ИНФОРМАЦИОННЫЙ АНАЛИЗ

УДК 004.7:004.49

Г. Б. Гольфельд, Н. А. Малыхин, И. И. Потапов

Оценка потенциальной осуществимости цели глобальных информационно-вычислительных систем в условиях действия "интеллигентных компьютерных вирусов"

Рассматривается применение принципов теории сложных систем к формализации задачи анализа влияния компьютерных вирусов замедленного действия на глобальные информационно-вычислительные системы. Результаты могут представлять интерес для специалистов по информатике и экоинформатике.

Подлинным бедствием в компьютерном мире стало распространение "компьютерных вирусов". Так, по данным [1], в 1988 г. было отмечено свыше 400 эксцессов в работе 90 тыс. персональных компьютеров. Ущерб от перебоев в работе вычислительных систем при этом исчисляется сотнями миллионов долларов.

К настоящему времени ассортимент вирусов чрезвычайно разнообразен [1]: это и вирусы, распространяющиеся по системе сразу после ее включения и с задержкой, и вирусы, поражающие систему на этапе загрузки, разрушающие ее системные ресурсы, способствующие ускоренному изнашиванию электромеханических узлов дисководов, а также искажающие прикладное программное обеспечение.

Для глобальных информационно-вычислительных систем (ИВС) особую опасность представляют вирусы, действие которых запрограммировано на длительный срок (до нескольких лет), а характер воздействия на ИВС носит завуалированный характер. Так, в ИВС глобального экологического мониторинга вирусы могут "правдоподобно" искать базы данных без явных признаков нарушения работы системы. Нетрудно представить себе, каким будет качество экологических прогнозов, основанное на массивах гидрометеорологических данных, подвергшихся некоторой "коррекции". Для информационно-поисковых систем можно представить себе длительное бесплодное блуждание по компьютерным библиотекам.

Таким образом, становится весьма актуальной проблема заблаговременного обнаружения действия вирусов "интеллигентов" с тем, чтобы ликвидировать результаты их деятельности до того, как процесс эрозии баз данных (и знаний?!) примет необратимый характер.

Возникновение таких проблем стимулировало появление новой междисциплинарной науки — "компьютерной вирусологии". В ней пока не сформировался канонический формализм. Поэтому для того, чтобы последующие размышления носили конструктивный характер, попытаемся рассмотреть проблемы вирусной инфекции в рамках кибернетической теории сложных систем, разработанной в монографии [2].

В публикациях [3–5] нами уже затрагивались аспекты системотехнического формализма применительно к ИВС в банковской и образовательной сферах.

В работе [6] на примере информационно-издательского комплекса (ИК) ВИНИТИ рассматривалась формализация процесса функционирования сложных информационно-вычислительных систем в системологических терминах оптимального (u, v)-обмена, предложенного в работе [2]. Напомним его основные особенности.

Итак, в соответствии с системологическими принципами [2], реальная ИВС представляется абстрактной системой A, а информационная среда, в которой действует ИВС, — абстрактной средой, также можно рассматривать как некоторую систему B. Система A определяется своей структурой $Str(A)$ и поведением $Beh(A)$:

$$A = \{Str(A),\ Beh(A)\}.$$

Цель функционирования системы A — достижение некоторого заданного предпочтительного состояния. Обозначим эту цель через $Goal(A)$. Аналогичные понятия вводятся для среды B :

$$B = \{Str(B),\ Beh(B)\}.$$

Цель среды обозначим как $Goal(B)$. Взаимодействие систем A и B представляется в виде взаимного (u, v)-обмена, соответственно, расходуемыми и потребляемыми v информационными и материальными ресурсами. При этом целью систем является установление выгодного (оптимального) в некотором смысле режима обмена. Из-за объективно случайного характера взаимодействия системы и среды, следуя [2], можно говорить лишь о некоторой вероятности $P(u, v) = P[Goal(A)]$ достижения системой своей цели.

В условиях конфликтной ситуации, когда у системы A и среды B цели противоположны, вероятности их достижения за фиксированное время T равны, соответственно:

$$P(T) = P[Goal(A)],$$

$$Q(T) = P[Goal(B)] = 1 - P(T).$$

Из практических соображений могут быть назначены допустимые вероятность P' и время T' достижения своей цели системой A. Пару значений (P', T'), следуя [2], будем называть *порогами осуществимости*. При этом будем говорить, что достижение цели системой A потенциально (в принципе) осуществимо, если для некоторого времени T одновременно выполняются два неравенства:

$$P(T) \geqslant P',$$

$$T \leqslant T'.$$

Аналогичное верно для среды B. В соответствии с работой [2], вероятность достижения ИВС своей цели при этом можно представить в виде:

$$P(T) = p(T)\,q(T).$$

Здесь $p(T)$ — надежность системы A, т. е. вероятность безотказного функционирования системы A (суть ИВС) за время T, а $q(T)$ — вероятность достижения цели системой A за время T при условии безотказного функционирования ИВС в течение этого времени.

Из теории потенциальной эффективности сложных систем [6] также известно, что в качестве предельных допустимы экспоненциальные оценки:

$$p(T) = \exp(-T/f),$$

$$q(T) = 1 - \exp(-gT),$$

где f — не зависящий от T параметр внутренней эффективности системы A, численно равный среднему времени между ее отказами, а g — также не зависящий от T параметр внешней эффективности системы A.

Теория сложных систем [2], формальных правил для установления семантического смысла параметра внешней эффективности g, вообще говоря, не дает. Поэтому его идентифицировать следует индивидуально — для каждой конкретной информационно-вычислительной системы [3–6].

Соответственно, вероятность достижения цели системой A в экспоненциальном случае, как показано в [2], выражается формулой:

$$P(T) = [\exp(-T/f)] \times [1 - \exp(-gT)].$$

Если учитывать действие вирусов, поражающих ИВС таким образом, что процесс ее баз данных и программного обеспечения развивается постепенно, среднее время между отказами системы f уже нельзя полагать не зависящим от времени функционирования системы T, т. е. $f = f(T)$.

Поскольку в настоящее время еще нет надежных статистических данных о влиянии "интеллигентных вирусов" на базы данных, то пока неизбежно привлечение эвристических и имитационных моделей.

Так, на рис. 1 в относительном масштабе представлены некоторые эпюры вероятности достижения системой своей цели для характерных эвристических экспоненциальной, периодической и экспоненциально-периодической моделей зависимости f от T:

$$f(T) = \begin{cases} f(0)\exp(-T), \\ f(0)[\cos(T) + 1]/2, \\ f(0)\exp(-T) \times [\cos(T) + 1]/2. \end{cases}$$

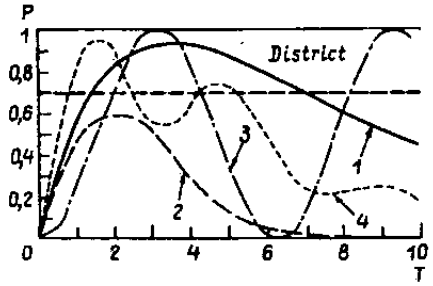

Рис. 1. Зависимость вероятности осуществления цели ИВС: 1 — при отсутствии вируса, 2 — экспоненциальный вирус, 3 — периодический вирус, 4 — экспоненциально-периодический вирус

Здесь $f(0)$ — среднее время между отказами ИВС в начале ее эксплуатации. Зона осуществимости цели системы обозначена как District.

Нетрудно видеть, к каким катастрофическим для пользователя ИВС последствиям может привести действие вируса: это и потеря системой осуществимости своей цели и циклический выход из критической зоны параметров, ограниченной порогами осуществимости, а также не предусмотренное при проектировании ИВС изменение оптимальных значений параметров.

На рис. 2 показан возможный вид экспоненциального поля вероятности достижения цели системой как функции параметров внешней и внутренней эффективности.

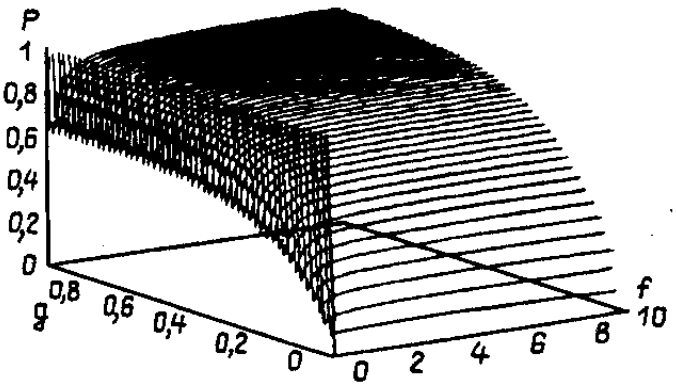

Рис. 2. Поле вероятности осуществления цели ИВС

Таким образом, применение методов теории сложных систем в принципе позволяет формализовать процесс функционирования ИВС в условиях действия на базы данных "интеллигентных компьютерных вирусов".

В перспективе развитие такого подхода позволит перейти к разработке программно-алгоритмических средств мониторинга состояния ИВС с целью заблаговременного обнаружения вирусной инфекции и ослабления или ликвидации ее последствий.

В заключение обращаем внимание читателей на принципиальный момент: до сих пор в теории