991.

107. *Lotka A. J.* Elements of physical biology. Baltimore: Williams and Wilkins, 1925.

108. *May, R. M.* Bifurcations and dinamic complexity in ecological systems. – Annals, New York Academy of Sciences, 1979. – P. 517.

109. *May, R. M.* Theoretical Ecology: Principles and Applications. – Oxford: Blackwell, 1976.

110. *Maynard, Smith J.* Models in ecology. Camdridge University Press, London.NY, 1974.

111. *Neelamkavil, Francis.* Computer Simulation and Modeling, John Wiley & Sons, 1987.

112. *Nicolis G., Prigogine I.* Self-Organization in Non-Equilibrium Systems. From Dissapative Structures to Order through Fluctuations.- New York^ Wiley, 1977.

113. *Pritsker, Alan B. Pegden, Claude Dennis.* Introduction to Simulation and SLAM, John Wiley & Sons. 1979.

114. *Thompson, J.M.T.* An evolution game for a prey – predator ecology. – Bull. Inst. Math. And Its Appl., 1979. – P. 162.

115. *Thompson J.M.T.* Experiments in catastrophe. – Nature, 1975. – P. 392.

116. *Tumay, Kerim*, Business Process Reengineering Using Simulation, Autofact Workshop, 1993.

117. *Yuill, J., Wu F., Settle J., Gong F.* Intrusion-detection for incident-response, using a military battlefield-intelligence process // Computer Networks, No. 34. – 2000.

Оглавление

Научное издание

МОНАХОВ Юрий Михайлович
ГРУЗДЕВА Людмила Михайловна

ТЕОРЕТИЧЕСКОЕ И ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ РАСПРЕДЕЛЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ ВРЕДОНОСНЫХ ПРОГРАММ

Монография

Подписано в печать 18.12.13.
Формат 60x84/16. Усл. печ. л. 7,67. Тираж 50 экз.
Заказ
Издательство
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых.
600000, Владимир, ул. Горького, 87.